

جامعة قسنطينة 1 الإخوة منتوري

كلية الحقوق

قسم القانون الخاص



رقم الترتيب: 57/D3C/2024

الرقم التسلسلي: 08/Dpr/2024

السياسة الجنائية في مكافحة الجريمة الإلكترونية في التشريع الجزائري

أطروحة لنيل شهادة الدكتوراه ل م د

شعبة الحقوق، تخصص: قانون العقوبات والعلوم الجنائية

من إعداد الطالبة:

قنفود نبيهة

لجنة المناقشة

جامعة قسنطينة 1	أستاذ التعليم العالي	رئيسا	بولمكل أحمد
جامعة قسنطينة 1	أستاذ التعليم العالي	مشرفا ومقررا	فوزي عمارة
جامعة قسنطينة 1	أستاذ التعليم العالي	ممتحنا	نقاش حمزة
جامعة قسنطينة 1	أستاذ محاضرا-أ	ممتحنا	بن مسعود شهرزاد
جامعة - سكيكدة	أستاذة التعليم العالي	ممتحنا	غزيوي هنده
جامعة - سكيكدة	أستاذ محاضرا-أ	ممتحنا	بن مشيرح محمد

تاريخ المناقشة:

2024/10/08

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

شكر و تقدير

أتقدم بداية بالشكر لله سبحانه وتعالى، الذي أعانني وأمدني العزم والصبر ووفقني لإنجاز هذا العمل المتواضع .

وإمتثالاً لقول المصطفى عليه أفضل الصلاة وأزكى التسليم "من لا يشكر الناس لا يشكر الله"

أتقدم بأسمى عبارات الشكر والتقدير لأستاذي الفاضل الأستاذ الدكتور فوزي عمارة، الذي قبل الإشراف على هذه الأطروحة بصدر رحب رغم كثرة إنشغالاته، الذي لم يخلني بتوجيهاته القيمة التي كانت نبراساً أناري لطريقي لإنجاز هذا العمل، فجزاه الله عن خير الجزاء .

الشكر موصول كذلك لأعضاء لجنة المناقشة المحترمة التي قبلت تحمل عبء مراجعة هذا العمل، وتصويب أفكاره وأخطائه بما تراه ملائماً ومناسباً لهذه الأطروحة كل باسمه: أ. د/ أحمد بولمكاحل، أ. د/ حمزة نقاش، أ. د/ هنده غزوي، د/ محمد بن مشيرح ود/ شهرزاد بن مسعود .

الباحثة/ نبيهة قنفود

إهداء

إلى روح أبي وأمي الطاهرتين . رحمة الله عليهما وجعل الله مثواهما جنة الفردوس

إلى رفيق دربي الذي صبر وقدم لي يد العون في كل أطوار الرسالة زوجي الغالي

إلى من أشد بهم أزرى إخوتي حفظهم الله

إلى أخواتي سندي في هذه الحياة رعاهم الله

إلى صغيرتي نور الهدى شكرا على المساعدة

إلى كل هؤلاء أهدي ثمرة جهدي

فهرس الموضوعات

فهرس الموضوعات

الملخص

2 مقدمة

الباب الأول

الجوانب الموضوعية لمكافحة الجريمة الالكترونية

الفصل الأول: الإطار المفاهيمي للجريمة الالكترونية

7 المبحث الأول: ماهية الجريمة الإلكترونية

8 المطلب الأول: مفهوم الجريمة الإلكترونية

8 الفرع الأول: تعريف الجريمة الإلكترونية

9 الفقرة الأولى: تعريف الجريمة الإلكترونية فقها

13 الفقرة الثانية: التعريف القانوني للجريمة الإلكترونية

16 الفرع الثاني: خصائص الجريمة الإلكترونية

21 الفرع الثالث: التطور التاريخي للجريمة الإلكترونية

25 الفرع الرابع: تصنيف الجرائم الإلكترونية

25 الفقرة الأولى: تصنيفات تبعا لنوع المعطيات ومحل الجريمة

26 الفقرة الثانية: تصنيف الجرائم تبعا لدور الكمبيوتر في الجريمة

27 الفقرة الثالثة: تصنيف الجرائم تبعا لمساسها بالأشخاص والأموال

29 الفقرة الرابعة: تصنيف الجرائم تبعا لمساسها بالمصلحة العامة

30 الفقرة الخامسة: تصنيف الجرائم كجرائم حاسوب وجرائم أنترنت

31 الفرع الخامس: دور الحاسب الآلي في ارتكاب الجريمة الإلكترونية

33 المطلب الثاني: البنيان القانوني للجريمة الإلكترونية

34 الفرع الأول: المعلومات كمحل للجريمة الإلكترونية

34	الفقرة الأولى: تعريف المعلومات.....
38	الفقرة الثانية: الشروط الواجب توافرها في المعلومة محل الاعتداء.....
39	الفقرة الثالثة: أنواع المعلومات.....
40	الفقرة الرابعة: الطبيعة القانونية للمعلومات.....
44	الفرع الثاني: أركان الجريمة الإلكترونية.....
44	الفقرة الأولى: الركن الشرعي للجريمة الإلكترونية.....
46	الفقرة الثانية: الركن المادي.....
50	الفقرة الثالثة: الركن المعنوي للجريمة الإلكترونية.....
51	الفرع الثالث: الشروع.....
55	الفرع الرابع: الاتفاق الجنائي.....
56	الفقرة الأولى: تعريف الاتفاق الجنائي.....
57	الفقرة الثانية: أركان الاتفاق الجنائي.....
59	الفقرة الثالثة: الركن المعنوي.....
60	المطلب الثالث: طرفا الجريمة الإلكترونية.....
61	الفرع الأول: الجاني في الجريمة الإلكترونية.....
61	الفقرة الأولى: سمات المجرم المعلوماتي.....
65	الفقرة الثانية: طوائف وفئات الجاني.....
69	الفرع الثاني: أسباب ودوافع ارتكاب الجريمة الإلكترونية.....
70	الفقرة الأولى: الدوافع الشخصية.....
74	الفرع الثالث: المجني عليه في الجريمة الإلكترونية.....
77	المطلب الرابع: مبررات الحماية.....
77	الفرع الأول: خطورة الجرائم الإلكترونية.....
82	الفرع الثاني: قصور القوانين التقليدية.....

85	المبحث الثاني: المرجعيات المؤطرة للجرائم الإلكترونية وتأثر المشرع بها.....
86	المطلب الأول: الجهود الدولية لمكافحة الجريمة الإلكترونية.....
86	الفرع الأول: جهود الأمم المتحدة لمكافحة الجريمة الإلكترونية.....
88	الفرع الثاني: دور المنظمة العالمية للملكية الفكرية.....
90	الفرع الثالث: الإتحاد الدولي للاتصالات.....
91	المطلب الثاني: الجهود الإقليمية لمواجهة الجريمة الإلكترونية.....
91	الفرع الأول: دور المجلس الأوروبي في مكافحة الجريمة الإلكترونية.....
92	الفقرة الأولى: إتفاقية بودابست.....
99	الفقرة الثانية: البرتوكول الإضافي لاتفاقية مجلس أوروبا.....
101	الفقرة الثالثة: جهود مجموعة الدول الثمانية (G 8)
102	الفرع الثاني: جهود الدول العربية في مكافحة الجريمة الإلكترونية.....
106	الفرع الثالث: جهود الاتحاد الأفريقي في مكافحة الجريمة الإلكترونية.....
106	المطلب الثالث: تأثر الجزائر بالجهود الدولية في مجال الجريمة الإلكترونية.....
107	الفرع الأول: جهود الدول الغربية.....
110	الفرع الثاني: التشريع الجزائري.....

الفصل الثاني:

المواجهة التشريعية للجريمة الإلكترونية

118	المبحث الأول: مواجهة الجريمة الإلكترونية بموجب قانون العقوبات.....
118	المطلب الأول: جريمة القذف أو السب أو الإهانة باستعمال الوسائل الإلكترونية.....
119	الفرع الأول: جريمة الإساءة لرئيس الجمهورية.....
119	الفقرة الأولى: جريمة الإهانة.....
122	الفقرة الثانية: جريمة القذف.....
125	الفقرة الثالثة: جريمة السب.....

127	الفرع الثاني: جرائم الإهانة والقذف والسب في حق مؤسسات الدولة.....
128	المطلب الثاني: جرائم المساس بأنظمة المعالجة الآلية للمعطيات.....
129	الفرع الأول: جريمة الدخول أو البقاء غير المصرح به.....
129	الفقرة الأولى: مفهوم نظام المعالجة الآلية للمعطيات.....
133	الفقرة الثانية: صور جريمة الدخول أو البقاء غير المصرح به.....
142	الفرع الثاني: جريمة التلاعب غير المصرح به بمعلومات نظام المعالجة الآلية.....
146	الفرع الثالث: جريمة التعامل في معلومات غير مشروعة.....
152	الفرع الرابع: الجرائم الأخرى ضد الأنظمة.....
153	الفقرة الأولى: جريمة إعاقة أو تحريف تشغيل نظم المعالجة الآلية للمعطيات.....
155	الفقرة الثانية: جريمة سرقة وقت النظام المعلوماتي.....
157	المطلب الثالث: جريمة الإرهاب الإلكتروني.....
157	الفرع الأول: مفهوم الإرهاب الإلكتروني.....
161	الفرع الثاني: صور وأشكال الارهاب الإلكتروني.....
163	الفرع الثالث: صور جرائم الإرهاب الإلكتروني.....
163	الفقرة الأولى: جريمة السفر إلى دولة أخرى لارتكاب أفعال إجرامية.....
167	الفقرة الثانية: جريمة التجنيد.....
170	المطلب الرابع: الاعتداء على حرمة الحياة الخاصة.....
171	الفرع الأول: مفهوم حرمة الحياة الخاصة.....
173	الفرع الثاني: صور الاعتداء على حرمة الحياة الخاصة.....
173	الفقرة الأولى: جريمة التقاط الأحاديث والصور دون رخصة.....
177	الفقرة الثانية: جريمة التقاط أو تسجيل أو نقل الصورة.....
179	الفقرة الثالثة: جريمة الاحتفاظ أو الوضع أو الاستعمال للتسجيلات أو الصور أو الوثائق..
182	المطلب الخامس: الاستغلال الأطفال في المواد الاباحية عبر شبكة الأنترنت.....

183	الفرع الأول: مفهوم جريمة الاستغلال في المواد الاباحية.....
184	الفرع الثاني: موقف المشرع الجزائري.....
185	الفرع الثالث: صور الاستغلال الجنسي.....
188	المبحث الثاني: مواجهة الجريمة الإلكترونية بموجب قوانين خاصة.....
188	المطلب الأول: جرائم الاعتداء على الملكية الفكرية.....
189	الفرع الأول: مفهوم المصنف الرقمي.....
189	الفقرة الأولى: تعريف المصنفات الرقمية.....
190	الفقرة الثانية: أنواع المصنفات الرقمية.....
198	الفرع الثاني: صور جرائم التعدي على حق الملكية الأدبية والفنية.....
198	الفقرة الأولى: جريمة تقليد.....
202	الفقرة الثانية: الجرائم الملحقة بجريمة التقليد.....
204	المطلب الثاني: التوقيع الإلكتروني.....
204	الفرع الأول: مفهوم التوقيع الإلكتروني.....
209	الفرع الثاني: صور الجرائم الواقعة على التوقيع الإلكتروني.....
213	المطلب الثالث: جرائم الإعتداء على المعطيات الشخصية.....
214	الفرع الأول: مفهوم المعطيات ذات الطابع الشخصي.....
216	الفرع الثاني: صور الجرائم الماسة بمعطيات ذات الطابع الشخصي.....
216	الفقرة الأولى: التجريم المتعلق بالجمع غير المشروع للمعطيات ذات الطابع الشخصي....
220	الفقرة الثانية: الجرائم المتعلقة بالأفعال المرتكبة خلال المعالجة الآلية للمعطيات الشخصية
	الفقرة الثالثة: تجريم الأفعال المتعلقة بالاستغلال غير المشروع للمعطيات ذات الطابع
224	الشخصي.....
230	الفقرة الرابعة: تجريم الأفعال المساس بصلاحيات السلطة الوطنية لحماية المعطيات.....
234	المطلب الرابع: جرائم الاعتداء على التجارة الإلكترونية.....

235	الفرع الأول: التجارة الإلكترونية والجرائم الواقعة عليها.....
235	الفقرة الأولى: مفهوم التجارة الإلكترونية.....
237	الفقرة الثانية: صور الاعتداء على التجارة الإلكترونية.....
241	الفرع الثاني: المستهلك الإلكتروني.....
241	الفقرة الأولى: مفهوم المستهلك الإلكتروني.....
243	الفقرة الثانية: صور الاعتداء.....
250	الفرع الثالث: وسائل الدفع الإلكتروني وصور الإعتداء عليها.....
251	الفقرة الأولى: مفهوم وسائل الدفع الإلكتروني.....
252	الفقرة الثانية: صور الاعتداء على وسائل الدفع الإلكترونية.....

الباب الثاني:

الجوانب الاجرائية لمكافحة الجريمة الالكترونية

الفصل الأول:

مواجهة الجريمة الالكترونية وفقا لقانون الإجراءات الجزائية

260	المبحث الأول: تكييف القواعد الإجرائية التقليدية لإستخلاص الدليل الإلكتروني.....
261	المطلب الأول: الشكوى والبلاغ في الجريمة الإلكترونية.....
261	الفرع الأول: تلقي البلاغات والشكاوى بصفة عامة.....
263	الفرع الثاني: كيفية الشكوى والبلاغ في الجريمة الإلكترونية.....
265	المطلب الثاني: المعاينة والخبرة التقنية لاستخلاص الدليل الإلكتروني.....
266	الفرع الأول: المعاينة في الجريمة الإلكترونية.....
266	الفقرة الأولى: مفهوم المعاينة.....
269	الفقرة الثانية: الضوابط المتبعة في إجراء المعاينة.....
273	الفرع الثاني: الخبرة التقنية في الجريمة الإلكترونية.....
273	الفقرة الأولى: مفهوم الخبرة التقنية.....

278	الفقرة الثانية: الضوابط القانونية والفنية للخبرة التقنية.....
283	المطلب الثالث: الشهادة في الجريمة الالكترونية.....
284	الفرع الأول: مفهوم الشهادة والشاهد المعلوماتي في الجريمة الإلكترونية.....
288	الفرع الثاني: التزامات الشاهد المعلوماتي.....
293	المطلب الرابع: الاختصاص القضائي للجهات القضائية في الجريمة الإلكترونية.....
293	الفرع الأول: توسيع الاختصاص المحلي للجهات القضائية.....
296	الفرع الثاني: القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.
303	المبحث الثاني: الإجراءات المستحدثة لمكافحة الجريمة الإلكترونية.....
304	المطلب الأول: اعتراض المراسلات وتسجيل الأصوات.....
304	الفرع الأول: مفهوم اعتراض المراسلات وتسجيل الأصوات.....
304	الفقرة الأولى: تعريف اعتراض المراسلات.....
307	الفقرة الثانية: تسجيل الأصوات.....
308	الفرع الثاني: شروط وضوابط تنفيذ إجراء اعتراض المراسلات وتسجيل الأصوات.....
309	الفقرة الأولى: الشروط الموضوعية.....
310	الفقرة الثانية: الشروط الشكلية لإجراءات اعتراض المراسلات وتسجيل الأصوات.....
312	المطلب الثاني : التقاط الصور.....
313	الفرع الأول: مفهوم التقاط الصور.....
314	الفرع الثاني: إجراءات التقاط الصور.....
316	المطلب الثالث: التسرب الإلكتروني.....
316	الفرع الأول: مفهوم التسرب.....
317	الفرع الثاني: الأحكام الضابطة لعملية التسرب.....
317	الفقرة الأولى الشروط الشكلية.....
319	الفقرة الثانية: الشروط الموضوعية.....

320		الفرع الثالث: آثار التسرب
323		المطلب الرابع: صعوبات الحصول على الدليل الإلكتروني بالوسائل التقليدية
324		الفرع الأول: مفهوم الدليل الإلكتروني
333		الفرع الثاني: صعوبات إثبات الدليل الإلكتروني
336		الفرع الثالث: القاضي الجزائي ودوره في تقدير الدليل الإلكتروني وحجته في الإثبات
		الفصل الثاني:

مواجهة الجريمة الإلكترونية وفقا للقانون 04/09

344		المبحث الأول: الإجراءات المستحدثة للوقاية من الجريمة الالكترونية
345		المطلب الأول: المراقبة الإلكترونية كإجراء للوقاية من الجريمة الإلكترونية
345		الفرع الأول: مفهوم المراقبة الإلكترونية
349		الفرع الثاني: حصر حالات اللجوء للمراقبة الإلكترونية
351		الفرع الثالث : الضمانات المقررة لتنفيذ المراقبة الالكترونية وكيفية اجرائها
355		المطلب الثاني : التفتيش في الجريمة الإلكترونية
355		الفرع الأول: مفهوم التفتيش في الجريمة الإلكترونية
356		الفقرة الأولى: مدى خضوع مكونات الحاسب الآلي للتفتيش
360		الفقرة الثانية: تفتيش المنظومة المعلوماتية عن بعد
362		الفرع الثاني: شروط التفتيش في البيئة الرقمية
362		الفقرة الأولى: الشروط الموضوعية
365		الفقرة الثانية: الشروط الشكلية
368		الفرع الثالث: حجز المعطيات المعلومات (الضبط)
368		الفقرة الأولى: مفهوم الضبط
372		الفقرة الثانية: أساليب حجز (ضبط) المعطيات
374		المطلب الثالث: الاستعانة بمزودي الخدمات

375	الفرع الأول: المقصود بمقدم الخدمات الأنترنت.....
379	الفرع الثاني: التزامات مقدمي خدمات الأنترنت.....
382	الفرع الثالث: مسؤولية مقدمي الخدمات.....
385	المطلب الرابع: إنشاء الهيئات والأجهزة الوطنية للوقاية ولمكافحة الجريمة الإلكترونية.....
	الفرع الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال
385	ومكافحتها.....
392	الفرع الثاني: السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي.....
397	الفرع الثالث الأجهزة المتخصصة التابعة للأمن والدرك الوطني.....
397	الفقرة الأولى: الوحدات التابعة للدرك الوطني.....
401	الفقرة الثانية: الهيئات المتخصصة التابعة للأمن الوطني.....
402	المبحث الثاني: التعاون الدولي لمكافحة الجريمة الإلكترونية.....
402	المطلب الأول: المساعدة القضائية المتبادلة كآلية للتعاون الدولي.....
403	الفرع الأول: مفهوم المساعدة القضائية.....
403	الفقرة الأولى: تعريف المساعدة القضائية.....
404	الفقرة الثانية: شروط قبول المساعدة القضائية.....
406	الفقرة الثالثة: القيود الواردة على طلبات المساعدة القضائية الدولية.....
407	الفرع الثاني: صور المساعدة القضائية الدولية.....
412	المطلب الثاني: التعاون الأمني في مجال مكافحة الجريمة الإلكترونية.....
412	الفرع الأول: المنظمة الدولية للشرطة الجنائية (Interpol).....
416	الفرع الثاني: مركز الشرطة الأوروبية (الأوروبول) Europol.....
419	الفرع الثالث: شرطة الأفريبول.....
421	المطلب الثالث: تسليم المجرمين.....
421	الفرع الأول: مفهوم التسليم.....

421	الفقرة الأولى: تعريف نظام تسليم المجرمين ومصادره.....
425	الفرع الثاني: إجراءات التسليم.....
432	الخاتمة.....
438	قائمة المصادر والمراجع.....

ملخص

إن التقدم التكنولوجي المذهل الذي شهدته البشرية في الآونة الأخيرة ،أدى إلى ظهور ما يعرف بالجريمة الإلكترونية ، ذات الطبيعة الخاصة والمعقدة التي تثير العديد من الإشكاليات سواء من ناحية اكتشافها أو صعوبة إثباتها ، وتبعاً لذلك تطلب الأمر جهود لمكافحتها .

لقد واكب المشرع الجزائري التشريعات الدولية في مواجهة الجريمة الإلكترونية، و ذلك بانتهاج سياسة جنائية متكاملة، من خلا إرساء تدابير مستحدثة، فمن الناحية الموضوعية سن قواعد قانونية متضمنة التجريم والعقاب خاصة في مجال المساس بأنظمة المعالجة الآلية للمعطيات، الحق في الخصوصية ،استغلال الأطفال في الإباحية ...إلخ، باعتبار عدم كفاية الإجراءات التقليدية في مكافحة الجريمة الإلكترونية بادر المشرع بإقرار إجراءات مستحدثة ملائمة لكشف خبايا هذه الجريمة، بعد التعديلات الماسة بقانون الإجراءات الجزائية كإجراء أساليب التحري الخاصة، إنشاء قطب جزائي متخصص، و نتيجة لخطورة هذه الجريمة أصدر قانون يختص بالوقاية منها قبل وقوعها و يتمثل في القانون 09-04 المتعلق بالقواعد الخاصة للوقاية الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وأقر المراقبة الإلكترونية والتفتيش عن بعد، وإنشاء هيئة وطنية مختصة بمكافحتها و الوقاية منها.

الكلمات المفتاحية: الجريمة الإلكترونية، السياسة الجنائية، المشرع الجزائري ، التجريم والعقاب ، إجراءات مستحدثة، الهيئة الوطنية.

Résumé

Les progrès technologiques stupéfiants que l'humanité a connus ces derniers temps ont conduit à l'émergence de ce qu'on appelle la criminalité électronique, qui est d'une nature particulière et complexe, posant de nombreux problèmes tant au niveau de la détection que de la difficulté à la prouver, d'où la nécessité de déployer des efforts pour la combattre. Le législateur algérien s'est mis au diapason de la législation internationale en matière de cybercriminalité en adoptant une politique pénale intégrée à travers l'adoption de mesures innovantes et la mise en place objective de dispositions légales incluant l'incrimination et la répression, notamment en matière d'atteinte aux systèmes de traitement automatisé des données et au droit à la vie privée, pornographie infantile ...etc., compte tenu de l'incrimination et de l'inadéquation des procédures traditionnelles dans la lutte contre la cybercriminalité, le législateur a pris l'initiative d'adopter de nouvelles procédures appropriées pour découvrir les secrets de ce crime, après modifications apportées au code de procédure pénale, telles que la mise en œuvre de méthodes d'enquête spéciales, la création d'un pôle pénal spécialisé, et en raison de la gravité de ce crime, une loi a été publiée pour sa prévention avant qu'il ne se produise, représentée dans la loi 09-04 sur les règles spéciales pour la prévention et la lutte contre les crimes liés aux technologies de l'information et de la communication, l'ordre de surveillance électronique et d'inspection à distance, et la création d'un environnement national spécialisé dans la lutte et la prévention.

Mots-clés: cybercriminalité, politique pénale, législateur algérien, incrimination et répression, prévention, nouvelles mesures, autorité nationale.

Abstract

The astounding technological progress that humanity has witnessed in recent times has led to the emergence of what is known as electronic crime , wich is of a particular and complex nature , posing many problems both in terms of detection and difficulty in provin git, and therefore efforts have been required to combat it.The Algerian legislator has kept pace with international legislation on cybercrime by adopting an integrated criminal policy through the adoption of innovative measures and the objective enactment of legal provisions that include criminalization and punishment , particularly in the area of the violation of automated data processing systems and the right to privacy .Child pornography ...etc, In viw of the inadequacy of traditional produres in combating cybercrime, the legislator took the initiative to adopt appropriate new procedures to uncover the secrets of this crime , after the amendments to the code of criminal procedure , such as the implementation of special investigate methods ,the establishment of a specializedpenal pole , and as result of the seriousness of this crime , A law has been issued for its prevention before it occurs , represented in the law 09-04 on special rules for the prevention and combating of crimes related to informtion and communication technology, the order of electronic surveillance and remote inspection, and the establishment of a national environment specialized in combating and preventing them.

Keywords:cubercrime, criminal policy, Algerian legilator, criminalization and punishment , prevention, new measures, national authority.

قائمة المختصرات

اولا باللغة العربية

ص : صفحة

د.س.ن : دون سنة النشر

د.م.ن : دون مدينة النشر

د.ط : دون طبعة

ق.ع.ج : قانون العقوبات الجزائري

ق.إ.ج.ج : قانون الإجراءات الجزائية الجزائري

ق.ع.ف : قانون العقوبات الفرنسي

ثانيا باللغة الأجنبية

P:page

Ed: édition

N: numéro

Art: article

Rev: revue

Vol:volume

Op.cit.:ouvrage précité

Ibid.: le même ouvrage

c.p.f: code pénale français

c.p.p.f:code procédure pénale français

مقدمة

مقدمة

تطورت الجريمة بتطور نمط حياة الإنسان ولقد بلغ هذا التطور أوجه بظهور المجتمعات بمفهومها المعاصر، حيث أن المجتمعات أصبحت تعيش الكثير من التراكبات، ما نتج عنها وقوع الكثير من الجرائم، وأصبح الفرد يسعى بشتى الطرق للوصول إلى إشباع رغباته الشخصية حتى ولو وصل به الأمر إلى ارتكاب العديد من الجرائم تكون نتائجها وخيمة على الأفراد بصفة خاصة وعلى المجتمع بصفة عامة.

ومع التطور الذي يشهده هذا العصر بظهور ثورة جديدة، والتي يطلق عليها ثورة المعلومات التي ظهرت نتيجة اندماج وسيلتين هما تقنية المعلومات ووسيلة الاتصالات، فإختراع الحاسب الآلي الذي لعب دورا كبيرا في عملية تخزين المعلومات والسرعة في معالجتها، وكذلك ظهور شبكة الأنترنت كوسيلة للاتصال حيث حولت العالم الى قرية صغيرة، ربطت بين الشعوب فأصبح الإنسان يستطيع أن يرصد ما يجري على الطرف الآخر من العالم بالصوت والصورة في لحظة قيام الحدث، أصبحت عملية تبادل المعلومات، والاتصال سهلة وتتم في وقت قصير وعلى نطاق واسع، لكن رغم الإيجابيات التي حققتها الثورة المعلوماتية، إلا أنها في المقابل عرفت العديد من الإنعكاسات الخطيرة، نتيجة سوء استخدام هذه التقنيات المتطورة، مما أدى إلى إنتشار ظاهرة خطيرة، على المجتمعات وعلى أمنها وإستقرارها وهو ما يعرف بالجريمة الإلكترونية، حيث صنف هذه الجريمة من أخطر الجرائم المعاصرة لما تشكله من مخاطر تمس الجوانب الاقتصادية والاجتماعية والأمنية، ومن جهة أخرى جلبت هذه الجريمة نوعا جديدا من المجرمين، الذي يتميز بالذكاء والخبرة والكفاءة، يرتكب جرائمه بضغطة زر على الحاسب الآلي دون اللجوء إلى العنف، حتى عرفت جرائمه بالجرائم الناعمة، فهذه الجرائم تدور وقائعها في العالم الافتراضي، لا ترى بالعين المجردة لوقوعها على أشياء غير ملموسة، لها طابع معنوي تتمثل في المعلومات والبيانات والبرامج، مما نتج عن ذلك صعوبات في اكتشاف وإثبات هذا النوع من الجرائم، لعدم قدرة النظم القانونية التقليدية من مكافحة هذا النوع من الإجرام، فانعكس ذلك سلبا على السياسة الجنائية، ما جعل الدول المتقدمة تدرك خطورة هذه الجرائم، فسارعت إلى عقد المؤتمرات وإبرام الإتفاقيات الدولية ولعل أهمها إتفاقية بودابست¹ والتي جاءت لهدف واحد وهو مكافحة الجريمة الإلكترونية، دعت دول العالم بانتهاج

¹ - أبرمت هذه الإتفاقية في 23 نوفمبر 2001 وذلك تحت إشراف المجلس الأوروبي رغم أن، هذه الاتفاقية أوروبية المنشأ إلا أنها دولية النزعة وذلك لأنها فتحت باب التوقيع والتصديق والقبول والإقرار والانضمام أمام جميع الدول.

سياسة جنائية مشتركة فيما بينها في مجال مجابهة هذه الجريمة، التي تتميز بطبيعة خاصة معقدة وباعتبارها عابرة للحدود الوطنية، وبفضل هذه الإتفاقية وما إحتوته من إجراءات فعالة، جعلت الدول تسن تشريعات جزائية للحد من مخاطر هذه الجريمة، ولردع مرتكبيها والعمل على الاستمرار لتطوير هذه التشريعات بالشكل الذي يواكب تطور الجريمة.

ولم يتأخر المشرع الجزائري عن مواكبة التشريعات الدولية في هذا المجال، فكانت مواجهة الجريمة الإلكترونية إحدى بنود إتفاق يؤسس لشراكة بين الجزائر والإتحاد الأوروبي، عقد بتاريخ 22 أفريل 2002 وتضمنت ذلك المادة 86¹، حيث خطا المشرع خطوات كبيرة لمواكبة التشريعات الدولية في هذا الصدد، فكانت أولى بؤادر تكييف المنظومة التشريعية مع التطورات الحاصلة في مجال مكافحة الجريمة الإلكترونية، صدور القانون رقم 01-09 المؤرخ في 26/06/2001² المتعلق بجريمة القذف والسب والإهانة ضد رئيس الجمهورية، وفيما يخص دين الإسلامي والرسول أين إستعمل مصطلح وسيلة إلكترونية أو معلوماتية، ثم تلاه القانون رقم 04-15 المؤرخ في 11/10/2004

³المتضمن قانون العقوبات والذي تم بموجبه إستحداث الفصل السابع مكرر تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات تضمن ثمانية مواد جديدة، تتعلق بالإعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات .

بعدها صدر القانون 06-22 المؤرخ في 20/12/2006 المتضمن تعديل قانون الإجراءات الجزائية

¹ - Art 86 prévention et lutte contre la criminalité organisée

1-les parties conviennent de coopérer afin de prévenir et de combattre la criminalité organisée ,notamment dans les domaine du trafic de personne ;de l'exploitation à fin des sexuelles, du trafic illicite de produits prohibés, contrefais ou piratés et de transactions illégales concernant notamment les déchets industriels ou du matériel radioactifs ,de la corruption, du trafic de voitures volées, du trafic d'armes feu et des explosifs, de la criminalité informatique ,et du trafic de biens culturels.

Les parties coopéreront étroitement afin de mettre en place les dispositifs et les normes appropriés

2-la coopération technique et administrative dans ce domaine pourra inclure la formation ,et le renforcement de l'efficacité des autorités et de structures chargées de combattre et de prévenir la criminalité et la formulation de mesures de prévention du crime.

²-القانون رقم 01-09 المؤرخ في 26/06/2001 يعدل ويتم الأمر رقم 66-156 المتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، عدد 34 الصادرة بتاريخ 27/06/2001.

³- القانون رقم 04-15 المؤرخ في 10/11/2004 العدل والمتمم للأمر رقم 66-56 المتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، عدد 71، الصادرة بتاريخ 10/11/2004.

الذي جاء بقواعد إجرائية خاصة بالبحث والتحري عن بعض الجرائم المستحدثة، ومنها الجريمة الإلكترونية والتي أصبحت ضرورية في الوقت الراهن، حتى تتمكن الشرطة القضائية من مواجهة الإجرام الخطير الذي أفرزه التطور التكنولوجي والعلمي، ونظرا لطبيعة الجريمة نص المشرع على القانون 04-09¹ المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، هدفه تعزيز الحماية الجزائية للأنظمة المعلوماتية، ووضع إطار قانوني أكثر ملاءمة للتصدي للإجرام المعلوماتي، ثم قام المشرع بإنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها بموجب المرسوم الرئاسي رقم 15-261 المؤرخ في 08/11/2015، المعدل بالمرسوم الرئاسي 20-183 المؤرخ في 13/07/2020، الذي يعيد تنظيم الهيئة الوطنية²، ثم مرة أخرى قام بتعديل قانون العقوبات بالقانون رقم 16-06 المؤرخ في 19/06/2016³، فأدرج المادتين 87 مكرر 11 و 87 مكرر 12 جرم من خلالهما أفعال، تعد خطيرة تتمثل في التجنيد والسفر بغرض ارتكاب أفعال إرهابية باستخدام تكنولوجيا الإعلام والاتصال، لم يكتف المشرع بهذا القدر بل واصل سياسته الجنائية بسن قوانين خاصة في مجال مكافحة هذه الجريمة، فأصدر القانون 18-04 المتضمن تحديد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية⁴، والقانون 15-04 الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكتروني⁵ والقانون 18/05/2018 المؤرخ في 10/05/2018 المتعلق بالتجارة الإلكترونية، والقانون 18/07/2018 المؤرخ في 10/06/2018 المتعلق بحماية الأشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي، ولخطورة هذه الجرائم وتكملة للجهود المبذولة، أنشأ المشرع قطبا جزائيا وطنيا يختص بمكافحتها بموجب الأمر 21-11 المؤرخ في 25/08/2021 بعدما كانت تنتظر أمام الأقطاب

¹ - القانون 04-09 المؤرخ في 08/05/2009 المتضمن القواعد الخاصة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، عدد 47، الصادرة بتاريخ 16/08/2009.

² - المرسوم الرئاسي رقم 20-183 المؤرخ في 13/07/2020 يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية ن عدد 40 الصادرة بتاريخ 18/07/2020.

³ - القانون رقم 16-02 المؤرخ في 19/06/2016 يعدل ويتم الأمر 66/156 المتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، عدد 37 الصادرة بتاريخ 22/06/2016.

⁴ - القانون رقم 18-04 المؤرخ في 10/05/2018 يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، الجريدة الرسمية للجمهورية الجزائرية، عدد 27، الصادرة بتاريخ 13/05/2018.

⁵ - القانون رقم 15-04 المؤرخ في 01/02/2015 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، الجريدة الرسمية للجمهورية الجزائرية، عدد 06، الصادرة بتاريخ 10/02/2015.

الجزائية المتخصصة، ولم يكتف المشرع بهذا ولإنجاح سياسته، أبرم العديد من الإتفاقيات منها الإتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 21 ديسمبر 2010، والتي تهدف إلى تعزيز التعاون بين الدول العربية في مجال مكافحة الجرائم الإلكترونية.

ومن خلال هذا، تظهر أهمية الموضوع في كونه موضوعا يعالج نمطا جديدا من الجرائم لم تكن معروفة من قبل، تسمى الجرائم الإلكترونية، بالإضافة أن هذه الأخيرة مرتبطة بتكنولوجيا متطورة هي تكنولوجيا الحاسبات الآلية وشبكة الأنترنت، مما أسفر عن تمييزها بمجموعة من الخصائص تختلف عن غيرها من الجرائم، مما يستتبع ضرورة التعامل معها بما يتلاءم مع هذه الخصوصية، وما يزيد في أهمية الموضوع أن هذه الجريمة عابرة للحدود ما يجعلها تثير العديد من الإشكاليات القانونية.

ومن جهة أخرى ظهور نوع جديد من المجرمين يستخدمون التقنية في ارتكاب جرائمهم الخطيرة على المجتمع وبأسماء مستعارة وسمتهم الذكاء، وحتى المجني عليه يلعب دورا كبيرا في تفشيها، عن طريق إحجامه عن التبليغ مما يزيد في إنتشار هذا النوع من الجرائم، مآدى إلى صعوبة إكتشافها وإثباتها من طرف السلطات القضائية المختصة، كما أن هذه الجرائم لا يزال يكتنفها غموض في نواحي عديدة، خاصة من الناحية القانونية لوجود العديد من المشكلات القانونية، وبروز ظاهرة الفراغ التشريعي والذي خلق ضرورة حتمية لتدخل المشرع للتصدي لهذه الأنماط المستحدثة من الإجرام ، لذا فإن أهمية موضوع هذا البحث يعد موضوعا مستجدا ومستحدثا لدراسته، و لمواجهة هذه الظاهرة يجب إتباع سياسة جنائية من خلال تكريس القواعد القانونية الجنائية الكفيلة بمواجهتها، إماعن طريق تطوير القواعد التقليدية، أو وضع قواعد مستحدثة تواجه المشكلات التي أسفر عنها التطور التكنولوجي.

ومن خلال البحث و الدراسة في موضوع السياسة الجنائية لمكافحة الجريمة الإلكترونية في التشريع الجزائري نتوخى الأهداف الآتية والتي تتمثل أساسا في :

-تبيان الطبيعة الخاصة للجريمة الإلكترونية.

-محاولة معرفة الآليات التي وضعها المشرع الجزائري لمواجهة هذه الجريمة سواء على مستوى التجريم والعقاب أو الإجراءات.

-كيفية مواجهة الجريمة الإلكترونية بأساليب تتوافق مع طبيعتها الخاصة و المعقدة و موقف المشرع منها.

عرض أهم الجهود الوطنية والدولية المبذولة في مجال مكافحة الجريمة الإلكترونية.

-الخروج بإقتراحات تحد من أضرار الجريمة الإلكترونية.

و من الأسباب التي دفعتنا الى إختيار هذا الموضوع الرغبة الحثيثة لمعرفة هذه الظاهرة المستجدة من الجرائم التي تعتمد على وسائل التكنولوجيا الحديثة لارتكابها، وانتشارها بسرعة فائقة في كافة أنحاء العالم، فلم تعد الحدود الجغرافية ولا بعد المسافات عائقا أمام مرتكبيها، وكذلك الصبغة العلمية التي تتصف بها فمصطلحاتها غريبة على رجال القانون، مما يجعلنا نرغب في التعمق في دراسة موضوع الجرائم الإلكترونية، ومن الأسباب كذلك التي أدت بنا الى إختيار هذا الموضوع معرفة كيفية مواجهة المشرع الجزائري لهذه الجريمة سواء من الناحية الموضوعية أو الإجرائية، خاصة بعد تفشي الجرائم الإلكترونية في المجتمع الجزائري، ومن جانب آخر يعتبر من المواضيع الجديدة التي لم تتناول بكثرة من طرف الباحثين، وإن وجدت تهتم وتركز على الجانب الموضوعي.

ومن هذا المنطلق يمكن تحديد الإشكالية المتعلقة ببحثنا فهدف كل سياسة جنائية، هو محاربة السلوكيات الإجرامية والسعي إلى الحد من تطور الجريمة، وتزايد حماية للحقوق الفردية والجماعية، هذا يكون بإتباع الوسائل الكفيلة بضمان هذه الأهداف، فالإشكالية التي يعالجها البحث وتتمثل في إلى أي مدى تمكن المشرع الجزائري من توفير إطار قانوني يمكن من خلاله رسم سياسة جنائية فعالة وناجحة للتصدي للجريمة الإلكترونية ؟

ويندرج عن هذه الإشكالية عدة تساؤلات تتمثل في:

- ماهي الجريمة الإلكترونية ؟ وماهي خصائصها وطبيعتها القانونية ؟

- ماهي صور الجرائم المنصوص عليها في التشريع الجزائري ؟

- هل ركز المشرع في سياسته على سياسة الردع، أو الوقاية، أو على الجانب الإجرائي ؟

- هل تلعب الهيئات والأجهزة المتخصصة دور فعال في مكافحة الجريمة الإلكترونية ؟

- هل للتعاون الدولي الدور الفعال في مكافحة الجريمة الإلكترونية ؟

ولهذا اعتمدنا في هذا البحث على المنهج التحليلي، كمنهج أساسي وذلك باستقراء النصوص القانونية بالجرائم الإلكترونية وتحليلها، من خلال البحث في جزئيات مشكلة موضوع البحث وشرح

كل جريمة على حدة، وكذا الجوانب الإجرائية التي تحكم هذا النوع من الجرائم، لمعرفة مدى كفاية النصوص القانونية لمواجهتها والحد منها، وذلك دون الإستغناء عن المنهج الوصفي لوصف الظاهرة الإجرامية، دون أن ننسى المنهج التاريخي و المنهج المقارن إذا إقتضت الضرورة ذلك.

وقد وجهتنا أثناء القيام بهذا البحث العديد من الصعوبات، أهمها الطبيعة الفنية و التقنية للموضوع، فارتباط محل الدراسة بالحاسب الآلي يتطلب الإحاطة بمكونات هذا الأخير، و بنظام المعالجة الآلية للمعطيات و الشبكات و كل ما يتعلق بهذه الجريمة، إلى جانب الإلمام بالنصوص القانونية و هذا يحتاج إلى جهد فني فضلا عن الجهد القانوني، ومن الصعوبات أيضا حداثة الموضوع مما أدى إلى نقص لبعض المراجع خاصة في الجانب الإجرائي، كذلك بالنسبة للأحكام القضائية تكاد تكون منعدمة و لم نتمكن من الحصول عليها.

وقد عاجت العديد من رسائل الدكتوراه موضوع الجريمة الإلكترونية منها:

-رسالة دكتوراه بعنوان جرائم الأنترنت دراسة مقارنة للباحثة نبيلة هبة هروال صادرة عن كلية الحقوق والعلوم السياسية بجامعة أبو بكر بلقايد، للسنة الجامعية 2013-2014، تناولت مختلف الجرائم كجرائم الإعتداء على الأشخاص عبر الأنترنت في (الباب الأول) وجرائم الإعتداء على الأموال عبر الأنترنت في (الباب الثاني) وجرائم العدوان على أمن الدولة عبر الأنترنت في (الباب الثالث) فركزت في دراستها على الجوانب الموضوعية للجريمة الإلكترونية دون الجانب الاجرائي .

-رسالة دكتوراه بعنوان آليات إثبات الجريمة المعلوماتية في التشريع الجزائري -دراسة مقارنة للباحث عبد القادر عمير صادرة عن كلية الحقوق لجامعة الجزائر 01، للسنة الجامعية 2019-2020، تناول فيها أهم التحديات التي تثيرها مسألة إثبات الجريمة الالكترونية، وكيفية تعامل المشرع معها .

-رسالة دكتوراه بعنوان الجرائم العابرة للحدود المرتكبة بتقنية الأنترنت للباحثة أمينة علالي، صادرة عن كلية الحقوق والعلوم السياسية بجامعة باجي مختار، للسنة الجامعية 2018، تناولت هذه الأطروحة دراسة الجرائم التقليدية التي أصبحت ترتكب بواسطة شبكة الأنترنت وهي الجرائم العابرة للأوطان، فتناولت في (الباب الأول) الإجرام العابر للحدود عبر الأنترنت، أما فيما يخص الباب الثاني تطرقت إلى الجهود الوطنية والدولية لمكافحة الجرائم العابرة للحدود عبر الأنترنت .فهذه الدراسات تختلف عن دراسة موضوعي والمتمثل في سياسة المشرع الجزائري في مكافحة الجريمة الالكترونية.

وقصد إعطاء صورة واضحة عن أبعاد السياسة الجنائية للمشرع الجزائري بخصوص مكافحة الجرائم الإلكترونية وما يثير ذلك من إشكالات في الجانبين الموضوعي والإجرائي، ارتأينا تقسيم بحثنا إلى بابين

-الباب الأول: الجوانب الموضوعية لمكافحة الجريمة الإلكترونية.

الفصل الأول: الإطار المفاهيمي للجريمة الإلكترونية .

الفصل الثاني: المواجهة التشريعية للجريمة الإلكترونية .

-الباب الثاني:الجوانب الإجرائية لمكافحة الجريمة الإلكترونية .

الفصل الأول: مواجهة الجريمة الإلكترونية وفقا لقانون الإجراءات الجزائية .

الفصل الثاني:مواجهة الجريمة الإلكترونية وفقا للقانون 04-09.

وانهينا بحثنا بخاتمة تتضمن أهم النتائج والتوصيات المقترحة.

الباب الأول

الجوانب الموضوعية

لمكافحة الجريمة الالكترونية

الباب الأول: الجوانب الموضوعية لمكافحة الجريمة الإلكترونية

عرفت البشرية في نهاية القرن العشرين اتساعا وتزايدا كبيرا لنطاق استخدام تقنية المعلوماتية في المجتمع، ونظرا للتطور السريع لهذه التقنية فقد تعددت استعمالاتها وفي جميع المجالات سواء الاقتصادية، الاجتماعية والسياسية والثقافية، رغم الإيجابيات التي أفرزتها هذه التقنية، إلا أنها من جانب آخر كان لها آثار سلبية منها أنها أفرزت نوعا جديدا من الجرائم سمي بالجرائم الإلكترونية، التي تمثل خطرا على أمن الدول وعلى حق الأفراد في الحياة الخاصة أو على حقهم في الخصوصية المعلوماتية، ذلك لكونها جريمة ذات طابع خاص تختلف عن الجرائم التقليدية، ونظرا لجسامة أخطارها وفداحة خسائرها وسرعة انتشارها أصبحت لها اهتمام بالغ من قبل الدول، زيادة على ذلك خلق هذا النوع المستحدث من الجرائم صعوبات بالغة سواء على مستوى التجريم أو العقاب أو على مستوى الإجراءات المتعلقة بالبحث والتحري عنها، والجزائر كباقي الدول لم تسلم من خطر الجريمة الإلكترونية، وهذا بعد الإنتشار الواسع لاستعمال وسائل التكنولوجيا الحديثة، من حواسيب وهواتف محمولة، وازدياد عدد مستعملي شبكة الأنترنت، أدرك المشرع الجزائري ضرورة التصدي لها عن طريق القيام بتعديلات مختلفة سواء من خلال تعديل قانون العقوبات، أو بواسطة سن تشريعات تجرم الأفعال غير المشروعة في نصوص قانونية خاصة، لذلك ارتأينا أن نقسم هذا الباب إلى قسمين، نلقي من خلاله الضوء على ماهية الجرائم الإلكترونية في (الفصل الأول) ثم نتطرق إلى أهم الجرائم التي تمثل مجمل النصوص القانونية المتعلقة بمواجهة الجريمة الإلكترونية سواء الواردة في قانون العقوبات أو الجرائم تضمنتها نصوص خاصة في (الفصل الثاني).

الفصل الأول: الإطار المفاهيمي للجريمة الإلكترونية

شهد العالم تقدما تكنولوجيا لم يسبق له مثيل وقد نتج عن ذلك ظهور وسائل اتصال متطورة، جعلت العالم قرية صغيرة مفتوحة تلاشت معها الحدود الجغرافية والسياسية للدول، ولقد أدى الاستخدام السيء لهذه الوسائل إلى ظهور الجرائم الإلكترونية التي تتميز بطبيعة خاصة ومعقدة، وارتكابها في عالم افتراضي غير ملموس وبأساليب غير معهودة تعتمد على التقنية العالية كالحواسيب والهواتف النقالة كما جلبت نمودجا مستحدثا من المجرمين يتميزون بالذكاء والفتنة والخبرة، لم تسلم جميع الدول من الأفعال المرتكبة من طرفهم، فجرائمهم التي تخلف أضرار جسيمة في جميع النواحي منها الإقتصادية والإجتماعية، العسكرية والسياسية، مما أدى إلى تضافر الجهود الدولية للتصدي لهم عن طريق محاولة ايجاد سن تشريعات تجرم هذا النوع المستجد من الجرائم، ولم يتخلف المشرع الجزائري عن مواجهتها عن طريق استحداث نصوص قانونية من أجل مكافحتها و الوقاية منها.

و هذا الفصل قمنا بتقسيمه إلى مبحثين تناولنا في (المبحث الأول) ماهية الجريمة الإلكترونية، فيما خصصنا (المبحث الثاني) والذي جاء تحت عنوان المرجعيات المؤطرة للجريمة الإلكترونية وتأثر الجزائر بها.

المبحث الأول: ماهية الجريمة الإلكترونية

تعتبر الجرائم الإلكترونية من أخطر وأحدث جرائم العصر، وذلك لارتباطها بتكنولوجيا متطورة ألا وهي تكنولوجيا المعلومات، مما أكسبها طبيعة خاصة ومعقدة بسبب البيئة التي ترتكب فيها الجريمة وهو العالم الافتراضي، وحدثة طرق وأساليب ارتكابها ووسائل كشفها وتميز مرتكبيها، ونتيجة لحدثة هذه الجريمة واعتبارها ظاهرة إجرامية حديثة طرحت العديد من التساؤلات، وأثيرت عدة مسائل في مجال القانون الجنائي.

وعليه قسمنا مبحثنا من خلال محاولة إعطاء مفهوم للجريمة الإلكترونية (المطلب الأول) ثم التطرق للبنيان القانوني لها (المطلب الثاني) ودراسة طرفي الجريمة (المطلب الثالث) وفي الأخير تناول مبررات الحماية في (مطلب رابع).

المطلب الأول: مفهوم الجريمة الإلكترونية

قبل التطرق إلى تعريف الجريمة الإلكترونية، لابد أن نشير إلى أنه لا يوجد مصطلح قانوني موحد للدلالة على الجرائم الناشئة عن استغلال تقنية المعلومات واستخدامها، ففي بدايات هذا النوع من الجرائم أطلق عليها مصطلح "إساءة استخدام الكمبيوتر" ثم "احتياال الكمبيوتر"¹ ف"الجريمة المعلوماتية"² بعدها "جرائم الكمبيوتر"³ ثم جرائم التقنية العالية"⁴ إلى "جرائم الأنترنت" و"الجريمة الإلكترونية" وأخيرا "السيبيركرايم"⁵، إن عدم الاتفاق على مصطلح معين نتج عنه عدم وضع تعريف موحد لهذه الظاهرة الإجرامية وذلك خشية حصرها في مجال ضيق يمكن أن يضر بها⁶.

الفرع الأول: تعريف الجريمة الإلكترونية

اشتقت كلمة "الجريمة" في اللغة من الجرم وهي التعدي، أو الذنب وجمع الكلمة إجرام وجرم وهو الجريمة، وقيل جرم يجرم واجترام وأجرم فهو مجرم وجرم⁷.

¹ - أصبح هذا المصطلح لا يلائم هذا النوع من الجرائم، ذلك أن الاحتيال هو الآن أحد أنواع هذه الجرائم أو صورة من صورها وليس مصطلح يطلق على الظاهرة ككل. انظر نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية- دراسة تطبيقية ونظرية -منشورات الحلبي الحقوقية، لبنان، ط1، 2005، ص27.

² - استعمل مصطلح الجريمة المعلوماتية من طرف الفقه الفرنسي بوصفها ترجمة لمصطلح "informatique" بمعنى المعالجة الآلية للبيانات، استخدم في وصف الظاهرة الإجرامية المستحدثة وتبعاً لذلك أطلقت تعبيرات الجرائم المعلوماتية ومحلها المال المعلوماتي، وأصبح هذا المصطلح فرع مستقل من فروع المعرفة وعلومها ويتصل بقواعد البيانات بوجه عام، أنظر في ذلك يونس عرب، جرائم الكمبيوتر والأنترنت، ورقة مقدمة لمؤتمر الأمن العربي، المنعقد يومي 2002/02/12-10، المركز العربي للدراسات والبحوث الجنائية، ص2.

³ - جرائم الكمبيوتر والذي يشير لتعريف أية أنشطة إجرامية ترتكب ضد الحاسب الآلي أو جهاز مشابه، أو البرنامج أو البيانات في داخله، أي أن الحاسب يكون فيها الهدف للنشاط الإجرامي.

⁴ - تعتبر هذه التسمية واسعة ومطلقة بحيث تشمل الكثير من الأجهزة التي لا ترتبط مع الهدف المقصود من التسمية، زيادة على ذلك هناك الكثير من الأجهزة التقنية يمكن أن تستخدم لارتكاب الجريمة وبالتالي الخلط بين مفهوم الظاهرة التي نحن بصدد دراستها وبين هذه الجرائم التي ترتكب بواسطة الأجهزة التقنية في مجال الطب وغيرها، أنظر مشتاق طالب وهيب، مفهوم الجريمة الإلكترونية ودور الحاسب في ارتكابها، مجلة العلوم القانونية والسياسية كلية القانون والعلوم السياسية، جامعة دالي، العراق، المجلد الثالث، العدد الأول، 2014، ص336.

⁵ - وهو المصطلح الذي تعتمده الدول الغربية كفرنسا وإنجلترا والولايات المتحدة الأمريكية... وغيرها.

⁶ - محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، دط، 2004، ص43.

⁷ - ابن منظور، لسان العرب، الجزء12، دا صادر، بيروت، ط3، 1994، ص91.

أما الجريمة الإلكترونية فهي التي تدخل مادة الإلكترونيات في أدق العمليات الحسابية وبأسرع وقت ممكن، وهو فرع من فروع الفيزياء.¹

وتتكون الجريمة الإلكترونية من مقطعين هما "الجريمة" و"الإلكترونية" ويستخدم مصطلح الجريمة الإلكترونية لوصف فكرة جزء من الحاسب أو عصر المعلومات²، أما الجريمة فتعرف بأنها "سلوك الفرد عملاً كان أو امتناعاً يواجهه المجتمع عموماً بتطبيق عقوبة جزائية، وذلك بسبب الاضطرابات التي يحدثها في النظام الاجتماعي"³، كما تعرف أيضاً الجريمة في نطاق القانون الجنائي "بأنها فعل غير مشروع صادر عن إرادة جنائية يقرر له القانون عقوبة أو تدبيراً احترازياً"⁴، والجرائم الإلكترونية هي المخالفات التي ترتكب ضد الأفراد أو المجموعات من الأفراد بدافع الجريمة ويقصد إيذاء سمعة الضحية أو أذى مادي أو عقلي للضحية مباشرة أو غير مباشر باستخدام شبكات الاتصالات مثل الأنترنت، غرف الدردشة، والبريد الإلكتروني⁵.

ولقد تعددت التعاريف التي قبلت بشأن الجريمة الإلكترونية وتباينت فيما بينها ضيقاً واتساعاً، مما تعذر إيجاد مفهوم للجريمة الإلكترونية حتى قيل أن الجريمة الإلكترونية تقاوم التعريف⁶، وهذا ما يصعب على وضع تعريف جامع ومانع للجريمة الإلكترونية، وللوقوف على إعطاء تعريف للجريمة الإلكترونية يقتضي منا الحال التعرض إلى التعريف الفقهي لهذه الجريمة (الفقرة الأولى) ومن ثم تبين التعريف القانوني (الفقرة الثانية).

الفقرة الأولى: تعريف الجريمة الإلكترونية فقهاً

اختلف الفقهاء اختلافاً كبيراً حول تعريف الجريمة الإلكترونية، حيث انقسم الفقهاء في تعريف هذه

¹ - عمر طه خليل، عفاف بديع جميل، التكييف الفقهي والقانوني لجرائم الأنترنت، مجلة كلية التراث الجامعة، العدد السابع عشر، د.س.ن، ص 165.

² - نياض موسى البدانية، الجرائم الإلكترونية المفهوم والأسباب، ورقة علمية مقدمة في إطار الملتقى العلمي، الجرائم المستحدثة في ظل التغيرات والتحولات الإقليمية والدولية، المنعقد خلال الفترة من 2-4 سبتمبر 2014، كلية العلوم الاستراتيجية، الأردن، ص 3.

³ - أحسن بو سقيعة، الوجيز في القانون الجزائري العام، دار هومة، الجزائر، ط 3، 2006، ص 3.

⁴ - محمد نجيب حسني، شرح قانون العقوبات - القسم العام -، دار النهضة العربية، القاهرة، ط 6، 1989، ص 40.

⁵ - نياض موسى البدانية، المرجع السابق، ص 3.

⁶ - أيمن عبد الله فكري، جرائم نظم المعلومات -دراسة مقارنة-، دار الجامعة الجديدة، الإسكندرية، د ط، 2007، ص 29.

الظاهرة إلى عدة اتجاهات تقوم على أسس مختلفة.

أولاً: تعريفات تركز حول وسيلة الجريمة

تعتمد هذه التعريفات على وسيلة ارتكاب الجريمة، فطالما كان الحاسب الآلي أو إحدى وسائل التقنية من وسائل ارتكابها حتى تعتبر من الجرائم الإلكترونية، ومن أنصار هذا الاتجاه الفقيه الألماني Laus Tiedemann و Leslie De Ball، إذ يعرف الأول الجريمة الإلكترونية على أنها "كل أشكال السلوك غير المشروع - أو الضار بالمجتمع الذي يرتكب باستخدام الحاسوب". أما الأستاذ Leslie فقد عرفها على أنها "فعل إجرامي يستخدم الحاسب الآلي في ارتكابه كأداة رئيسية وأنها الفعل الإجرامي الذي يستخدم في اقترافه الحاسب الآلي كأداة رئيسية".¹

كما أورد ثوم فريستر في مؤلفه "قصة ثورة تقنية المعلومات" تعريفاً يكاد يكون مطابقاً للتعريف السابق بقوله "أنها فعل إجرامي يتم باستخدام الحاسوب كأداة رئيسية".²

وعرفها أيضاً مكتب تقييم التقنية في الولايات المتحدة الأمريكية بأنها "الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دوراً رئيساً".³

تعرض هذا الاتجاه إلى الانتقاد خاصة التعريف الذي جاء به الفقيه tiedemann الذي يعاب عليه أنه بالغ العمومية والإتساع⁴، ' لأنه يدخل فيه كل سلوك غير مشروع أو ضار بالمجتمع كما أن مجرد استخدام الحاسب الآلي لا يضيف إلى السلوك غير المشروع جديداً، مادام أن استخدام البيانات والمعلومات والبرامج هو الذي يميز الجريمة الإلكترونية.

إذن فأساس الانتقاد الموجه إلى هذا التصنيف أن تعريفه ليس جامعاً ولا مانعاً كما أنها تتسم بقصور كبير في إعطاء تصور علمي للجرائم الإلكترونية.⁵

¹ - سميرة معاشي، الجريمة المعلوماتية دراسة تحليلية لمفهوم الجريمة المعلوماتية، مجلة المفكر، العدد السابع عشر، جوان 2018، ص402.

² - محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة، عمان، د ط، 2005، ص15.

³ - أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، الاسكندرية، د ط، 2005، ص94.

⁴ - محمد علي العريان، المرجع السابق، ص44.

⁵ - سميرة معاشي، المرجع السابق، ص403.

ثانيا: التعريفات المرتكزة حول موضوع الجريمة

يستند أنصار هذا الاتجاه في تعريفهم للجريمة الإلكترونية إلى وجوب أن الحاسب الآلي هو محل الجريمة، فيجب أن يتم الاعتداء على الحاسب الآلي أو على نظامه، ويمثل أنصار هذا الاتجاه الفقيه روز نبلات Rosenblatt الذي عرف الجريمة الإلكترونية بأنها "تشاط غير موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلي أو التي تحول عن طريقه"¹، أو هي حسب تعريف الدكتورة هدى قشقوش بأنها "كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات"،² كما تعرف الجريمة الإلكترونية على أساس موضوع الجريمة بأنها "كل سلوك إيجابي أو سلبي يتم بموجبه الاعتداء على البرامج أو المعلومات للاستفادة منها بأية صورة كانت".³

وهذا المعيار لم يسلم من الانتقاد لأنه قصر مفهوم الجريمة الإلكترونية على المصالح المحمية وهي المعلومات والبرامج ومكونات الحاسوب المادية والمعنوية، فهذا المعيار أدى إلى إيراد تعريفات عامة ومطلقة، لا تحدد الأفعال المتصلة بجرائم الحاسوب بصورة دقيقة ذلك أن الأخذ به يؤدي إلى اعتبار بعض الأفعال من جرائم الحاسب الآلي، مع أنها ليست كذلك في حقيقة الأمر.⁴

ثالثا: التعريف المستند إلى وجوب إمام الفاعل بتقنية المعلومات

إن أصحاب هذا الرأي لا يستندون في تعريفهم للجريمة على وجود الحاسب الآلي، وإنما على الشخص الجالس أمامه، أي أن التعريف يستند على معيار شخصي إذ يستوجب أن يكون الفاعل ملما بتقنية المعلومات واستخدام الحاسب الآلي.

ومن دعاة هذا الاتجاه David Thomson فيرى أنها "جريمة تتطلب لاقترافها لدى فاعلها معرفة

¹ -Michael D.Roster ,Robert H.Rines, computer jurisprudence :legal reponses to the information revolution ,New York,N.Y. :Oceana publications ,1986,p104.

مشار إليه: Mohamed chawki, Essai sur la notion de cybercriminalité, site ichei.org,2006,p27

² - هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، د ط، 1992، ص6.

³ - محمد حماد مرهج الهييتي، التكنولوجيا الحديثة والقانون الجنائي، دار الثقافة، عمان، ط1، 2004، ص123.

⁴ - محمود أحمد عبابنة، المرجع السابق، ص18.

بتقنية النظام المعلوماتي"¹، وقد أعطى الفقيه Stein schiolberg تعريفا للجريمة الإلكترونية بقوله "أي فعل غير مشروع تكون المعرفة بتقنية المعلوماتية أساسية لمرتكبه وللتحقيق فيه وملاحقته قضائيا أو الجريمة التي تعد المعرفة بالحاسب أو استخدامه شرطا ضروريا لارتكابها"² أوهي " أي نمط من أنماط الجرائم المعروفة في قانون العقوبات طالما كان مرتبطا بتقنية المعلومات وهذا تعريف الأستاذ Artar Solerz³.

وكما في الاتجاهات السابقة لم يوفق أصحاب هذا الاتجاه في أن يسلموا من الإنتقاد، إذ هذا الإتجاه تتميز تعاريفه بالقصور، لأن شخصية الجاني لا تكفي وحدها لتعريف الجريمة الإلكترونية، حيث يمكن لشخص عادي غير مؤهل بتقنيات الحاسب الآلي ارتكاب جريمة الغش المعلوماتي أو السرقة المعلوماتية.

رابعا: التعريف المستند إلى معايير مختلفة ومتعددة

لقد اختلف هذا الإتجاه في المعايير المتبناة لتعريف الجريمة الإلكترونية بعيدا عن المعايير السابقة ومن التعاريف ما تضمنته توصيات منظمة التنمية والتعاون الاقتصادي OCDE لسنة 1989 ورد فيه "أنها كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها"⁴، في حين يذهب الفقيه الفرنسي (Massa) إلى تعريف الجريمة الإلكترونية بأنها "الإعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق الربح"⁵، وأيضا عرفها الخبير الأمريكي "دون باركر" "Don B.Parker" الذي قال أنها "فعل إجرامي أيا كانت صلته بتقنية المعلومات، فيه يتكبد المجني عليه نتيجة له خسارة ويحقق الفاعل ربحا عمدياً"⁶.

كما عرفت أيضا بأنها "أي سلوك غير مشروع يرتكب بواسطة نظام حاسوبي أو شبكة حاسوبية بما في ذلك جرائم من قبيل حيازة المعلومات أو عرضها أو توزيعها بصورة غير مشروعة"⁷.

¹ -أحمد خليفة الملط، المرجع السابق، ص96.

² - Mohamed chawki ; op.cit, p72.

³ - خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، دار الثقافة، عمان، ط1، 2011، ص28.

⁴ - Mohamed Chawki , op.cit, P7.

⁵ - محمد علي العريان، المرجع السابق، ص44.

⁶ - محمود أحمد عبابنة، المرجع السابق، ص17.

⁷ - مشتاق طالب وهيبه، المرجع السابق، ص340.

فقد جاءت توصيات مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاينة المجرمين المنعقد في فيينا سنة 2000 بتعريف لجرائم الحاسوب على أنه "يقصد بالجريمة الإلكترونية أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، أو داخل نظام حاسوبي، والجريمة تلك تشمل من الناحية المبدئية، جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية"¹.

إن الإتجاه الذي اعتمد على أكثر من معيار كان موفقا بعض الشيء في مجال شمولية التعريف، لكنه لم يكن في ذات الدرجة في الترتيب والتحديد والتكييف، ولكنه كان أفضل من سابقه في هذا المجال، لأنه أراد من خلال اللجوء إلى عدة معايير للتغلب على معوقات كثيرة لتحديد هذه الظاهرة²، ويعتبر تعريف الأمم المتحدة من أدق التعاريف المقدمة، إذ أحاط بجميع الأشكال الإجرامية للجريمة الإلكترونية سواء التي تقع على النظام المعلوماتي أو التي تقع بواسطة النظام المعلوماتي، كما أنه لم يحصر التعريف بالمعايير المضيق للجريمة أي بواسطة الارتكاب أو مرتكب الجريمة أو الغاية أو النتيجة التي تسعى لها الجريمة³. وصفوة القول أن تعريف الجريمة الإلكترونية لا بد أن يتكيف مع التغيير السريع لتكنولوجيا الحاسبات الآلية لاحتواء مختلف أشكال سلبات العالم الرقمي.

الفقرة الثانية: التعريف القانوني للجريمة الإلكترونية

عادة أن المشرع لا يقوم بوضع تعاريف خاصة بالجريمة لأن ذلك ليس من اختصاصه بل من اختصاص الفقه والقضاء، غير أن وللضرورة الملحة يجد نفسه مضطرا إلى ذلك، إما لتحديد أركان الجريمة العامة أو الخاصة، أو تحديد السلوك الإجرامي المستحدث للجريمة.

والشأن ذاته بالنسبة للجرائم الإلكترونية، فالمشرع لم يعرفها تاركا ذلك للفقه والقضاء كما سبق ذكره ولكن بالرغم من ذلك نجد الاتفاقية الأوروبية بشأن الجريمة الإلكترونية التي أبرمت في بودابست عام 2001، تعتبر أن مصطلح الجريمة الإلكترونية يتناول " النشاطات غير القانونية أو غير المشروعة المرتبطة بأجهزة الكمبيوتر وباستخدام شبكة الأنترنت، وقد صنفّت هذه الجرائم إلى أربعة أنواع هي:

¹ - خالد عياد الحلبي، المرجع السابق، ص30. / محمد أمين الشوابكة، جرائم الحاسوب والأنترنت (الجريمة المعلوماتية)، مكتبة دار الثقافة، عمان، ط1، 2004، ص10.

² - مشتاق طالب وهيب، المرجع السابق، ص341.

³ - نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة عمان، ط2، 2010، ص50.

الجرائم ضد سلامة المعلومات وخصوصيتها، الجرائم ذات الصلة بالكمبيوتر، الجرائم المتعلقة بمحتوى الكمبيوتر، الجرائم التي تتعلق بالعلامات التجارية والملكية الفكرية.¹

كما نجد القانون الأمريكي قد عرف الجريمة الإلكترونية في القانون رقم 1213 لسنة 1982 الخاص بمواجهة الكمبيوتر والجريمة الإلكترونية بأنها " الاستخدام غير المصرح به لأنظمة الكمبيوتر المحمية أو ملفات البيانات، أو الاستخدام المتعمد الضار لأجهزة الكمبيوتر أو ملفات البيانات، وتتراوح خطورة تلك الجريمة ما بين جنحة من الدرجة الثانية إلى جنائية من الدرجة الثالثة".²

كما قام النائب السيد جون مارك ناسم بتقديم تقرير بإسم لجنة الأعمال الخارجية حول مشروع القانون رقم 905 المجيز قبول نفاذ الاتفاقية الأوروبية المبرمة بشأن الجريمة الإلكترونية عرف مصطلح الجريمة الإلكترونية بأنها "مجموعة الجرائم الجنائية المرتكبة عبر شبكة الأنترنت، والتي تشمل ثلاثة أنواع من الجرائم هي:

جرائم المحتوى، جرائم المساس بالملكية الفكرية، الجرائم المعلوماتية".³

أما بالنسبة لموقف المشرع العربي، لم يكن بعيدا عن حماية الأنظمة المعلوماتية ووسائل الاتصال الحديثة، فقد عرف المشرع الإماراتي في المادة الأولى من القانون العربي النموذجي الموحد بشأن مكافحة سوء استخدام تكنولوجيا المعلومات والاتصالات على أنها " كل فعل مؤثم يتم ارتكابه عبر أي وسيط إلكتروني"⁴، أما المشرع السعودي فقد عرف الجريمة الإلكترونية من خلال نظام مكافحة جرائم المعلوماتية

¹ - أبرمت الاتفاقية الأوروبية حول الإجرام المعلوماتي في 2001/11/23 ببودابست بدولة المجر من قبل 30 دولة أوروبية بالإضافة إلى الدول الأربعة غير الأعضاء في المجلس الأوروبي والمتمثلة في كندا، اليابان، الولايات المتحدة الأمريكية، وجنوب إفريقيا.

² - نبيلة هبة هروال، جرائم الأنترنت-دراسة مقارنة-أطروحة لنيل شهادة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بن بوزيد، تلمسان، 2013 -2014، ص 16.

³ - La cybercriminalité peut se définir comme l'ensemble des infractions pénales commises sur le réseau d'internet et elle correspond à trois catégories distinctes d'infraction: Les infractions de contenu, les atteintes à la propriété intellectuelle et les infractions informatiques Député Jean Marc Nesme: Assemblée nationale rapport fait au nom de la commission des affaires étrangères sur le projet de loi n°905 autorisant l'approbation de la convention sur la cybercriminalité.

مشار إليه لدى نبيلة هبة هروال، جرائم الأنترنت، المرجع نفسه، ص 16.

⁴ - عبد الفتاح بيومي حجازي، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي، منشأة المعارف الإسكندرية، ط1، 2009، ص 14.

بأنها " كل فعل يرتكب متضمنا إستخدام الحاسب الآلي والشبكة المعلوماتية بالمخالفة لأحكام هذا النظام".¹

وبالرجوع إلى المشرع الجزائري فمن خلال تعديل قانون العقوبات الجزائري وبموجب القانون رقم 15/04 المؤرخ في 2004/11/10، نجده لم يعط تعريفا للجريمة الإلكترونية، بل اكتفى بالعقاب على بعض الأفعال تحت عنوان "الجرائم الماسة بنظام المعالجة الآلية للمعطيات" المحددة في المواد من 394 مكرر إلى غاية 394 مكرر 7، وقد وجهت عدة انتقادات لهذا القانون لأنه اقتصر الحماية فقط على الجرائم الواقعة على الأنظمة المعلوماتية للحاسب الآلي ولم يشمل الجرائم الأخرى، لهذا تدخل المشرع الجزائري مرة أخرى ليتدارك الأمر وأصدر القانون 04/09 المؤرخ في 26 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الذي وفق هذه المرة في تسميتها لأنها ترادف مصطلح الجريمة الإلكترونية، لاشتمالها على الجرائم المرتكبة على الحاسب الآلي أو عبر شبكة الأنترنت، حيث عرف الجريمة في المادة الثانية من فقرة الأولى وأطلق عليها مصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بقوله "يقصد في مفهوم هذا القانون بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال بأنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، وأي جريمة أخرى ترتكب أو يسهل إرتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الإلكترونية".²

ويلاحظ على هذا التعريف ما يلي:

أن المشرع الجزائري اعتمد عدة معايير لتعريف الجريمة الإلكترونية منها معيار الوسيلة وهو نظام الاتصالات الإلكترونية، أما الثاني هو معيار موضوع الجريمة المتمثل في المساس بأنظمة المعالجة الآلية للمعطيات، أما المعيار الثالث القانون الواجب التطبيق المنصوص عليه في قانون العقوبات.

أما المعيار الرابع تمثل في تحديد نطاق الجريمة الإلكترونية، كونه أقر أن هذه الجريمة ترتكب في نظام معلوماتي أو يسهل إرتكابها عليه، وهذا ما يوسع من نطاق الجريمة الإلكترونية في القانون الجزائري.

¹ - المادة 8/1 من نظام مكافحة جرائم المعلوماتية السعودي.

² - القانون رقم 04/09 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، عدد رقم 47، الصادر بتاريخ 16 أوت 2009.

وترتبط على كل هذه التعاريف الفقهية والقانونية يمكننا القول أن الجريمة الإلكترونية هي كل سلوك غير مشروع يقع على النظام المعلوماتي أو بواسطته ويمس الأشخاص أو الأموال أو أمن الدولة¹، كما يمكن أن نورد هذا التعريف للجريمة الإلكترونية بأنه "فعل أو امتناع للاعتداء على مصلحة مشروعة مادية أو معنوية عن طريق وسائل التكنولوجيا الحديثة".

وفي الأخير يمكن القول أن الجريمة الإلكترونية يغلب عليها عناصر الجريمة التقليدية، لكن المستجد محل الاعتداء المتمثل في المعطيات والبيانات والمعلومات، هذه الكيانات المعنوية فإن كان قانون العقوبات يهتم بالكيان المادي للجريمة، فإن الكيانات المعنوية ذات القيمة المالية ترتبط بالجريمة الإلكترونية وهذا ما جعلها ظاهرة مستحدثة وبالغة الخطورة، وتتميز بخصائص وميزات تختلف عن الجرائم التقليدية.

الفرع الثاني: خصائص الجريمة الإلكترونية

تعد الجرائم الإلكترونية إفرزا ونتاجا لتقنية المعلومات وهذا ما أكسبها طابعا قانونيا خاصا يميزها عن غيرها من الجرائم التقليدية بمجموعة من الخصائص تتمثل في:

أولا: الجريمة الإلكترونية جريمة عابرة للحدود

لم يعد يقتصر مدى الجريمة الإلكترونية على النطاق الوطني فقط، بل بدأت تأخذ بعدا دوليا عابرا للحدود نتيجة سهولة الاتصالات بين دول العالم بسبب انتشار شبكات الاتصال الإلكترونية السلوكية واللاسلكية، التي أحاطت بالعالم وجعلت منه قرية صغيرة، والتي ذابت من خلالها الحدود الجغرافية بين الدول وياتت الجريمة الإلكترونية لا تخضع لنطاق إقليمي محدد، وإنما أصبحت ترتكب في دولة وتمر عبر دولة أخرى وتتحقق نتائجها في دولة أخرى، وكل ذلك في ثوان معدودة، وصارت أكثر من دولة مسرحا لتلك الجريمة.²

و من السمات التي تتميز بها الجريمة الإلكترونية كذلك كونها جريمة عابرة للحدود الوطنية، مما يجعلها تواجه العديد من المشاكل منها تحديد الدولة صاحبة الاختصاص القضائي، وكذلك القانون

¹ -رحيمة نمديلي، خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة، ورقة علمية مقدمة في إطار أعمال المؤتمر الدولي الرابع عشر للجرائم الإلكترونية، المنعقد في طرابلس، لبنان، 24-25 مارس 2017، ص100.

² - أحمد عبد اللاه المراغي، الجريمة الإلكترونية ودور القانون الجنائي في الحد منها -دراسة تحليلية تأصيلية مقارنة-، المركز القومي للإصدارات القانونية، القاهرة، ط 1، 2017، ص73.

الواجب التطبيق عليها، إضافة إلى إشكاليات تتعلق بإجراءات الملاحقة القضائية وغير ذلك من النقاط التي تثيرها الجرائم العابرة للحدود بشكل عام¹.

إذا هذه الاشكاليات أدت إلى لفت أنظار الدول، إلى ضرورة الاهتمام بتدعيم آليات التعاون الدولي في مجال مكافحة الجريمة الإلكترونية، من خلال العمل على تحقيق التنسيق بين تشريعاتها الجنائية من خلال تجريم السلوكات المختلفة، وذلك عن طريق إبرام الاتفاقيات الثنائية أو الإقليمية الجماعية².

و من القضايا التي أعطت البعد الدولي للجرائم الإلكترونية، قضية تعرف باسم مرض نقص المناعة المكتسبة، التي حدثت سنة 1989 التي تتلخص وقائعها في قيام أحد الأشخاص بتوزيع عدد كبير من النسخ الخاصة بأحد البرامج التي تهدف إلى منح بعض النصائح لمرضى نقص المناعة المكتسبة، إلا أن هذا البرنامج في حقيقته عبارة عن فيروس (حصان طروادة) ،هذا ما أدى إلى تعطيل الحواسيب الآلية وعدم قدرتها على العمل نهائيا، وحتى تتمكن من الحصول على مضاد للفيروس لابد من إرسال مبلغ مالي لهذا الشخص، وفي الأخير تم القبض على جوزيف بوب في أوهايو بالولايات المتحدة الأمريكية في 3 فبراير 1990، وقد تقدمت المملكة المتحدة بطلب تسليمه لها لمحاكمته أمام القضاء الإنجليزي، حيث أن إرسال هذا البرنامج قد تم من داخل المملكة المتحدة، وقد وافق القضاء الأمريكي على تسليم المتهم، لكن لم تستمر محاكمته بسبب حالته العقلية وكان لهذه القضية أهميتها من ناحيتين:

الأولى تتمثل في: لأول مرة يتم فيها تسليم متهم في جريمة إلكترونية.

الثانية: تقديم أول مرة شخص للمحاكمة بتهمة إعداد برنامج فيروسي في جريمة إلكترونية³.

ثانيا: صعوبة اكتشاف الجريمة الإلكترونية

تتميز الجريمة الإلكترونية بصعوبة اكتشافها، وإذا اكتشفت فإن ذلك يكون بمحض الصدفة عادة⁴،

¹ - نهلا عبد القادر المومني، المرجع السابق، ص 51.

² - عادل يحيى، السياسية الجنائية في مواجهة الجريمة الإلكترونية، دار النهضة العربية، القاهرة، ط1، 2014، ص58. من أهم هذه الاتفاقيات اتفاقية بودابست المؤرخة في 2001/11/23 التي انضمت إليها الدول الأوروبية كما تم التوقيع عليها من طرف الولايات المتحدة الأمريكية، كندا واليابان، وجنوب إفريقيا، ولعبت دورا هاما في مجال مكافحة الجريمة الإلكترونية، كذلك الاتفاقية العربية لمكافحة تقنية المعلومات المنبثقة عن اجتماع مجلس وزراء الداخلية والعدل العرب بالقاهرة بتاريخ 2010/12/21 والتي صادقت عليها الجزائر في نفس اليوم.

³ - نائلة عادل محمد فريد قورة، جرائم الحاسب الاقتصادية، المرجع السابق، ص48.

⁴ - جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، ط1، 1992، ص17.

والدليل على ذلك أنه لم يكتشف إلا نسبة 1% فقط منها، وأن 15% منها تم الإبلاغ عنها، وأن خمس النسبة الأخيرة هي التي يصدر فيها أحكام بإدانة مرتكبيها.¹

وتتسم الجرائم الإلكترونية بأنها مستترة وخفية في أغلبها حيث أن المجني عليه لا يلاحظها رغم أنها تقع أثناء وجوده على الشبكة، لأن الجاني يتمتع بقدرات فنية يمكنه من تنفيذ جريمته بدقة²، كإرسال الفيروسات أو التجسس على البيانات المخزنة.

ثالثا: إجماع المجني عليه عن الإبلاغ

عند وقوع الجريمة الإلكترونية نجد أن بعض المجني عليهم سواء، كانوا أشخاص طبيعية أو معنوية يحجمون عن إبلاغ السلطات المختصة خشية على السمعة أو المكانة، وعدم هذه الثقة في الكفاءة ومحاولة إخفاء أسلوب ارتكاب الجريمة حتى لا يتم تقليدها من جانب الآخرين، الأمر الذي يشجع الجناة على ارتكاب المزيد من الجرائم، وقد أدى ذلك إلى إقتراح البعض في الولايات المتحدة بأن تفرض النصوص المتعلقة بجرائم الحاسبات إلزاما على عاتق موظفي الجهة المجني عليها بالإبلاغ عما يقع عليها من جرائم في هذا المجال متى وصل إلى علمهم، مع تقرير جزاء في حالة إخلالهم بهذا الالتزام.³

رابعا: جريمة ناعمة

من المتعارف عليه في الجرائم التقليدية أنه يستعمل فيها أدوات وسبل لتحقيق النتيجة الإجرامية، كجريمة السرقة مثلا فإن الأمر يتطلب كسر وخلع أو حتى الحرق... إلخ، كذلك جرائم الإرهاب أو جرائم المخدرات، بينما في الجرائم الإلكترونية فالأمر مختلف تماما، وهذا ما يميز هذا النوع من الجرائم ويجعلها من الجرائم الناعمة، لأنها لا تتطلب عنفا لسرقة المعلومات والبيانات أو نقلها من حاسب لآخر أو معرفة الشيفرات الخاصة بالبنوك والسطو على أرصدها، فرغم غياب العنف إلا أن النتيجة المراد تحقيقها تحققت وهذا سبب تسميتها بالجرائم الناعمة.⁴

¹ - نجاه بن مكي، السياسة الجنائية لمكافحة جرائم المعلوماتية، دار الخلدونية، الجزائر، د ط، 2017، ص 21.

² - عبد المؤمن بن صغير، الطبيعة الخاصة للجريمة المرتكبة عبر الأنترنت في التشريع الجزائري والمقارن، بحث مقدم في إطار الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، المنعقد أيام 16-17 نوفمبر 2015، كلية الحقوق، جامعة بسكرة، الجزائر، ص 8.

³ - محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الأنترنت دراسة مقارنة، دار النهضة العربية، القاهرة، ط 2، 2009، ص 40.

⁴ - عبد العالي الديري، محمد صادق إسماعيل، الجرائم الإلكترونية - دراسة قانونية قضائية مقارنة -، المركز القومي للإصدارات القانونية، القاهرة، ط 1، 2012، ص 56.

خامسا: صعوبة إثبات الجريمة الإلكترونية

قلنا سابقا أن الجريمة الإلكترونية صعبة الإكتشاف، و حتى في حال إكتشاف وقوع الجريمة والإبلاغ عنها فإن إثباتها يثير الكثير من المشاكل، لإتخاذ الجريمة الإلكترونية من البيئة الرقمية ملجأ لها، إذا فهي عبارة عن " حزمة من البيانات والمعلومات في شكل نبضات إلكترونية غير مرئية تنساب عبر النظام المعلوماتي"، مما يجعل أمر طمس الدليل ومحوه كليا أمرا متاحا للمجرم المعلوماتي¹، فهذا الأخير يعمل على إعاقة سلطات التحقيق للوصول إلى الدليل بشتى الوسائل، مثلا كمسح برامج أو وضع كلمات سرية، أو يقوم بتشفير التعليمات لمنع إيجاد أي دليل يدينه، ومن جهة أخرى فنقص الخبرة لدى الجهات القضائية المختصة بالبحث والتحري عن الجرائم الإلكترونية، تقف عائقا أمام إثبات هذا النوع من الجرائم، مما يستدعي تدريب وتأهيل هذه الجهات في مجال جمع الأدلة والتفتيش والملاحقة في البيئة الرقمية، ونتيجة لنقص الخبرة كثيرا ما تخفق أجهزة الشرطة في تقدير أهمية الجريمة الإلكترونية فلا تبذل جهودا لكشف غموضها وضبط مرتكبيها.²

سادسا: أعراض النخبة

إن بعض المتخصصين، يعتقدون في تقنية الحاسبات والمعلوماتية أن من مزايا مراكزهم الوظيفية ومهاراتهم الفنية، استخدام الحاسبات الآلية وبرامجها وتقنياتها لأغراض شخصية أو للتباري الفكري فيما بينهم، أو ممارسة بعض الهوايات الدائرة في فلك هذه التقنية، وهو ما يعبر عنه أو يطلق عليه أعراض النخبة Syndrome elitist وقد يدفع ذلك بعضهم إلى التماهي في استخدام الحاسب الآلي بطريقة غير مشروعة قد تصل إلى حد ارتكاب الجرائم الخطيرة.³

سابعا: الجرائم الإلكترونية جرائم الأذكياء

إن مرتكب الجريمة الإلكترونية في الغالب شخص يتميز بالذكاء والدهاء، ذو مهارات تقنية عالية ودراية بالأسلوب المستخدم في مجال أنظمة الحاسب الآلي وكيفية تشغيله، وكيفية تخزين المعلومات والحصول عليها، في حين أن مرتكب الجريمة التقليدية في الغالب يعتمد على الجهد العضلي ولا يستعمل

¹ - نهلا عبد القادر المومني، المرجع السابق، ص56.

² - نهلا عبد القادر المومني، المرجع نفسه، ص 57 .

³ - فتيحة رصاع، الحماية الجنائية للمعلومات على شبكة الأنترنت، مذكرة لنيل شهادة الماجستير، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، 2011-2012، ص46.

ذكاءه في ارتكاب جرائمه.¹

ثامنا: الجريمة الإلكترونية تتم عادة بتعاون أكثر من شخص

عادة تتم الجريمة الإلكترونية بتعاون أكثر من شخص على ارتكابها إضرارا بالجهة المجني عليها، وغالبا ما يشترك في إخراج الجريمة إلى حيز الوجود، شخص متخصص في تقنيات الحاسوب والانترنت يقوم بالجانب الفني، وشخص آخر من المحيط أو من خارج المؤسسة المجني عليها لتغطية عملية التلاعب وتحويل المكاسب إليه.²

تاسعا: طبيعة المال الذي يرد عليه الاعتداء

يحتوي الحاسب الآلي على عنصرين مادي ومعنوي، فصور الإعتداء على العنصر المادي لا يخرج عن كونه جرائم تقليدية، لكن الإشكال يظهر في حالة الإعتداء على العناصر المعنوية إذ أنها تأخذ وصف جرائم إلكترونية، لأن هذه الأخيرة لها طابع خاص، فهو مختلف تماما عن صور المال التقليدي التي لا تخرج عن كونها شيء مادي الذي يمكن إحرازه ونقله، فالمعلومات عبارة عن مال إلا أنها تتميز عن غيرها من الأموال بما يلي:

- أنه مال غير قابل للنفاذ بمعنى أنه لا ينفذ بالاستعمال.
- أنه مال لا يفقد قيمته بالإستعمال، ولكن يفقد تلك القيمة متى ظهرت معارف أو برامج جديدة.
- إنه مال يمكن إستعماله في آن واحد بواسطة أطراف عديدة دون أن يفقد قيمته، فقيمة المعلومات لا تتغير بإتساع استخدامها.³

وبناء على ما تقدم نصل إلى القول أن الجريمة الإلكترونية تتميز باستقلاليته وذاتيتها عن غيرها من الجرائم لا سيما التقليدية منها، مما جعلها محل اهتمام دول العالم بأسره.

¹ - اسمهان بوضياف، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد 11، 2018، ص 365.

² - عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، ودور الشرطة والقانون-دراسة مقارنة-، منشورات الحلبي الحقوقية، بيروت، د ط، 2003، ص 32.

³ - حسام محمد عيسى، نقل التكنولوجيا دراسة من الآليات القانونية للتبعية الدولية، دار المستقبل العربي، القاهرة، 1987، ص 62.

الفرع الثالث: التطور التاريخي للجريمة لإلكترونية

تعد دراسة التطور التاريخي للإجرام المعلوماتي الخطوة الأولى لبيان مفهوم هذا النوع الخطير من أشكال الإجرام، ذلك أن المجتمعات أصبحت تعتمد على الحاسب الآلي اعتمادا رئيسيا في كافة مجالات الحياة، فكان لزاما أن يرافق التطور التكنولوجي التعدد في الجرائم الإلكترونية تبعا لتطور التقنية واستخدامها¹، وما زاد من حدة هذه الجرائم ارتباط الحواسيب بشبكات الاتصال العالمية، ومن خلال هذا الفرع سوف نتناول مراحل تطور هذه الجريمة.

أولا: مرحلة ظهور واستخدام الحاسبات الآلية

من المعلوم أن هناك صعوبة في تحديد بداية معينة لنشأة الجرائم الإلكترونية، فالإجرام المعلوماتي ارتبط أولا بظهور الحواسيب² الموجودة منذ أمد بعيد، ولكن بأشكال مختلفة عن شكل الحواسيب الحالية، التي كانت تعتمد على أنظمة الترانزستور، بعدما كانت تعتمد على أنابيب التفريغ، مما أدى إلى صنع أجهزة كمبيوتر أصغر حجما وأقل تكلفة، ويرجع البعض أن الجريمة الأولى المتصلة بالحاسوب ارتكبت عام 1901 حيث قام صاحب مصنع للنسيج في فرنسا يدعى جوزيف جاكوارد Joseph Jacquard بتصميم لوحة إلكترونية بمثابة نموذج أولي للوحة الحاسوب الحالية، بحيث تقوم هذه اللوحة بتكرار مجموعة من الخطوات المستخدمة في عملية حياكة أنواع خاصة من المنسوجات، الأمر الذي أثار حفيظة بعض العاملين في المصنع، فقاموا تحت دافع الخوف من أن يؤثر هذا الأمر على وظائفهم ونمط عملهم قاموا بتخريب اللوحة³، بينما يرجع البعض الآخر أن بداية ظاهرة جرائم الحاسوب كانت نهاية الخمسينات من القرن العشرين وبالتحديد عام 1958 بالولايات المتحدة الأمريكية نتيجة إنتشار الحواسيب وتعدد استخداماتها، فبدأ معهد ستانفورد الدولي للأبحاث برصد حالات عرفت آنذاك بإساءة استخدام

¹ - نجاه بن مكي، المرجع السابق، ص15.

2 - يعرف الحاسوب بأنه "مجموعة من أجهزة متكاملة تعمل مع بعضها البعض بهدف تشغيل مجموعة من البيانات

الداخلية وفقا لبرنامج موضوع مسبقا للحصول على نتائج مطلوبة" كما يعرف أيضا بأنه "جهاز يتقبل إدخال input البيانات الأولية Data ويقوم بإجراء العمليات الحسابية أو المعالجة المطلوبة عليها processing وذلك وفقا لأوامر معينة توجه إليه instruction بواسطة برنامج مكتوب program للحصول منها على النتائج المطلوبة out put خروج". انظر أحمد خليفة الملط، المرجع السابق، ص 26/ هدى قشقوش، المرجع السابق، ص19.

³ - محمد بن نصير محمد السرحاني، مهارات التحقيق الجنائي الفني في جرائم الحاسوب والأنترنيت، دراسة مسحية على ضباط الشرطة بالمنطقة الشرقية، جامعة نايف للعلوم الأمنية، قسم العلوم الشرطية، الرياض، 2004، ص24.

الحاسوب في أمريكا، وصنفت إلى جرائم العبث أو التخريب الموجه إلى الحاسوب، سرقة المعلومات أو الممتلكات، وكانت الأنشطة الإجرامية المتصلة بالحاسوب تصاغ وفق مدلول أخلاقي أكثر منه قانوني، مما أدى إلى عدم التمييز بين الأنشطة الإجرامية التي تستهدف ماديّات الحاسوب، أو تلك التي تستهدف معطيات الحاسوب.¹

وفي ستينات القرن العشرين انتشر استعمال الحاسوب خاصة في مجال الأعمال ومنها الأعمال المصرفية، فزادت من نمو وبروز الجريمة الإلكترونية، فسهل ظهور عدة حالات ذات الصلة بالحاسوب، كان أبرزها جريمة سرقة بنك مينيسوتا الأمريكي عام 1966²، والتي اعتبرت أول سرقة إلكترونية تقع على بنك، وتناولت الصحف بعض المقالات الصحفية، وناقشت التلاعب بالبيانات المخزنة وتدمير أنظمة الحواسيب، وشكلت موضوع التساؤل إذا ما كانت هذه الجرائم مجرد حالة عابرة أم ظاهرة مستجدة، بل ثار الجدل حول ما إذا كانت جرائم بالمعنى القانوني أو مجرد سلوكيات أخلاقية في بيئة الحوسبة، فبقيت محصورة في إطار السلوك اللاأخلاقي دون النطاق القانوني³، ورغم استمرار تطور الظاهرة خلال حقبة السبعينات إلا أن الحالات المسجلة للجرائم لم تكن كثيرة والسبب يرجع إلى أن الجرائم المرتكبة تنحصر في العاملين في مجال أنظمة الحاسوب، بالإضافة إلى عدم التبليغ عنها لعدم فقد الثقة أمام العامة، ففي هذه الفترة إزداد إهتمام الباحثين بدراسات تخص جرائم الحاسوب كالدراسة التي أجراها معهد ستانفورد الدولي للأبحاث SRI سنة 1979، بالإضافة إلى دراسة مكتب المحاسبة العامة بالولايات المتحدة الأمريكية GAO، وتعتبر الدراسة التي قام بها معهد الإجرام وقانون العقوبات بألمانيا الاتحادية والتي نشرت عام 1988 من أهم الدراسات الخاصة بالجريمة المرتكبة على الحاسوب، إذ تضمنت وصفا تحليليا لـ 31 جريمة ارتكبت بواسطة الحاسوب⁴، كما صدرت عدة مؤلفات تخص هذا النوع من الإجرام⁵

¹ - نجاه بن مكي، المرجع السابق، ص 16.

² - ورقة بحثية فائزة بالمركز الأول في مسابقة جائزة الأمير نايف عبد العزيز للبحوث الأمنية لعام 2015، مجمعالبحوث والدراسات أكاديمية السلطان قابوس لعلوم الشرطة نزوى سلطنة عمان، الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، مجلس التعاون لدول الخليج العربي، الرياض، 2016، ص 25.

³ - ياسمينه بونغارة، الجريمة الإلكترونية، مجلة المعيار، كلية أصول الدين، جامعة الأمير عبد القادر للعلوم الإسلامية، قسنطينة، العدد 39، جوان 2005، ص 5.

⁴ - محمد بن نصير محمد السرياني، المرجع السابق، ص 25.

⁵ - أبرزها كتاب جرائم الحاسوب computer crime لمؤلفه Gerald Mok night عام 1974، وكتاب الجريمة بواسطة الحاسوب crime by computer لمؤلفه Don. B.Parker.

وبداية لبروز تشريعات وقوانين تجرم بعض الممارسات ذات الصلة بإساءة استخدام الحاسوب، فكانت السويد أول دولة يصدر فيها قانون يجرم بعض الأفعال المرتبطة بالحاسوب سنة 1973.¹

ثانيا: مرحلة ظهور شبكات الاتصال العالمية (الأنترنت)

وفي فترة الثمانينات برز إلى الوجود مفهوم جديد لجرائم الحاسوب، حيث أصبح الحاسب الآلي مرتبطا بشبكة الأنترنت، وبعمليات نظم الكمبيوتر عن بعد وانتشر ما يعرف بالفيروسات الإلكترونية عبر شبكات الحاسوب، التي تتسبب في تدمير البرامج والملفات، وكذلك شاع استخدام مصطلح "الهكرز" المعبر عن مقتحمي النظم، لكن الحديث عن دوافع ارتكاب هذه السلوكيات ظل في غالب الأحيان محصورا عن رغبة المخترقين في تجاوز إجراءات أمن المعلومات أوفي إظهار تفوقهم التقني²، وبعد عام 1988 بداية لارتكاب جرائم تنسم بالخطورة، وبالضبط جريمة "دودة موريس" حيث تمكن طالب يبلغ من العمر 23 سنة ويسمى "روبير موريس" "Robert Morris" من إطلاق ونشر فيروس إلكتروني³، عرف بـ "دودة موريس" (Morris Worms) عبر الأنترنت، حيث تمكن من مهاجمة 6 آلاف حاسوب مرتبط بالأنترنت، من ضمنها أجهزة العديد من المؤسسات والدوائر الحكومية، وقد تسبب بأضرار بالغة، وهو ما أدى إلى لفت النظر إلى حاجة شبكة الأنترنت إلى توفير معايير من الأمن، وبدأ المستخدمون يفكرون مليا في الثغرات ونقاط الضعف، وقد حكم على موريس بالسجن مدة 3 سنوات وبغرامة مالية قدرت بـ 10 آلاف دولار.⁴

ثالثا: الانتشار الواسع لشبكة الأنترنت

وبحلول سنوات التسعينات تغير مفهوم الجرائم الإلكترونية، وازداد انتشارها عبر العالم وكان ذلك

¹ - وأصدرت الولايات المتحدة الأمريكية قانونها سنة 1974 ثم تلتها ألمانيا عام 1977، وأما كل من النمسا والدنمارك وفرنسا والنرويج فكان ذلك عام 1978.

² - نسرين عبد الحميد نبيه، الجريمة المعلوماتية والمجرم المعلوماتي، منشأة المعارف، الإسكندرية، دط، 2008، ص 69.

³ - الفيروس عبارة عن "برنامج يصممه المجرم المعلوماتي بطريقة تعطيه القدرة على ربط نفسه ببرامج أخرى ثم يتوالد ويتكاثر تلقائيا وينتشر داخل البرامج المختلفة، أو بين مواقع معينة من ذاكرة الحاسب حتى يحقق الأهداف المؤاخذة، أو هي عبارة عن برنامج مصمم عمدا ليقترن ببرنامج آخر بحيث يعمل الفيروس عندما يعمل ذلك البرنامج ومن ثم يعيد إنتاج نفسه باقتارنه ببرامج أخرى نوخذ يغير الفيروس نفسه عند إعادة الإنتاج فيظهر كنسخة معدلة من النسخة التي قبلها". أنظر عبد اللاه أحمد هلال، جرائم الحاسب والأنترنت بين التجريم الجنائي وآليات المواجهة، دار النهضة العربية، القاهرة، د ط، 2015، ص 137.

⁴ - نسرين عبد الحميد نبيه، المرجع السابق، ص 81.

بسبب ما أحدثته وسائل الاتصال الحديثة خصوصا شبكة الأنترنت، فبعدها كانت مجرد شبكة ذات أغراض عسكرية، ثم إلى شبكة أكاديمية صغيرة إلى أن أصبحت تضم الآن ملايين المستخدمين في كافة أنحاء العالم، وبيئة متكاملة للاستثمار والعمل والإنتاج والإعلام والحصول على المعلومات.¹

وتواصلت سلسلة الهجمات الموجهة لإرتكاب الجرائم الإلكترونية، ومن أخطرها هجوم عرف باسم Ip-Spoofing الذي وقع عام 1995، حيث أدى إلى وقف عمل الحواسيب المتصلة بالأنترنت، وتشغيل حواسيب وهمية في مكانها تظاهرت بأنها الحواسيب الموثوقة، ومنذ ذلك التاريخ بدأت العديد من الهجمات تظهر مستفيدة من نقاط الضعف في الأنظمة المعلوماتية، كما شهد عام 1996 هجمات خطيرة عرفت باسم "هجمات إنكار الخدمة" استهدفت تعطيل النظام عن العمل من خلال ضخ سيل من المعلومات والرسائل تؤدي إلى عدم قدرة النظام المستهدف على التعامل مع الطلبات الصحيحة، أو تجعله مشغولا عنها، كما سعت أيضا الهجمات المعتمدة على الأنترنت لتعطيل مواقع الأنترنت²، هذه التغيرات في وسائل الهجوم وحجم الأضرار الناتجة عنها أظهر التفكير بخطط الأمن للدفاع عن النظم ومواقع المعلومات، وظهر ما يعرف بالأمن المعلوماتي، وبدأت تظهر معه طرق للحماية وللوقاية التقنية كالجدران النارية "fire walls" وبرامج مضادات الفيروسات Anti virus programs والتشفير.

لتأتي بعد ذلك فترة سنوات الألفين (2000) والتي تميزت بظهور أنواع أخرى من الجرائم الإلكترونية تنتم بالخطورة على أمن الفرد والجماعات، من خلال استهدافها لشتى المجالات سواء منها الحيوية للدولة أو الأفراد، فأصبحت الجريمة الإلكترونية سلوكا نتعايش معه يوميا في ظل التهديدات التي تشكلها على مصالحنا الخاصة والعامة، ونظرا لإعتمادنا المتزايد على تقنية المعلومات يوميا.³

فهذه الجرائم المستحدثة في تزايد مستمر بسبب التطور المستمر للتقنية، هذا ما جعل الدول تتظافر للتصدي لهذا النوع من الإجرام، من خلال سن القوانين والتشريعات لمواجهة هذه الظاهرة الإجرامية المستجدة، والمستجد فيها دخول الحاسوب عالم الإجرام، وما تحدثه شبكة الأنترنت من تسهيل لعمليات دخول الأنظمة واقتحام شبكات المعلومات ونشر الفيروسات وظهور صور جديدة من الجرائم مرتبطة

1- نسرين عبد الحميد نبيه، المرجع نفسه، ص 80.

2- نبيلة هبة هروال، جرائم الأنترنت دراسة مقارنة، أطروحة لنيل شهادة الدكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، الجزائر، 2013-2014، ص 29.

3- حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة لنيل شهادة دكتوراه علوم، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2015-2016، ص 23.

بالكيانات المعنوية ذات القيمة المالية.

الفرع الرابع: تصنيف الجرائم الإلكترونية

هناك حقيقة لا يمكن لأي شخص أن ينكرها وهي أنه رغم المحاولات التي برزت لإيجاد تصنيف واضح ومحدد لصور الجريمة الإلكترونية، إلا أنها أعجزت الفقهاء عن الاتفاق على ذلك، بسبب الطبيعة الخاصة والمعقدة لها، وكونها ظاهرة لها القابلية على التجدد وفقا لمتغيرات التكنولوجيا المستمرة، فكلما ظهرت تقنية ظهر بموازاتها نمط إجرامي¹، فتباينت أشكال وصور الجريمة الإلكترونية مما تعذر تحديدها، فلم يتفق الفقهاء على معيار واحد للتصنيف.

وعليه سنحاول عرض أهم محاولات تصنيف الجرائم الإلكترونية كما يلي:

الفقرة الأولى: تصنيفات تبعا لنوع المعطيات ومحل الجريمة

رافق هذا التصنيف موجات التشريع في ميدان قانون تقنية المعلومات، وهو يعكس أيضا التطور التاريخي لظاهرة الجريمة الإلكترونية، ونجد هذا التصنيف السائد في مختلف مؤلفات الفقيه "أولريش سيبر" "Ulrich Sieber" والمؤلفات المتأثرة بها²، ولهذا نجد أن الجرائم الإلكترونية بالإستناد إلى هذا المعيار يمكن تقسيمها ضمن الطوائف التالية:

أولا: الجرائم الماسة بقيمة معطيات الحاسوب

وتشمل هذه الطائفة فئتين هما الجرائم الواقعة على المعطيات، كجرائم الإلتلاف والتشويه للبيانات والمعلومات وبرامج الحاسوب بما في ذلك استخدام وسيلة (الفيروسات) التقنية، أما الفئة الثانية الجرائم الواقعة على ما تمثله المعطيات آليا من أموال أو أصول، كجرائم غش الحاسوب التي تستهدف الحصول على المال أو جرائم الإتجار بالمعطيات، وجرائم التلاعب في المعطيات المخزنة داخل نظم الحاسوب واستخدامها مثل تزوير المستندات المعالجة آليا.³

¹ - مشتاق طالب وهيب، المرجع السابق، ص 357.

² - نسرين عبد الحميد نبيه، المرجع السابق، ص 103.

³ - سمير شعبان، الجريمة الإلكترونية، مقارنة تحليلية لتحديد مفهوم الجريمة والمجرم، مجلة دراسات وأبحاث، المجلد 1، العدد 1، 2009، ص 120.

ثانيا: الجرائم الماسة بالمعطيات الشخصية أو البيانات المتصلة بالحياة الخاصة

وتشمل جرائم الاعتداء على المعطيات السرية أو المحمية وجرائم الاعتداء على البيانات الشخصية المتصلة بالحياة الخاصة.

ثالثا: الجرائم الماسة بحقوق الملكية الفكرية لبرامج الحاسوب ونظمه (جرائم قرصنة البرمجيات)

وتشمل نسخ وتقليد البرامج وإعادة انتاجها وصنعها دون ترخيص، والاعتداء على العلامة التجارية وبراءة الاختراع.

الفقرة الثانية: تصنيف الجرائم تبعا لدور الكمبيوتر في الجريمة

يؤدي الحاسب الآلي دورا كبيرا في ارتكاب الجريمة الإلكترونية، فقد يكون هدف الاعتداء المعطيات المعالجة أو المخزنة أو المتبادلة بواسطة الحاسوب والشبكات، وقد يكون وسيلة لارتكاب جرائم إلكترونية أخرى، وقد يكون الحاسب الآلي بيئة للجريمة أو وسطا مخزنا للمادة الجرمية، وفي هذا الإطار نجد مفهومين يجري الخلط بينهما يعبران عن هذا الدور الأول جرائم التخزين، ويقصد بها تخزين المواد الجرمية أو المستخدمة في ارتكاب الجريمة أو الناشئة عنها، والثاني جرائم المحتوى أو ما يعبر عنه بالمحتوى غير المشروع، وهذا المصطلح الأخير استخدم مع تطور أشكال الجريمة عند استعمال شبكة الأنترنت¹، وأصبح المحتوى غير القانوني يرمز إلى جرائم المقامرة ونشر المواد الإباحية بإعتبار أن مواقع الأنترنت تتصل بشكل رئيسي بهذه الأنشطة، والحقيقة أن كلا المفهومين يتصلان بالحاسوب والشبكات لإرتكاب الجريمة في نفس الوقت كوسيلة لإرتكابها، وتبعا له تنقسم الجرائم الإلكترونية إلى جرائم تستهدف الأنظمة المعلوماتية كالاستيلاء على المعلومات وإتلافها أو تعديلها، وجرائم ترتكب بواسطة النظم المعلوماتية كجرائم احتيال الحاسوب²، وفي ضوء تطور التدابير التشريعية في أوروبا تم تقسيمها كجرائم هدف ووسيلة ومحتوى، وأفضل ما يعكس هذا التقسيم الإتفاقية الأوروبية للجرائم الإلكترونية لعام 2001³، ومنذ مطلع عام 2000 اتجهت الجهود إلى وضع إطار عام لتصنيف جرائم الحاسوب والأنترنت وعلى الأقل وضع الحد الأدنى محل التعاون الدولي في مجال مكافحة هذه الجرائم، مع ملاحظة أنها تخرج من

¹ - يوسف حسن يوسف، الجرائم الدولية للأنترنت، المركز القومي للإصدارات القانونية، القاهرة، ط1، 2011، ص39.

² - علي عبود جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، منشورات زين الحقوقية، بيروت، ط1، 2013، ص89.

³ - نسرين عبد الحميد نبيه، المرجع السابق، ص106.

بينها طائفة جرائم الخصوصية لوجود إتفاقية أوروبية مستقلة تعالج حماية البيانات الإسمية من مخاطر المعالجة الآلية للبيانات.¹

ولقد أوجدت الإتفاقية الأوروبية تقسيما جديدا نسبيا، فقد تضمنت أربع طوائف رئيسية لجرائم الكمبيوتر والأنترنت هي:²

- الجرائم التي تستهدف عناصر السرية والسلامة وهو فورية المعطيات والنظم، وتضم الدخول غير القانوني، الإعتراض غير القانوني، تدمير المعطيات، إعتراض النظم، إساءة استخدام الأجهزة.
- الجرائم المرتبطة بالكمبيوتر وتشمل التزوير المعلوماتي، الإحتيال المعلوماتي.
- الجرائم المرتبطة بالمحتوى وتضم طائفة واحدة وفق هذه الإتفاقية وهي الجرائم المتعلقة بالأفعال الإباحية والأخلاقية.
- الجرائم المرتبطة بالإخلال بحق المؤلف والحقوق المجاورة كقرصنة البرمجيات.

الفقرة الثالثة: تصنيف الجرائم تبعا لمساسها بالأشخاص والأموال

تعتبر الدراسات والأبحاث الأمريكية من أبرز الدراسات التي ركزت على هذا التصنيف، فالتقسيم الذي تناوله مشروع القانون النموذجي لسنة 1998، وفي نطاقه قسمت الجرائم الإلكترونية إلى جرائم واقعة على الأشخاص، وجرائم واقعة على الأموال عدا السرقة، وجرائم السرقة والإحتيال، وجرائم التزوير، وجرائم المقامرة والجرائم ضد الآداب عدا الجرائم الجنسية، والجرائم ضد المصالح الحكومية، فالجرائم التي تستهدف الأموال تضم من حيث مفهومها السرقة والإحتيال، أما الجرائم التي تستهدف التزوير فتتمس الثقة والاعتبار والجرائم الواقعة ضد الآداب قد تتصل بالشخص وقد تتصل بالنظام والأخلاق العامة³، وعلى العموم فإنه تبعا لهذا التقسيم الوارد في القانون النموذجي الأمريكي تصنف الجرائم على النحو التالي:

أولا : طائفة الجرائم التي تستهدف الأشخاص

وتضم طائفتين رئيسيتين هما:

¹ - الاتفاقية الأوروبية بشأن حماية البيانات من مخاطر المعالجة الآلية لعام 1981.

² - يوسف حسن يوسف، المرجع السابق، ص 40.

³ - يونس عرب، المرجع السابق، ص 11.

1- الجرائم غير الجنسية التي تستهدف الأشخاص

وتتضمن جرائم القتل بالكمبيوتر، والتسبب بالوفاة جرائم الإهمال المرتبط بالكمبيوتر، والتحريض على الإنتحار، والتحريض القسدي للقتل عبر الإنترنت، التحرش والمضايقة عبر وسائل الاتصال المؤتمنة، والتهديد عبر وسائل الاتصال المؤتمنة، والملاحقة عبر الوسائل التقنية، وأنشطة اختلاس النظر أو الإطلاع على البيانات الشخصية، وقنابل البريد الإلكتروني، وأنشطة ضخ البريد الإلكتروني غير المطلوب أو غير المرغوب فيه، وبت المعلومات المضللة أو الزائفة والانتهاك الشخصي لحرمة كمبيوتر.¹

2- طائفة الجرائم الجنسية

وتشمل تحريض القاصرين على أنشطة جنسية غير مشروعة، وتلقي أو نشر المعلومات عبر الكمبيوتر من أجل أنشطة غير مشروعة، ونشر أو تسهيل نشر واستضافة المواد الفاحشة عبر الإنترنت بوجه عام وللقاصرين تحديداً، إظهار القاصرين ضمن أنشطة جنسية أو للإغواء أو لنشر المواد الفاحشة التي تستهدف استغلال عوامل الضعف لدى المستخدم، والحصول على الصور بطريقة غير مشروعة لاستغلالها في أنشطة جنسية، وهي أوصاف تجتمع جميعها تحت صورة واحدة هي استغلال الإنترنت والكمبيوتر لترويج الدعارة أو إثارة الفحش واستغلال الأطفال والقصر في أنشطة جنسية غير مشروعة.²

ثانياً: طائفة جرائم الأموال

ويستثنى من هذا التقسيم جريمة السرقة، وتشمل هذه الطائفة أنشطة إقتحام أو الدخول أو التوصل غير المصرح به مع نظام الكمبيوتر أو الشبكة، وكذلك تخريب المعطيات والنظم والممتلكات ضمن مفهوم تخريب الكمبيوتر وخلق البرمجيات الخبيثة والضارة، وإستخدام إسم النطاق أو العلامة التجارية أو إسم الغير دون ترخيص، وإدخال معطيات خاطئة أو مزورة إلى نظام الكمبيوتر، والإتلاف غير المصرح به لنظم الكمبيوتر، وأنشطة إنكار الخدمة أو تعطيل أو إعتراض عمل النظام أو الخدمات، و أنشطة الإعتداء على الخصوصية (جرائم الاختراق) وإفشاء كلمة سر الغير والحيازة غير المشروعة للمعلومات وإساءة استخدام المعلومات، ونقل المعلومات الخاطئة.³

¹ - عبد الصبور عبد القوي علي مصري، الجريمة الإلكترونية، دار العلوم، القاهرة، ط1، 2010، ص، ص، 32-33.

² - نسرین عبد الحمید نبیه، المرجع السابق، ص، ص، 109-110.

³ - یونس عرب، المرجع السابق، ص13.

1- جرائم الإحتيال والسرقة

ويشمل التلاعب بالمعطيات والنظم، وإستخدام البطاقات المالية للغير دون ترخيص أو تدميرها، والإختلاس عبر الحاسوب أو بواسطته، وسرقة معلومات الحاسب الآلي وقرصنة البرامج وسرقة خدمات الكمبيوتر، وسرقة أدوات التعريف والهوية عبر إنتحال هذه الصفات أو المعلومات داخل الكمبيوتر.¹

2- جرائم التزوير

وتشمل تزوير البريد الإلكتروني وتزوير الوثائق والسجلات وتزوير الهوية.

3- جرائم الكمبيوتر ضد الحكومة

وتشمل هذه الطائفة كافة جرائم تعطيل الأعمال الحكومية وتنفيذ القانون، والإخفاق في الإبلاغ عن جرائم الكمبيوتر، إضافة الحصول على المعلومات السرية، والإخبار الخاطئ عن جرائم الحاسب الآلي، العبث بالأدلة القضائية أو التأثير بها، كما تشمل الإرهاب الإلكتروني.²

4- جرائم المقامرة والجرائم الأخرى ضد الأخلاق والآداب

وتشمل تملك وإدارة مشروع مقامرة على الأنترنت، وتسهيل إدارة مشاريع القمار على الأنترنت واستخدام الأنترنت لترويج الكحول ومواد الإدمان للقصر.³

الفقرة الرابعة: تصنيف الجرائم تبعا لمساسها بالمصلحة العامة

لقد ساعدت الشبكات وعلى الأخص خدمة الأنترنت في اختراق الحواسيب الحكومية ومن ثم إمطة اللثام بكل سهولة على أسرار الدولة المتعلقة بأمنها وسلامتها وما ينتج عن هذا الفعل من تداعيات.

¹ - من أمثلة جرائم الإحتيال قضية المدعو Stanley Mark Ar الذي يعمل خبير حاسوب في بنك باسفيك في لوس انجلوس إذ قام المدعو بزيارة غرفة البرقيات في المصرف بعد توقفه عن العمل وحصل على الرقم السري للتحويلات ورقية من لوحة النشر باستعمال هذا الرقم تمكن من خلال حاسوب آخر عن بعد الدخول إلى حاسوب البنك وتحويل أكثر من عشرة ملايين دولار إلى حساب صديق له يعمل تاجرا للماس وذلك في أحد المصارف في سويسرا. أنظر آدم لمي عبد الباقي محمود، مدى فاعلية الجهود الدولية والإقليمية في مواجهة جرائم الكمبيوتر والحد منها، ص292.

² - يوسف حسن يوسف، المرجع السابق، ص 47.

³ - نسرین عبد الحمید نبیه، المرجع السابق، ص، ص 112-113.

الفقرة الخامسة: تصنيف الجرائم كجرائم حاسوب وجرائم أنترنت

بعد تطور الحواسيب وانتشار استعمالها في أوساط المجتمع، كثرت الجرائم المرتكبة على الحاسب الآلي خاصة منها الإعتداءات على الأنظمة المعلوماتية أو بواسطتها، هذا قبل أن يشيع إستخدام شبكات الأنترنت، ومن الطبيعي أن تخلق الأنترنت أنماطا جرمية مستجدة، أو تأثر بالآلية التي ترتكب فيها جرائم الكمبيوتر ذاتها بعد أن تحقق توصيل الكمبيوترات معا في نطاق شبكات محلية وإقليمية وعالمية، ومن هنا جاء هذا التقسيم.¹

وفي نطاق هذا المعيار يمكن التمييز بين الأفعال التي تستهدف المعلومات في نطاق الكمبيوتر ذاته خلال مراحل المعالجة والتخزين والاسترجاع، وبين الأنشطة التي تستهدف الشبكات ذاتها أو المعلومات المنقولة عبرها، والأنشطة التي تستهدف مواقع الأنترنت وخدامها من نظم الكمبيوتر، أو تستهدف تطبيقات وإستخدامات وحلول الأنترنت وما نشأ في بيئتها من أعمال إلكترونية وخدمات إلكترونية²، ومن جانب آخر يحدد البعض أنشطة جرائم الأنترنت بتلك المتعلقة بالإعتداء على المواقع وتعطيلها وتشويهها أو تعطيل تقديم الخدمة، وكذلك أنشطة المحتوى الضار لترويج المواد الإباحية والمقامرة، وأنشطة إثارة الأحقاد والتحرش والإزعاج، ومختلف صور الأنشطة التي تستخدم البريد الإلكتروني والمراسلات الإلكترونية، وأنشطة الإستيلاء على كلمات السر الخاصة بالمستخدمين والهوية ووسائل التعريف، وأنشطة احتيال الأنترنت كاحتيال المزادات وعدم التسليم الفعلي للمنتجات والخدمات، وأنشطة نشر الفيروسات ... إلخ.³

أما فيما يتعلق بجرائم الحاسب الآلي فإنها وفق هذا التقسيم ترجع إلى الأنشطة التي تستهدف المعلومات والبرامج المخزنة داخل نظم الكمبيوتر، وتحديدًا أنشطة التزوير واحتيال الكمبيوتر وسرقة المعطيات وسرقة وقت الحاسوب وإعتراض المعطيات خلال النقل مع أنه مفهوم يتصل بالشبكات أكثر من نظم الكمبيوتر، إضافة للتدخل غير المصرح به، والذي يتوزع ضمن هذا التقسيم بين دخول غير مصرح به لنظام الكمبيوتر ودخول غير مصرح به للشبكات فيتبع لمفهوم جرائم الأنترنت.⁴

¹ - يوسف حسن يوسف، المرجع السابق، ص 47.

² - نسرین عبد الحمید نبیه، المرجع السابق، ص 114.

³ - یونس عرب، المرجع السابق، ص 14.

⁴ - عبد الصبور عبد القوي علي مصري، المرجع السابق، ص 30.

وانتقد هذا التقسيم من الفقه وباعتباره غير دقيق وغير منضبط ومخالف للمفاهيم التقنية والمرحلة التي وصل إليها تطور وسائل تقنية المعلومات وعمليات التكامل والدمج بين وسائل الحوسبة والاتصال، ففي هذه المرحلة ثمة مفهوم عام لنظام الكمبيوتر يستوعب كافة مكوناته المادية والمعنوية المتصلة بعمليات الادخال والمعالجة والتخزين والتبادل، مما يجعل الشبكات وارتباط الكمبيوتر بالإنترنت جزء من فكرة تكاملية للنظام،¹ ومن جهة أخرى فإن أنشطة الإنترنت تتطلب أجهزة كمبيوتر تتجزأ بواسطتها، وهي تستهدف أيضا معلومات مخزنة أو معالجة ضمن أجهزة كمبيوتر، هي الخوادم التي تستضيف مواقع الإنترنت أو تديرها، وعليه يعتبر هذا المعيار غير صحيح إذا ما عمدنا إلى تحليل كل نمط من أنماط الجرائم المتقدمة في ضوء هذا المعيار، فعلى سبيل المثال تعد الجريمة الدخول غير المصرح به لنظام الكمبيوتر وفق هذا المعيار جريمة كمبيوتر، أما الدخول غير المصرح به إلى موقع أنترنت فهي تعتبر جريمة أنترنت، مع أن الحقيقة التقنية تبين أن الدخول في الحالتين هو دخول إلى نظام الكمبيوتر عبر الشبكة²

واستخلاصا لما سبق لأهم التصنيفات المتعلقة بالجرائم الإلكترونية، ويمكن القول أن أكثر التقسيمات انضباطية هو معيار تصنيف هذه الجرائم تبعا لدور الكمبيوتر في الجريمة، سواء كان هدفا للجريمة أو وسيلة لإرتكابها.

وهو المعيار الذي تبناه المشرع الجزائري ولمواكبة تطور القوانين العقابية في مواجهة الجريمة الإلكترونية، فقام بتعديل قانون العقوبات وأصدر القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، فجرم المساس بأنظمة المعالجة الآلية للمعطيات وأدرجها ضمن القسم السابع مكرر.

الفرع الخامس: دور الحاسب الآلي في ارتكاب الجريمة الإلكترونية

يلعب الحاسوب دورا كبيرا ومهما في إرتكاب الجريمة الإلكترونية، فقد يكون له دور في ارتكابها وإما يكون الهدف المباشر للاعتداء أو موضوع الاعتداء، أو وسيلة الاعتداء لتحقيق نتيجة إجرامية وهذا ما سوف نتناوله من خلال هذا الفرع.

¹ - عبد الصبور عبد القوي علي مصري، المرجع السابق، ص37.

² - حسن يوسف حسن، المرجع السابق، ص50.

أولاً: الحاسب الآلي هدفاً للجريمة

يعرف الحاسب الآلي بأنه "مجموعة متكاملة من الأجهزة التي تعمل مع بعضها البعض بهدف تشغيل مجموعة البيانات الداخلة طبقاً لبرنامج تم وضعه مسبقاً للحصول على نتائج معينة"¹، ويقصد بالحاسوب هدفاً للجريمة أي الجرائم التي تستهدف معطيات الحاسوب المعنوية من برامج وتطبيقات وبيانات التي ترتكب من خلال برامج الحاسوب، أو عن طريق الأنترنت، وكذلك الإعتداء على بعض الأجهزة الإلكترونية الخاصة بالاتصال²، ومن أوضح المظاهر لإعتبار الحاسوب هدفاً للجريمة في مجال التصرفات غير القانونية عندما تكون السرية (confidentialité) والتكاملية أي السلامة (intégrité)، والقدرة أو التوفر (availability) هي التي يتم الإعتداء عليها، بمعنى أن توجه هجمات الكمبيوتر إلى معلومات الحاسوب أو خدماته، أو تعطيل الأنظمة للقيام بأعمالها، وهدف هذا النمط الإجرامي هو النظام المعلوماتي، وبشكل خاص المعلومات المخزنة داخله³، كما يكون الحاسوب هدفاً للنشاط الإجرامي وموضوعاً للجريمة مثل جرائم التخريب والإتلاف التي توجه إلى مكونات الحاسوب نفسه مثل الأسطوانات المدمجة أو الأشرطة الممغنطة.⁴

ثانياً : الحاسب الآلي أداة لإرتكاب الجريمة

في هذه الحالة تقع الجريمة بواسطته أي أنه يستخدم كأداة لارتكابها، ومن الناحية النظرية يمكن أن تقع بعض الجرائم بواسطة الحاسوب مثل الجرائم التي تقع على الذمة المالية من سرقة ونصب وخيانة الأمانة والتزوير⁵، كما تستخدم في القتل وذلك عن طريق برمجة جهاز تفجير يتم التحكم فيه آلياً أو جهاز لإطلاق الأشعة القاتلة.⁶

ومن أخطرها كذلك التعدي على البيانات الخاصة، ويشمل ذلك تجاوز استخدام المعلومات المجمعة

¹ - عبد العال الديري، المرجع السابق، ص 16.

² - تركي بن عبد الرحمن المويشير، بناء نموذج أمني لمكافحة الجرائم المعلوماتية وقياس فاعليته، أطروحة لنيل شهادة دكتوراه الفلسفة، كلية الدراسات العليا، قسم العلوم الشرطية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2009، ص 41.

³ - نسرين عبد الحميد نبيه، المرجع السابق، ص 90.

⁴ - نجاه بن مكي، المرجع السابق، ص 37.

⁵ - عفيفي كامل عفيفي، المرجع السابق، ص 23.

⁶ - جميل عبد الباقي الصغير، الأنترنت والقانون الجنائي، دار النهضة العربية، القاهرة، د ط، 2012، ص 47.

عن الفرد لغرضها المقصود، والدخول والتداول غير المرخص به للمعلومات.¹

ثالثا: الحاسب الآلي بيئة للجريمة

ويكون الحاسب الآلي بيئة لارتكاب الجرائم الإلكترونية، كتخزين البرامج المقرصنة فيه أو في حالة استخدامه لنشر المواد غير القانونية، أو استخدامه أداة تخزين أو اتصال لصفقات ترويج المخدرات وأنشطة الشبكات الإباحية.

كما يمكن للحاسوب أن يلعب دور في اكتشاف الجريمة، إذ يستخدم على نطاق واسع في التحقيق الاستدلالي لكافة الجرائم، عوضا عن جهات تنفيذ القانون إذ تعتمد على النظم التقنية في إدارة المهام من خلال بناء قواعد بيانات ضمن جهاز إدارة العدالة والتطبيق القانوني.²

ومع تزايد نطاق الجرائم الإلكترونية، وإعتماد مرتكبيها على وسائل التقنية المتجددة والحديثة، فإنه أصبح لزاما استخدام نفس وسائل الجريمة المتطورة للكشف عنها، ومن هنا يلعب الكمبيوتر ذاته دورا رئيسيا في كشف جرائم الكمبيوتر وتتبع فاعليها بل وإبطال أثر الهجمات التدميرية لمخترقي النظم وتحديد هجمات الفيروسات وإنكار الخدمة وقرصنة البرمجيات.³

المطلب الثاني: البنيان القانوني للجريمة الإلكترونية

إذا كانت تعريفات الجريمة عموما تقوم على أساسين هما عناصر الجريمة والسلوك ووصفه، والنص القانوني على تجريم السلوك وإيقاع العقوبة، فإن الجديد في مجال الجرائم الإلكترونية هو إضافة عنصر ثالث يبرز محل الاعتداء في هذه الظاهرة الإجرامية المستحدثة متمثلة بمعلومات الحاسوب⁴، وعليه سوف نقوم من خلال هذا المطلب بدراسة ركنها المفترض أو محل الجريمة (الفرع الأول) بالإضافة إلى أركان الجريمة الإلكترونية (الفرع الثاني)، وكذا الوقوف على مسألة الشروع (الفرع الثالث) والإتفاق الجنائي في هذا النوع من الإجرام وما يثار من إشكالات (الفرع الرابع).

¹ - تركي بن عبد الرحمن المويشير، المرجع السابق، ص 42.

² - فتحة رصاع، المرجع السابق، ص 72.

³ - يونس عرب، المرجع السابق، ص 9.

⁴ - نسرین عبد الحميد نبيه، المرجع السابق، ص 67.

الفرع الأول: المعلومات كمحل للجريمة الإلكترونية

تحتل المعلومات مكانة كبيرة في الواقع المعاصر، فهي باب الوصول إلى المعرفة، والمعرفة كما قيل هي سلطة، فالمعلومات يتم تداولها داخليا أو عبر الدول، فإدراك المجتمعات المعاصرة لأهمية المعلومات وزيادة الاعتماد عليها كمورد حيوي أدى إلى ظهور صناعة المعلومات وتنظيمها وتسويقها وإيصالها إلى من يطلبها كالسلع الأخرى¹.

ولما كانت المعلومات هي المحل الذي يقع عليه الإعتداء في الجرائم الإلكترونية، فيقتضي الأمر منا أن نعرف المعلومات ونبين خصائصها، وأنواعها وطبيعتها القانونية وذلك فيما يلي:

الفقرة الأولى: تعريف المعلومات

لقد تعددت التعاريف بخصوص المعلومات، وقبل عرض هذه التعاريف لابد من تعريفها من الناحية اللغوية.

أولاً: المعلومات لغة

المعلومات من حيث مدلولها اللغوي مشتقة من كلمة "علم" ودلالاتها تدور حول المعرفة التي يمكن نقلها واكتسابها، وأعلم فلانا الخبر أي أخبره به وأعلم فلانا الأمر حاصلًا جعله يعلمه والعلم نقيض الجهل²، وعلمت الشيء أعلمه أي أعرفه³، والمصطلح القريب من ذلك في اللغة الفرنسية هو information وتعني نقل وتوصيل إشارة أو رسالة أو الإعلام منها واتخاذ وظيفتها في نقل المعارف والمعلومات.

ثانياً: التعريف الاصطلاحي

أما إصطلاحاً فتعرف المعلومات بأنها "الحقائق التي تغير من الحالة المعرفية للشخص في موضوع

¹ - محمد سامي الشوا، المرجع السابق، ص55.

² - لقد وجدت المعلومات منذ أن خلق الله سبحانه وتعالى الإنسان عندما خلق الله آدم عليه السلام وعلمه الأسماء كلها، قال الله تعالى في كتابه العزيز «وعلم آدم الأسماء كله وعرضهم على الملائكة فقال انبئوني بأسماء هؤلاء إن كنتم صادقين». سورة البقرة الآية رقم 31، وقوله تعالى في سورة العلق من الآية رقم 1 إلى الآية رقم 5 "اقرأ باسم ربك الذي خلق (1) خلق الإنسان من علق (2) اقرأ وربك الأكرم (3) الذي علم بالقلم (4) علم الإنسان ما لم يعلم (5)".

³ - رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن، مشورات الحلبي الحقوقية، بيروت، ط1، 2012، ص64.

معين" وكذلك هي " كل ما يعرفه الإنسان عن حادث، أو قضية، أو الأخبار، أو التحقيقات وكل ما يؤدي إلى الكشف عن الحقائق وإيضاح الأمور"، وتعرف أيضا بأنها "المعرفة التي تكتسب من خلال الاتصال أو البحث أو التعليم أو الملاحظة، أو كل ما يؤدي الى كشف وإيضاح الأمور.¹

أما من الناحية الفقهية تعددت آراء الفقهاء حيث يعرفها الأستاذ باركر بأنها "مجموعة من الرموز أو الحقائق أو المفاهيم أو التعليمات التي تصلح لأن تكون محلا للتبادل والاتصال، أو التفسير والتأويل أو للمعالجة بواسطة الأفراد أو الأنظمة الإلكترونية، وهي تتميز بالمرونة بحيث يمكن تغييرها وتجزئتها وجمعها أو نقلها بوسائل وأشكال مختلفة".²

أما الأستاذ كاتالا (catala) يعرف المعلومة بأنها " رسالة معبر عنها في شكل يجعلها قابلة للتنقل أو الإبلاغ للغير"، ويعرفها البعض الآخر بأنها "رمز أو مجموعة رموز تتطوي على إمكانية الإفضاء إلى المعنى".³

ثالثا : التعريف القانوني

إهتمت بعض التشريعات بوضع تعريف للمعلومات، حيث عرفها المشرع الفرنسي في القانون الصادر في 29 يوليو 1982 الخاص بالاتصالات السمعية والبصرية، وأشار إلى تعريف المعلومة على أنها "صور الوثائق والبيانات أو الرسائل من أي نوع".⁴

كما عرفها المشرع الأمريكي في قانون المعاملات التجارية الإلكترونية بأنها " تشمل البيانات والكلمات والصور والأصوات والرسائل وبرامج الكمبيوتر والبرامج الموضوعة في الأقراص المرنة وقواعد البيانات أو ما شابه ذلك".⁵

عرفها المشرع الأردني في قانون المعاملات الإلكترونية رقم 85 لسنة 2001 أنها " البيانات

1- مسعود خثير، المرجع السابق، ص 15.

2- نهلا عبد القادر المومني، المرجع السابق، ص 101.

3 - محمد سامي الشواء، المرجع السابق، ص 156 .

4 - محمد محمد شتا، فكرة الحماية الجنائية لبرامج الكمبيوتر، دار الجامعة الجديدة، الاسكندرية، د ط، 2001، ص 20.

5 - عفاف خديري، الحماية الجنائية للمعطيات الرقمية، أطروحة لنيل شهادة دكتوراه علوم، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي، تبسة، 2017-2018، ص 17.

والنصوص والصور، والأشكال والأصوات والرموز، وقواعد البيانات وبرامج الحاسوب وما شابه ذلك"¹، كما عرفها في قانون جرائم أنظمة المعلومات رقم 30 لسنة 2010 أنها " المعلومات التي تمت معالجتها وأصبح لها دلالة"².

رابعاً: التمييز بين المعطيات والمعلومات

إن مصطلح المعطيات تقابله في اللغة البيانات، والبيانات لغة مصدرها الفعل بين أي أظهر واتضح وأفصح، ومن معانيه فيها ما تبين به الشيء من الدلالة وغيرها، ويقابل هذا في الفقه اللاتيني كلمة "Datum" وتعني شيء معطى أو مسلم به أو شيء ما معروف، وتعني في المصطلح الفرنسي "Données" وهي عبارة "عن حقائق أو أشياء معروفة يقينا، ويمكن من خلالها الوصول إلى نتيجة معينة."³

أما إصطلاحاً فيعبر "عن مجموعة من الأرقام والكلمات والرموز، أو الحقائق أو الاحصاءات الخام التي لا علاقة بين بعضها البعض، ولم تخضع بعد للتفسير أو التجهيز للاستخدام، أما المعلومات فهي المعنى الذي يستخلص من هذه المعطيات."⁴

فيما عرفها المشرع الجزائري بموجب المادة 2 من الفقرة "ج" من القانون رقم 04/09 لسنة 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها بأنها "أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل المنظومة المعلوماتية تؤدي وظيفتها".

وفي نفس الاتجاه ذهبت الاتفاقية الأوروبية لمكافحة الجريمة الإلكترونية حيث عرفت بها بموجب الفقرة

(1) - قانون المعاملات الإلكترونية الأردني رقم 85 لسنة 2001، جريدة رسمية 2001/4524 المؤرخة في 2001/12/31 لصفحة 6010، عن الموقع: <http://www.wipo.int/edocs/lexdocs/laus/ar/jo/jo058ar.pdf>، أطلع عليه بتاريخ 2017/03/15، على الساعة 15h 30.

2 القانون الأردني لجرائم أنظمة المعلومات رقم 30 لسنة 2010، الجريدة الرسمية، عدد 5056 المؤرخة في 2010/90/16 الموجودة على الموقع 2 <http://www.law.jo.net/vb/showthread.php?116512> أطلع عليه بتاريخ 2017/30/15، على الساعة 15:30.

³ - رشيدة بوكري، المرجع السابق، ص 65.

⁴ - نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة لنيل شهادة الماجستير في العلوم القانونية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2012-2013، ص 15.

"ب" من المادة الأولى على أنها " كل تمثيل للوقائع أو المعلومات أو المفاهيم تحت أي شكل وتكون مهيأة للمعالجة الآلية، بما في ذلك برنامج معد من ذات الطبيعة ويجعل الحاسب يؤدي المهمة"¹، والملاحظ أن تعريف المشرع الجزائري هو نفسه المنصوص في إتفاقية بودابست ما يبين تأثر المشرع بهذه الإتفاقية كما تشير المذكرة التفسيرية لإتفاقية بودابست أن تعريف المعطيات المعلوماتية الواردة المادة الأولى فقرة "ب" مأخوذة من هيئة التوصيف العالمية الأيزو (ISO)².

فيما عرفت الوكالة الفرنسية للتقييس (Afnor) المعطيات على أنها " كل حادث مفهوم أو تعلية تقدم في شكل متفق عليه، قابل للتبادل عن طريق البشر أو بوسائل أوتوماتيكية"³، وهناك من يرى أن ما يدخل إلى الحاسب الآلي يعتبر معطيات وليس لها معنى بمفردها إلا بعد معالجتها وتحويلها إلى معلومات، وعليه فإن كل ما يميز الواحدة عن الأخرى هو الصورة التي توجد عليها في الواقع، فالمعطيات المقصودة هنا لابد أن تأخذ شكلا معينا، والمعطيات يمكن معالجتها داخل النظام وتصبح معلومات⁴، ومن خلال ما سبق ذكره يتبين لنا أن المعطيات هي المعلومات في حالة كمون وأن المعلومات هي المعطيات في حالة تبلور⁵، إذن المعلومات هي المعطيات التي تمت معالجتها آليا أو إلكترونيا.

ونظرا إلى أن للمعلومة قيمة باعتبارها نتاج نشاط إنساني، لهذا يجب أن تتوفر فيها شروط معينة فيما تتمثل هذه الشروط؟

¹ - Art.1 du convention sur la cybercriminalité ; L'expression "données information « désigne toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction », convention sur la cybercriminalité Budapest 23 novembre 2001, série des traités européens n° 185.

⁴ - والحروف الثلاثة ISO هي أوائل الكلمات الثلاث التالية: International Standar dization أي هيئة التوصيف العالمية (أيزو) وهي هيئة دولية لوضع المواصفات تمثل فيها الدول بهيئات التوصيف الإقليمية بهدف توحيد المواصفات على المستوى الدولي.

³ - رشيدة بوكري، المرجع السابق، ص66.

⁴ - غنية باطلي، الجريمة الإلكترونية -دراسة مقارنة-، الدار الجزائرية، الجزائر، ط، 2015، ص70.

⁵ - محمد محمد شتا، المرجع السابق، ص62.

الفقرة الثانية: الشروط الواجب توافرها في المعلومة محل الإعتداء

يجب توافر مجموعة من الشروط لكي تتمتع المعلومة بالحماية الجنائية، وتتمثل هذه الشروط في:

أولاً: التحديد والإبتكار

من أهم شروط المعلومة إتصافها بالتحديد، وهذه الصفة تعتبر خاصية أساسية تفرض نفسها دائماً، فالمعلومة التي تفقر لصفة لا يمكن أن تكون معلومة حقيقية، ويقول الأستاذ كاتالا Catala " أن المعلومة قبل كل شيء تعبير وصياغة محددة، تجعل رسالة ما قابلة للتبليغ عن طريق علامات أو إشارات معينة، فهذا يتطلب أن تكون محددة ويصبح هذا التحديد ضرورياً، وبصفة خاصة في مجال الاعتداءات على الأموال، فهذه الاعتداءات تفترض دائماً وجود شيء محدد.¹

أما شرط الإبتكار فإنه يجب أن تنصب هذه الصفة على الرسالة التي تحملها المعلومة، فمعلومة غير مبتكرة هي معلومة عامة، متاحة للجميع، ولا يمكن نسبتها إلى شخص محدد، أو طائفة من الأشخاص.²

ثانياً: السرية

السرية هي أهم خصائص المعلومات التي تنطبق عليها الحماية القانونية، وإضفاء الطابع السري يحصر دائرة الرسالة التي تحملها هذه المعلومة محدداً بمجموعة معينة من الأشخاص، وبدون هذا التحديد فإنه لا يمكن أن تكون المعلومة محلاً، يعتدى عليه بالسرقة أو النصب على سبيل المثال³، فالمعلومة غير السرية تكون قابلة للتداول، ومن ثم تكون بمنأى عن أي حيازة كالمعلومات التي تتعلق بحقيقة معينة (كحالة الجو في وقت معين).

كما تكتسب المعلومة سريتها من طبيعتها، أو بالنظر إلى رغبة صاحبها أو للأمرين معاً، كما في حالة الشفرة السرية الخاصة باستعمال بطاقات الائتمان، وفي جميع الحالات فإن السرية التي تتمتع بها المعلومة هي التي تحدد نطاق استعمالها في دائرة محددة، بحيث يستفيد أصحابها من الخاصية الثانية وهي الإستتار.⁴

¹- Pierre catala, les transformations de droit par l'informatique, Emergences du droit de l'informatique, 1983, p264.

مشار إليه لدى :خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، ط1، 2009، ص27.

²- نائلة عادل محمد فريد قورة، المرجع السابق، ص113.

³- محمد سامي الشوا، المرجع السابق، ص157.

⁴- نائلة عادل محمد فريد قورة، المرجع السابق، ص114.

ثالثا: الاستثناء

تعد خاصية الاستثناء بالمعلومة أمرا ضروريا وهاما، والسبب في ذلك أنه في جميع الجرائم التي تنطوي على اعتداء قانوني على الأموال، فإن الفاعل يعتدي على حق الغير على سبيل الاستثناء، ويتوافر للمعلومة هذه الصفة ، إذا كان الوصول إليها غير مصرح به إلا لأشخاص محددين.¹

الفقرة الثالثة: أنواع المعلومات

تقسم المعلومات إلى ثلاثة طوائف هي:

أولا: المعلومات الإسمية

هي التي تتضمن المعلومات المرتبطة بشخص معين كإسمه، موطنه، حالته الإجتماعية، وهي كلها معلومات سرية لا يجوز الإطلاع عليها إلا بموافقتة.

ويرى الأستاذ "كاتالا" "Catala" أنه ليس للغير الحق في الإطلاع على هذه المعلومات، مراعاة للخصوصية ولا يجوز الإطلاع عليها إلا بموافقة صاحبها أو السلطة المختصة، وهناك من عرفها بأنها " تلك البيانات المتعلقة بشخص معين، وليس بالضرورة أن تتعلق بحياتهم الخاصة، بل حتى المتعلقة بحياتهم المهنية أو العامة أو إنتمائهم السياسي أو النقابي".²

ثانيا: المعلومات الخاصة بالمصنفات

هي عبارة عن معلومات متبلورة في شكل مصنفات فكرية، وهذه المصنفات محمية بقوانين الملكية الفكرية، يستوي في ذلك أن تكون تلك القوانين متعلقة بالملكية الأدبية والفنية، أو متعلقة بالملكية الصناعية.³

ثالثا: المعلومات المباحة

يقصد بها تلك المعلومات المتاحة للجميع ويمكن الحصول عليها بسهولة، لأنها بدون مالك مثل

¹- خالد ممدوح إبراهيم، المرجع السابق، ص 60.

²- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الإسكندرية، د ط، 2007، ص 92.

3 - خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص 55.

تقارير البورصة والنشرات الجوية هذه المعلومات مباحة للكافة وغير محمية بأي من وسائل الحماية.¹

الفقرة الرابعة: الطبيعة القانونية للمعلومات

تعتبر المعلومات أساس الثروة المعلوماتية التي نعيشها اليوم، هذه المعلومات كانت غريبة بالنسبة للكثير من القوانين، ولم تكن تعرفها إلا قوانين الملكية الفكرية، لكن مع الوقت بدأت تزداد أهمية هذه المعلومات في حياة الناس²، حيث أصبح للمعلومات في الوقت الحالي أسواق تجارية تخضع لقوانين السوق الإقتصادية، وبدأت تفرض نفسها كسلعة لا غنى عنها³، لهذا ثار التساؤل حول الطبيعة القانونية للمعلومة محل الجريمة الإلكترونية، هل تعتبر من قبيل المال أو لها طبيعة خاصة؟، لهذا انقسم الفقه للإجابة على هذا التساؤل إلى مذهبين أو اتجاهين سوف نتناول كلاهما.

أولاً: المعلومات لها طبيعة من نوع خاص

يرى أنصار هذا الاتجاه إن إدراج المعلومات ضمن القيم المالية التي يمكن الإعتداء عليها، لأن هذه القيم يجب أن تكون قابلة للتملك، ويترتب على ذلك أن المعلومات نظراً لما تتميز به من طبيعة معنوية لا يمكن الاستئثار بها، ولا تندرج في مجموعة القيم المحمية، لهذا يمكن إدراجها في نطاق حقوق الملكية الأدبية أو الذهنية أو الصناعية، ولا يمكن أن تكتسب وصف القيمة إلا في هذا الإطار، ومع ذلك لا ينكر أنصار هذا الاتجاه ما للمعلومة من قيمة إقتصادية، وهو ما أدى بالبعض إلى إدخال المعلومات في عداد الحقوق المالية، مع استبعادها من طائفة القيم المالية وإعتبارها كخدمة أو منفعة تقوم بالمال.⁴

وقد اختلف الفقهاء في هذا الاتجاه التقليدي في تبرير العقاب، الذي يمكن أن يترتب على الإستلاء غير المشروع على معلومات الغير على الوجه التالي:

ذهب الرأي الأول إلى القول أن أساس العقاب، هو المنافسة غير المشروعة التي ترى أن أساس الخطأ هو الظروف التي اقترنت بهذا الإستيلاء، التي تتمثل في عدم القدرة على الإستئثار بالشيء،

1 - عبد الله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، دار النهضة العربية، القاهرة، د ط، 2001، ص161.

² - محمد خليفة، المرجع السابق، ص96.

³ - نائلة عادل محمد فريد قورة، المرجع السابق، ص110.

⁴ - رشيدة بوكري، المرجع السابق، ص، ص، 90 - 91.

مستندا في ذلك إلى حكم محكمة النقض الفرنسية¹، التي أعلنت فيه أن الغاية من دعوى المنافسة غير المشروعة هي تأمين حماية الشخص الذي لا يمكن أن ينتفع بأي حق استثنائي.

بالرغم أن الدائرة التجارية لمحكمة النقض الفرنسية رأت عدم توافر الخطأ الذي يستوجب التعويض في هذا الحكم لعدم توافر شروط قبول دعوى المنافسة غير المشروعة التقليدية²، وقد حاول الأستاذ Letourneau أن يبرز الخطأ المعترف به وفقا لهذا الحكم إستنادا إلى التطبيق الواسع لنظرية التصرفات الطفيلية، وهذا لا يتعارض مع الإقرار بحق الإستثناء على المعلومة.³

فيما ذهب إتجاه آخر يتزعمه الأستاذ "Lucas" حيث حاول تبرير الخطأ على أساس نظرية الإثراء بلا سبب باعتباره تطبيقا خالصا وبعيدا عن المنافسة غير المشروعة.

وقد رأت محكمة النقض الفرنسية إن الإستعانة بفكرة الخطأ لكي تعترف بالحق في احترام الحياة الخاصة، ويبدو أن هذا الحكم أقر بوجود الخطأ، ليس على أساس المنافسة غير المشروعة، وإنما على أساس المسؤولية التقصيرية، وبذلك يكون قد أقر بوجود حق على المعلومات.

وفي الأخير انتهت هذه الآراء الفقهية في مضمونها على وجود حق على المعلومات المستولي عليها، ولكن لهذا الحق طبيعة من نوع خاص، إذ الأصل أن الأشياء القابلة للاستحواذ والتي يمكن الإستثناء بها هي التي يكون لها قيمة مادية.⁴

ثانيا: المعلومات مجموعة مستحدثة من القيم

إن الإنتشار الواسع للمعلومات خاصة وبصورة كبيرة في مجال المعاملات التجارية، مما أدى في بعض الأحيان إلى إرتفاع قيمتها عن الأموال المادية، مما دفع بالفقه الحديث البحث عن معيار آخر والمتمثل في معيار القيمة الإقتصادية للشيء⁵، يذهب هذا الإتجاه الفقهي إلى اعتبار المعلومات قيمة

¹ - وقد صدر هذا الحكم في 3 أكتوبر 1978، بخصوص الاستعمال بغير حق لأفكار الغير حيث تمكنت إحدى المؤسسات من التعرف على أفكار تقنية توصل إليها شخص كان يفوضها ولم يقم بتسجيلها بعد، لم تسفر هذه المفاوضات عن إبرام العقد بينهما ورغم هذا فقد استغلت هذه المؤسسة تلك الأفكار في عملها.

² - أحمد خليفة الملط، المرجع السابق، ص124.

³ - محمد سامي الشوا، المرجع السابق، ص161.

⁴ - أحمد خليفة الملط، المرجع السابق، ص125.

⁵ - رشيدة بوكري، المرجع السابق، ص92.

تضاف إلى غيرها من القيم الأخرى، ولقد تبنى هذا المعيار جانب من الفقه الفرنسي وعلى رأسهم كاتالا Pierre Catala وميشال فيفانت Michel Vivant.

يرى الأستاذ كاتالا Catala إلى أن المعلومة قابلة للاستحواذ كقيمة واستقلال عن دعامتها المادية، وذلك لأنها تقوم وفقا لسعر السوق متى كانت غير محصورة تجاريا، وأنها منتج بصرف النظر عن دعامتها المادية وعن عمل من قدمها، وأنها ترتبط بمؤلفها عن طريق علاقة قانونية تتمثل في علاقة المالك بالشئ الذي يملكه، وهي تخص مؤلفها بسبب علاقة التبني التي تجمع بينهما¹، ويستند Catala على حجتين أساسيتين لإضفاء وصف القيمة على المعلومة، أولهما قيمتها الإقتصادية، مستندا إلى رأي الأستاذ Carbonnier الذي تبنى في دراسته صلة القيمة بدعامتها المادية، حيث أشار إلى أن " الجوهر على قدر كبير من الأهمية في مجال المنفعة الإقتصادية بالمقارنة بنظره في مجال البيانات المادية، وأنه من الواضح أن أي قانون يرفض أن يرى قيمة في شيء له أهمية إقتصادية سيقى حتما بمعزل عن الحقيقة"، ومن المقبول إذن وفقا لأهمية المعلومة وعلى نحو ما أشار إليه الأستاذ كاتالا أن ينطبق وصف القيمة عليها.²

والثانية علاقة التبني من شأنها أن تعطي الحق لصاحب المعلومة من حيازتها لأنها بين الأشياء القابلة للتملك وأقلها عرضة للاعتداء هي نتاج الذهن بدون منازع.³

وعليه فإذا ما وضع في الاعتبار الرابطة التي تجمع المعلومة بمؤلفها فيجوز إذا الإقرار بمكنة حيازتها بوصفها قيمة وفقا لهذا التصور⁴، وأن المعلومات التي ترتبط بشخص صاحبها يكون لهذا الأخير حق في أن لا ينقلها لغيره، وهذا النوع من المعلومات هو الجدير بالحماية⁵.

أما الأستاذ Vivant يتفق مع الرأي السابق، وأسس اتجاهه على حجتين، الأولى مستمدة من رأي Ripert و Planion ومضمونها " إن فكرة الشئ أو المال والذي يغلب عليه الطابع المعنوي وأن صفة محل الحق معنوية يجوز أن يستند إلى مال معنوي بحيث يكون هذا المال من قبيل الأموال الإقتصادية وأنه جدير بحماية القانون."⁶

¹ - محمد علي العريان، المرجع السابق، ص 50.

² - أحمد خليفة الملط، المرجع السابق، ص 127.

³ - محمد سامي الشوا، المرجع السابق، ص 163.

⁴ - أحمد خليفة الملط، المرجع السابق، ص 127.

⁵ - محمد خليفة، المرجع السابق، ص 49.

⁶ - عبد الله حسين علي محمود، المرجع السابق، ص 170.

الحجة الثانية أن كل الأشياء المملوكة ملكية معنوية، والتي يحميها القانون تقوم على اعتراف مسبق بأن المعلومات قيمة، عندما تكون أمام براءات الاختراع والرسوم أو حتى حق المؤلف، وأن الشخص الذي يقدم المعلومات بغض النظر على الشكل أو الفكرة فهو يقدم المعلومات بالمعنى الواسع، ويصل الأستاذ Vivant إلى أن "المعلومات بوصفها قيمة تقع في المضمون" قواعد القانون الوضعي، ويستخلص Vivant أن المعلومات قيمة نتيجة لأهميتها الاقتصادية¹، وقد إنتهى هذا الفقيه إلى القول أن المعلومات قد تكون محلا لعقد البيع ويمكن نقل منفعتها واستغلالها، وهي فكرة التبني أو علاقة الارتباط التي طرحها الأستاذ Catala هي أن المعلومات ترتبط بمن أنتجها وأبتدعها، ولهذا الأخير أن يتنازل عنها بعقد أو يتوقف عن استعمالها.

وعليه نخلص إلى أن المعلومة بوصفها قيمة، فهي تتدرج تحت القيم المستحدثة وتصبح بذلك قيمة معلوماتية، وتتدرج تحت الملكية التي تعتبر لها قيمة قانونية والاستيلاء عليها يستوجب العقاب.²

وفي الأخير يقول الأستاذ محمد سامي الشوا، أن المعلومة وبالنظر إلى حقيقتها الذاتية واستقلالها، تعد قيمة في ذاتها ولها مظهرها المعنوي، ولها قيمة اقتصادية مؤكدة وهذه القيمة ترفعها إلى مصاف القيم القابلة لأن تحاز حياة مشروعة، إستنادا إلى ما إستند عليه الأستاذ كاتالا Catala من أن المعلومة ترتبط بصاحبها بسبب علاقة الأبوة أو التبني التي تربط بينهم.³

وبناء على ما سبق وإستنادا إلى الحجج والآراء التي قبلت حول الطبيعة القانونية للمعلومات، فإننا نؤيد الإتجاه الحديث القائل بأن المعلومات عبارة عن مجموعة قيم مستحدثة، لأن التطور الحديث للمعلوماتية أدى إلى إضفاء قيمة إقتصادية للمعلومة تتمثل في قيمتها التجارية، لهذا يجب معاملتها على أنها مال، وهذا ما تبنته كل الدول والدليل على ذلك سعي هذه الدول، إلى حماية هذه المعلومات من الناحية القانونية، ومن بينها المشرع الجزائري الذي يقر لصاحب هذه المعلومات بالحق في الملكية الذهنية والأدبية، وإعتبار المعلومات مالا.

¹ - نائلة عادل محمد فريد قورة، المرجع السابق، ص120.

² - بن مكي ناجة، المرجع السابق، ص30.

³ - محمد سامي الشوا، المرجع السابق، ص156.

الفرع الثاني: أركان الجريمة الإلكترونية

تعد أركان الجريمة الأساس والأصل لقيام أي جريمة، والمشرع يتطلب لقيام الجريمة توافر أركانها المادي والمعنوي، وبدون هذين الركنين لا تقوم الجريمة، وهذا هو الحال بالنسبة للجرائم الإلكترونية، ولقيام الجريمة الإلكترونية لابد من أن يتوافر فيها أركان الجريمة، ويتمثل في الركن الشرعي وهو نص التجريم الواجب التطبيق على الفعل، أو بعبارة أخرى هو النص القانوني الذي يبين الفعل المكون للجريمة ويحدد العقاب الذي يفرضه على مرتكبها¹ (الفقرة الأولى) والركن المادي ويتمثل في النشاط الذي يرتكبه الجاني (الفقرة الثانية) أما الركن المعنوي إتجاه الإرادة الخاطئة لمباشرة السلوك الإجرامي² (الفقرة الثالثة) وسوف نوضح هذه الأركان كما يلي:

الفقرة الأولى: الركن الشرعي للجريمة الإلكترونية

يعد التشريع المصدر الأساسي للتجريم والعقاب، كما أن صلاحية القاضي الجنائي محدودة بالنص التشريعي فهو لا يملك صلاحية إكمال تشريع ناقص، أو إستبدال العقوبة، أو حتى تفسير القاعدة القانونية، أو خلق نص تشريعي وذلك لضمان إرساء قواعد العدالة³، وبذلك فإن مبدأ عدم المشروعية لا يتوافر بمجرد الإعتداء على مصلحة إجتماعية أيا كانت أهميتها ما لم يكن المشرع قد نص صراحة على تجريم هذا الإعتداء وذلك تطبيقاً لمبدأ "لا جريمة ولا عقوبة إلا بالنص" الذي تضمنته جميع دساتير العالم. فإذا كانت الجرائم الإلكترونية من الجرائم التي رافقت التطور التكنولوجي الذي طرأ على العالم، فنجد أغلب قوانين العقوبات تخلو من نصوص عقابية لهذا النوع من الإجرام⁴، لذلك إستقر الفكر القانوني على ضرورة وجود نصوص قانونية خاصة لمواجهة الجرائم الإلكترونية، خاصة بعد ظهور شبكة الأنترنت التي ساهمت كثيراً في إنتشارها، حيث بادر المجلس الأوروبي عام 1989 من خلال وضع توصية من أجل

¹ - عبد الله سليمان، شرح قانون العقوبات الجزائري، القسم العام، الجزء الأول "الجريمة"، ديوان المطبوعات الجامعية، الجزائر، 1995، ص 68.

² - أحمد فتحي سرور، الوسيط في قانون العقوبات الجزء الأول القسم العام، دار النهضة العربية، القاهرة، 1981، د ط، 256.

³ - نداء نايل فايز المصري، خصوصية الجرائم المعلوماتية، مذكرة لنيل شهادة الماجستير في الحقوق، كلية الدراسات العليا، جامعة النجاح، نابلس، فلسطين، 2017، ص 12.

⁴ - طالب محمد جواد عباس، عبد الجبار ضاحي عباس، جرائم تقنية المعلومات وإثباتها، ص 8.

حث الدول على سن تشريع يخص الجريمة الإلكترونية،¹ واختلفت الدول في مواجهة هذه الجريمة، أو في طريقة معاملتها مع الظاهرة الإجرامية، فهناك أشكال وأنماط تشريعية قد يلجأ إليها المشرع:

-الإضافة وذلك من خلال قيام المشرع بإضافة السلوك الإجرامي بواسطة الحاسب الآلي إلى النصوص التقليدية، أو يضيف إلى محل النشاط الإجرامي المعلومات التي يحتويها نظام الحاسب الآلي كما في نصوص جريمة السرقة.

-وضع نصوص جديدة بالقياس مع النصوص التقليدية، حيث يتحول النص من صورته التقليدية إلى صورة أخرى، لكنه مرتبط بالحاسوب ونظامه، و أغلب هذه الدول تتبع هذه الطريقة.

- تجميع كل ما يتعلق بالجريمة الإلكترونية في قسم مستقل ملحق بالتشريع الجنائي، أو في تشريع مستقل، وقد تبنت الولايات المتحدة الأمريكية هذا الاتجاه.

- وضع قانون خاص يعالج كل مل يتعلق بالجريمة الإلكترونية سواء الجانب الموضوعي أو الإجرائي.²

وبناء على ذلك يمكن اعتماد كل دولة نمطا تشريعيا بما يتلاءم مع طبيعة النظام القانوني لها،³ إذ تعتبر الدول الأوروبية وأمريكا السبابة في سن قوانين تشريعية لمكافحة الجريمة الإلكترونية، فنجد السويد في طليعة الدول التي سنت أول قانون لها سنة 1973، و تلتها الولايات المتحدة الأمريكية بوضع قانون سنة 1976، كما قام المشرع الفرنسي بسن نصوص خاصة تتعلق بالإجرام المعلوماتي سنة 1986، وعلى هذا النهج سارت فيما بعد بعض الدول الأجنبية منها أو العربية ومن بينها المشرع الجزائري الذي أصدر القانون رقم 04-15 المؤرخ في 2004/11/10،⁴ لسد ما كان من فراغ قانوني في هذا المجال، وذلك من خلال تعديل قانون العقوبات وفي القسم السابع مكرر نص على الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، في المواد من 394مكرر الى 394 مكرر7، كما صدر نظام مكافحة الجرائم الإلكترونية في المملكة السعودية عام 2007 وتم تعديله سنة 2015، قانون مكافحة جرائم تقنية المعلومات الكويتي رقم 63 لسنة 2015، وكذا قانون الجرائم الإلكترونية الفلسطيني لسنة 2017.

1 -آمال قارة، الحماية الجنائية للمعلوماتية في التشريع الجزائري، دار هومة، الجزائر، ط2، ، ص37.

² -نداء نائل فايز المصري، المرجع السابق، ص 14.

³ - نداء نائل فايز المصري، المرجع نفسه، ص 14.

⁴ -القانون رقم 04-15 المؤرخ في 2004/11/10، يعدل ويتم الأمر 66-156 المتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، عدد 71، الصادرة بتاريخ 2004/11/10.

الفقرة الثانية: الركن المادي

يعد الركن المادي الوجه الظاهر للجريمة وبه يتحقق الإعتداء على المصلحة المحمية قانوناً، إذ تتجسد من خلاله الأعمال التنفيذية للجريمة، ويقصد بالركن المادي للجريمة، هو تجسيد للحالة النفسية والباطنية للفاعل، لأنه ينقل الفكر الباطني إلى العالم الخارجي بماديات الجريمة، فالفعل لا يكتسب الصفة الجرمية المنصوص عليها في القانون، إلا إذا تبلور بعمل مادي ينطبق على المواصفات الجرمية التي نص عليها القانون¹، فالجريمة الإلكترونية كغيرها من الجرائم تتطلب وجود ركن مادي على الهيئة والشكل التي يتطلبها المشرع سواء، من حيث إجتماع عناصره الثلاثة من نشاط أو سلوك مادي وعلاقة سببية ونتيجة إجرامية²، أو أن يكفي بالنشاط أو السلوك المادي فقط.

غير أن تحديد الركن المادي في الجرائم الإلكترونية، تكتنفه العديد من الصعوبات خاصة فيما يتعلق بتحديد النتيجة الإجرامية، وعلاقة السببية وسوف نتطرق لهذه العناصر كما يلي:

أولاً: السلوك الإجرامي

يعد السلوك³ الإجرامي من أهم عناصر الركن المادي، لأنه يمثل القاسم المشترك بين جميع أنواع الجرائم سواء تلك التي يكفي لوقوعها ارتكاب السلوك الإجرامي فقط، أو تلك التي يلزم لقيامها ضرورة تحقق نتيجة إجرامية معينة إلى جانب السلوك.⁴

إن السلوك الإجرامي في الجريمة الإلكترونية مرتبط دائماً بالمعلومة المخزنة على الحاسوب، أو تلك

¹ - معز أحمد محمد الحياوي، الركن المادي في الجريمة، مشورات الحلبي الحقوقية، لبنان، ط1، 2010، ص93.

² - خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص 98.

³ - ويتخذ السلوك الإجرامي إما سلوكاً إيجابياً، أو سلوكاً سلبياً، فالسلوك الإيجابي يصدر عن الفاعل في صورة حركة عضوية إرادية، فالفعل يبدأ بحركة تصدر عن عضو واحد أو أكثر من أعضاء الجسم وهي حركة مادية لأنها انعكاس لحركة عضلية قام بها الفرد، فإذا تكررت هذه الحركة وربطتها وحدة التسلسل كانت عملاً مادياً، فإذا ما اقترن العمل المادي هذا بإرادة اكتملت صورة السلوك أي صورة الفعل، أما السلوك السلبي يتمثل هذا الفعل بسلوك أو موقف يتخذه المكلف بقاعدة قانونية تفرض عليه أن يعمل فلا يعمل، ففي هذه الحالة يقوم المكلف بالحيلولة دون جسمه كله أو بعضه وبين الحركة التي يتطلبها القانون، أو قد يتحرك باتجاه مضاد لما أمر به.

يقوم الفعل السلبي على الامتناع أو إحجام شخص عن القيام بعمل يوجب عليه القانون إذا كان باستطاعته القيام به، وعليه فلا يجوز للقاضي أن يمتنع عن الحكم بالدعوى. أنظر عبد الله سليمان، المرجع السابق، ص، ص 147 - 148.

⁴ - علي القهوجي، قانون العقوبات - القسم العام -، الدار الجامعية للطباعة والنشر، بيروت، د ط، 2000، ص309.

التي يتم إدخالها للحاسوب، وصعوبة المشكلة أن السلوك يتحقق بمجرد ضغط زر على الحاسوب، فيتم تدمير النظام المعلوماتي أو حصول التزوير أو السرقة عن طريق التسلل إلى نظام أرصدة العملاء في البنوك.¹

فالنشاط أو السلوك الإجرامي في الجريمة الإلكترونية، يتطلب أولاً وجود بيئة رقمية، أي ينبغي توفر جهاز حاسوب وشبكة أنترنت للاتصال، ويتطلب أيضاً معرفة بداية هذا النشاط والشروع فيه ونتيجته، فمثلاً يقوم مرتكب الجريمة بتجهيز الحاسوب لكي يرتكب جريمته، عن طريق تحميل الحاسوب ببرامج الاختراق، أو يقوم بإعداد هذه البرامج بنفسه، وكذلك قد يحتاج إلى تهيئة صفحات تحمل في طياتها مواد مخلة بالأداب العامة وتحميلها على الجهاز المضيف، كما يمكن أن يقوم بجريمة إعداد برامج فيروسات تمهيداً لبثها.²

و يؤثر السلوك المادي المرتكب عبر شبكة الأنترنت عدة تساؤلات، منها ما يتعلق ببداية السلوك الإجرامي وكذا الشروع في ارتكاب الجريمة، وهذا النشاط يختلف عما هو عليه الحال في العالم المادي، فارتكاب الجريمة الإلكترونية يحتاج إلى منطق تقني، أي جعل مسألة استخدام الحاسوب والأنترنت جزءاً من النشاط المادي في هذه الجرائم، وبدونه لا يمكن للشخص أن يتصل بالأنترنت سواء بقصد ارتكاب الجريمة أو مجرد التصفح أو الدخول في الاتصال كالمحادثة وغيرها.³

إن السلوك المادي الإيجابي المتمثل في المنطق التقني يجعل الجريمة الإلكترونية ذات طابع موحد بالضرورة، فهي تجعل من هذا السلوك أحد عناصر الركن المادي، يضاف إلى فلسفة الركن المادي في الجريمة، وقد أدركت التشريعات المقارنة هذا الأمر حين النص على جرائم يمكن أن ترتكب عبر الحاسب الآلي، حيث استعمل المشرع نصوص يقرر صراحة عبارة ... إذا ارتكبت الجريمة باستخدام الكمبيوتر أو عبارة ... باستخدام المعالجة الآلية للبيانات ... إلخ⁴، وهذا ما أقره المشرع الجزائري من خلال الجرائم

¹ - عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والأنترنت، -دراسة متعمقة في جرائم الحاسب الآلي والأنترنت، بهجات للطباعة والتجليد، مصر، د ط، 2009، ص، ص، 113-114.

² - نداء نائل فايز المصري، المرجع السابق، ص16.

³ - عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الأنترنت، دار النهضة العربية، القاهرة، د ط، 2004، ص253.

⁴ - عبد الله دغش العجمي، المشكلات العملية والقانونية للجرائم الإلكترونية - دراسة مقارنة، رسالة لنيل شهادة الماجستير في القانون، جامعة الشرق الأوسط، 2014، ص28.

الواردة في قانون العقوبات في القسم السابع مكرر والتي تشمل المواد 394 مكرر إلى 397 مكرر 7 بإستعمال عبارات ... كل من يدخل ... منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك ... و... نظام المعالجة الآلية ...".

وبهذا يعتبر النشاط التقني أمراً لازماً وإلا فقدت الجريمة مقوماتها، وإن وصف الجريمة بالطابع التقني، مما يمكن أن يجعل هذه الجرائم المرتكبة بواسطة الحاسوب وشبكة الأنترنت، من نوعية جرائم الوسيلة، ومع ذلك فإن هذا الأمر لا يمكن قبوله على الإطلاق لسبب جوهري هو مشروعية هذا الوسيط، الذي يستخدم في الجريمة.¹

ثانياً: النتيجة في الجريمة الإلكترونية

تمثل النتيجة الإجرامية العنصر الثاني من عناصر الركن المادي، فقد اتفق الفقهاء على أن المقصود بالنتيجة هي الأثر الخارجي للسلوك الذي يتمثل في الإعتداء على حق يحميه القانون، سواء كان هذا الحق لفرد أو لمجتمع²، وتثير النتيجة الإجرامية في الجريمة الإلكترونية مشاكل عدة من بينها مكان وزمان تحقق النتيجة الإجرامية، فمثلاً لو قام أحد المجرمين في أمريكا باختراقه جهاز خادم Server أحد البنوك في الإمارات العربية، وهذا الجهاز موجود في الصين، فكيف يمكن معرفة وقت حدوث الجريمة هل هو توقيت بلد المجرم، أو توقيت بلد البنك المسروق أم توقيت الجهاز الخادم في الصين وهذا ما يثير اشكاليات القانون الواجب التطبيق³، مما أعطى للجرائم الأثر ذا البعد الدولي⁴، وهو امتداد أثر النتيجة الإجرامية فقط، سواء في شكل إمتداد الضرر أو الخطر إلى ما يتجاوز الحدود الإقليمية التي وقع فيها السلوك وبعض النتيجة، ويأخذ هذا الإمتداد شكل العدوان المحدد على مصلحة أو مصالح قائمة

¹ - خالد إبراهيم ممدوح، الجرائم المعلوماتية، المرجع السابق، ص 100.

² - عبد المالك جندبي، الموسوعة الجنائية، - الجزء الرابع-، مركز الأبحاث والدراسات القانونية، د م ن، د ط، 2006، ص 8.

³ - محمد علي قطب، الجرائم المعلوماتية ومواجهتها، الجزء الثاني، الأكاديمية الملكية للشرطة، وزارة الداخلية، البحرين، ص 3، أطلع عليه يوم 2017/05/26، منشور على الموقع: www.policemc.Giv.Bh/Reports.

⁴ - إن الأثر ذا البعد الدولي يختلف بالضرورة عن الجريمة ذات البعد الدولي، فالأخيرة يعرفها القانون المقارن كما هو الشأن في الاتجار غير المشروع، في المخدرات، والأطفال والارهاب، ويختص قانون العقوبات الاقليمي والاتفاقيات الدولية بتجريمها واقرار العقاب عليها، وهي عبارة عن جرائم عابرة للحدود لذلك نقرر اعتبارها جرائم ذات بعد دولي. للمزيد أنظر عمر أبو بكر بن يونس، المرجع السابق، ص 272.

ومشروعة في دولة أو دول متعددة، وهذا راجع لكون السلوك المرتكب في العالم الافتراضي من طبيعة إمتدادية يجعل النتيجة أو جزء من النتيجة متحققا في العالم الافتراضي أولا، ولما كان العالم المادي ككل متصلا بالعالم الافتراضي فإنه من الطبيعي أن يكون هذا الاتصال حادثا في أي مكان فيه¹، كما تثير النتيجة الإجرامية كذلك إشكالية أخرى تتمثل في صورة النتيجة المحتملة، حيث يترتب كنتيجة على النشاط الإجرامي أكثر من نتيجة لا يسعى الجاني إلا لتحقيق صورة واحدة منها، يتوقعها ويريدها أن تترتب عن نشاطه أو سلوكه المادي، والنتيجة المحتملة هي نتيجة إضافية للنتيجة التي يسعى الجاني لتحقيقها، وفكرة النتيجة المحتملة تنتشر كثيرا في الجرائم الإلكترونية، وذلك بسبب أن النشاط التقني له منطوق واسع المجال يمكن أن تترتب عليه عدة نتائج، فمن يقصد القرصنة تتحقق مع القرصنة إنتشار فيروسات، نتيجة لوجود دفاع فيروسي في البرمجية، وكذلك تخريب البرمجية المقصود إرتكاب القرصنة عليها، فمثل هذا السلوك الإجرامي تتحقق مع النتيجة الأصلية وهي الشروع في القرصنة، إلى جانب نتائج أخرى يبدو الإحتمال واضح في حدوثها كنتائج إلا أنها ليست من النتائج المقصودة من النشاط الاجرامي.²

ثالثا: علاقة السببية

يلزم لقيام الركن المادي أن تتوافر علاقة السببية بين السلوك الإجرامي والنتيجة الجرمية، وذلك بأن يثبت أن هذا السلوك هو سبب تلك النتيجة، أي أن إرتكاب هذا السلوك هو الذي أدى إلى حدوث النتيجة، كذلك فإن علاقة السببية تساهم في تحديد نطاق المسؤولية الجزائية، واستبعاد المسؤولية إذا لم ترتبط النتيجة الجرمية بالفعل³. أما في نطاق الجرائم الإلكترونية فإن علاقة السببية أساسية لقيام جميع أنواع الجرائم الإلكترونية، فهي عنصر أساسي من عناصر الركن المادي لأي جريمة إلكترونية، وتقوم العلاقة السببية في الجرائم الإلكترونية على البحث في الصلة بين مرتكب الجريمة والفعل الذي ارتكبه وبين الآلة، فالعلاقة التقنية بين مرتكب الجريمة، وبين الآلة محل الجريمة الإلكترونية هي الأساس لبيان رابطة السببية في الجرائم الإلكترونية.⁴

¹ - عمر محمد أبو بكر بن يونس، المرجع السابق، ص274.

² - عمر محمد أبو بكر بن يونس، المرجع نفسه، ص275.

³ - محمد صبحي نجم، قانون العقوبات -القسم العام (النظرية العامة للجريمة)، دار الثقافة للنشر والتوزيع، ط4، 2012، ص211.

⁴ - لورنس سعيد الحوامدة، الجرائم المعلوماتية أركانها وآلية مكافحتها -دراسة تحليلية مقارنة-، مجلة الميزان للدراسات الإسلامية والقانونية، المجلد 4، العدد 1، 2017، ص206.

الفقرة الثالثة: الركن المعنوي¹ للجريمة الإلكترونية

الجريمة بشكل عام ليست ظاهرة مادية خالصة قوامها الفعل وآثاره، ولكنها كذلك كيان نفسي، ومن ثم استقر في القانون الجنائي الحديث ذلك المبدأ الذي يقضي بأن ماديات الجريمة لا تنشأ مسؤولية، ولا تستوجب عقاباً ما لم تتوافر إلى جانبها العناصر النفسية التي يتطلبها كيان الجريمة، وتجتمع هذه العناصر في ركن مختص، يحمل إسم الركن المعنوي للجريمة²، يكتسي الركن المعنوي أهمية بالغة في الجريمة الإلكترونية كما هو الحال في الجريمة المرتكبة في العالم المادي، حيث بموجبه يمكن تحديد نطاق مسؤولية الجاني، وذلك بتحديد القصد الجنائي لديه، الذي بدونه لا يمكن معاقبة الشخص المرتكب للفعل.

تفترض الجرائم الإلكترونية وجود القصد الجنائي العام، المتمثل في العلم والإرادة لتحديد المسؤولية الجنائية، فالعلم هو إدراك الفاعل للسلوك المجرم، أما الإرادة هي اتجاه السلوك الإجرامي لتحقيق النتيجة، إذن فالقصد الجنائي متوافر في جميع الجرائم الإلكترونية دون استثناء، فقد يأخذ الإعتداء على الحاسب الآلي صورة العمد وسوء النية، ويتمثل في أفعال السرقة والنصب المعلوماتي وخيانة الأمانة، والتزوير وإتلاف المال المادي من الحاسوب من شاشات وكابلات ولوحة المفاتيح، والأقراص والبطاقات الممغنطة، أو إتلاف المال المعنوي من الحاسوب من البرامج والنظم التطبيقية ... الأمر الذي يترتب عليه خسائر جسيمة، من ذلك على سبيل المثال ما حدث في أحد البنوك الفرنسية، إذ أدى إتلاف نظام الشبكات الخاص به إلى تأخير معالجة البيانات آلياً وقدرت الخسارة الناشئة عن ذلك بمليوني فرك فرنسي³، ومن المتصور غالباً أن لا تقع الجريمة الإلكترونية، إلا بصورة عمدية سبقها التفكير في الحصول على المعلومة بإختراق شبكة حاسوب آخر من أجل الحصول على المنفعة أو تحقيق المخطط له.

أما فيما يخص وجود القصد الخاص في الجريمة الإلكترونية، فيرجع بالدرجة الأولى إلى طبيعة الجريمة المرتكبة والنية الخاصة لدى الجاني من وراء القيام بالفعل غير المشروع أو ارتكاب الجريمة،

¹ - ويطلق عليه الركن الأدبي أو الشخصي، وهو يعني في الحقيقة الجاني، المجرم تحديداً، فالركن المعنوي هو المسلك الذهني أو النفسي للجاني باعتباره محور القانون الجنائي، ذلك أنه في إطار الركن المعنوي تتوافر المسؤولية الجنائية من إسناد وإذئاب مع إقرار حق الدولة في العقاب، أنظر : عمر محمد أبو بكر بن يونس، المرجع السابق، ص 287.

² - محمود نجيب حسن، النظرية العامة للقصد الجنائي، -دراسة تأصيلية مقارنة في الجرائم العمدية-، دار النهضة العربية، القاهرة، ط2، 1971، ص1.

³ - بلال أمين زين الدين، جرام نظم المعالجة الآلية للبيانات في التشريع المقارن والشريعة الإسلامية، دار الفكر الجامعي، الاسكندرية، ط1، 2008، ص31.

فيرى جانب من الفقه، أن القضاء الأمريكي لم يستقر على حال بالنسبة لبعض الجرائم التي ترتكب بإستخدام الأنترنت من حيث مدى تحديد ما إذا كانت تتطلب قصدا عاما أو خاصا¹، أما القضاء الفرنسي فإن منطق سوء النية يغلب على النصوص التي تطبق بشأن الجرائم الإلكترونية، حتى أن هذه الجرائم لا يمكن أن تدخل حيز التطبيق ما لم يتوافر على سوء النية في منطق القصد الخاص وإرادة الإضرار² ومن ذلك ما هو مقرر في المادة 15/226 من قانون العقوبات الفرنسي³، كجريمة السرقة التي يفترض لإثباتها توافر قصد جنائي خاص والذي يعبر عن بنية التملك، فهي التي تكشف نية الجاني في حيازة الشيء المعلوماتي، ويستدل على توافر القصد من القرائن والظروف، ونية التملك التي تتجه إليها إرادة الجاني هي عنصر يضاف إلى عنصر في القصد العام (العلم والإرادة)، فبالإضافة إلى ضرورة إتجاه الإرادة إلى إختلاس الشيء المعلوماتي، مع علم الجاني أنه يختلس شيئا مملوكا للغير، يضاف إليهما عنصر نية الإستيلاء على الشيء المسروق وهي المعلومة أو البرنامج المخزن في الحاسوب⁴، وقد تباينت التشريعات المختلفة في إشتراط القصد الجنائي الخاص، هذا وسنحاول التطرق حين دراسة كل جريمة على حدة.

وخلاصة القول أن الجرائم الإلكترونية كالجرائم التقليدية، يشترط وجود أركان الجريمة المتمثلة في الركن المادي والمعنوي، ولكن طبيعتها الخاصة جعلت أركانها تتميز كذلك بهذه الصفة.

الفرع الثالث: الشروع

إن كانت العلة من العقاب على أي جريمة، هي أنها تحقق عدوانا على المصالح محل الحماية القانونية، فإن العلة من العقاب على الشروع بوصفه جريمة، لا بد أن تتمثل في تحقيق ذلك العدوان الذي يأخذ في الشروع صورة الخطر المهدد للمصالح القانونية فهو بمثابة إعتداء محتمل⁵، فالمرشح لا يحمي المصالح القانونية من الضرر الذي ينزل بها فيقضي عليه جزء أو كل فحسب، وإنما يوفر لها حماية إزاء

¹ - لورانس سعيد الحوامدة، المرجع السابق، ص 207.

² - خالد ممدوح إبراهيم، المرجع السابق، ص 110.

³ - Art 226/15 du code pénal français

"Le fait commis de mauvaise foi, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressés à des tiers, ou d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 4500 euros d'amende.

Et puni des mêmes peines le fait, commis de mauvaise foi d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser des telles interceptions.

⁴ - خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، دار الجامعة الجديدة، الإسكندرية، د ط، 2008، ص 107.

⁵ عبد الله سليمان، المرجع السابق، ص 146 .

الخطر الذي يهددها باحتمال القضاء عليها، وإذا كانت الجريمة لا تكتمل إلا بتوافر فعل مادي، فانه ليس من الضروري أن يترتب على هذا الفعل نتيجة ضارة حتى تكون الجريمة ويعاقب عليها، فإن تحققت النتيجة نكون بصدد الجريمة التامة، وإذا لم تتحقق نكون بصدد الشروع¹، والشروع هو " البدء في فعل أو أفعال ترمي مباشرة إلى ارتكاب الجريمة ولكن يحول دون تمامها ظروف خارجية عن إرادة الفاعل"²، وكذلك الشروع هو البدء الفعلي في الجريمة وهي مرحلة تأتي بعد مرحلة التخطيط والتحضير وقبل تمام الجريمة، فالجاني بدأ في تنفيذ الجريمة دون أن يكملها لأسباب خارجة عن إرادته³.

ويعد الشروع كالجريمة التامة، فنجد أغلب التشريعات تعاقب عليه في نصوصها العقابية، ومن بينها المشرع الجزائري الذي نص عليه بموجب المادة 30 من قانون العقوبات الذي جاء فيه " كل محاولات لارتكاب جناية تبتدئ بالشروع في التنفيذ أو بأفعال لا لبس فيها تؤدي مباشرة إلى ارتكابها تعتبر كالجناية نفسها إذا لم توقف أو لم يخب أثرها إلا نتيجة لظروف مستقلة عن إرادة مرتكبها حتى ولم يكن بلوغ الهدف المقصود بسبب ظرف مادي يجهله مرتكبها"⁴، أما في مواد الجناح لا يعاقب المشرع على الشروع إلا بنص، ولا يعاقب على الشروع في مواد المخالفات، إذ تنص المادة 31 من ق.ع.ج على " المحاولة في الجناية لا يعاقب عليها إلا بناء على نص صريح في القانون والمحاولة في المخالفة لا يعاقب عليها إطلاقاً".

أما بخصوص الجرائم الإلكترونية ، فقد نصت كل من إتفاقية بودابست و الإتفاقية العربية على العقاب في الشروع في المادة 11 منه⁵، وكذا المادة 19 المتعلقة بالاشتراك والشروع ضمن الفصل الثاني المتعلق بالتجريم، والتي جاء نصها كما يلي " ... الشروع في ارتكاب الجرائم المنصوص عليها في الفصل

¹ - رشيدة بوكري، المرجع السابق، ص- ص، 350، 351.

² - نجاة بن مكي، المرجع السابق، ص 207.

³ - جلال ثروت، قانون العقوبات - القسم العام-، الدار الجامعية، بيروت، ط1، د س ن، ص173.

⁴ - تقابلها المادة 45 من ق.ع. المصري، المادة 199 من قانون العقوبات السوري، المادة 68 من ق.ع. الأردني، والمادة 1/30 من ق.ع. الفلسطيني.

⁵ - Art ; 11 Tentative et complicité

1-« chaque partie adopte les mesures législatives et autres qui se relèvent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute complicité lorsqu'elle est commise internationalement en vue de la perpétration d'une des infractions établies en application des 2 à 10 de présente convention dans l'intention qu'une telle infraction soit commise.

2- chaque partie adopte les mesures législatives et autres qui se relèvent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute tentative intentionnelle de commettre l'une des infractions établies en application des articles 3 à 5, 7, 8, 9 (1) a et 9 (1) de la présente convention. »convention européenne de la cybercriminalité.

الثاني من هذه الإتفاقية ... " ولم يخرج المشرع الجزائري من نظام العقاب الذي رسمته القوانين الدولية، حيث نص في المادة 394 مكرر 7 من القسم السابع من قانون العقوبات على أنه " يعاقب على الشروع في إرتكاب الجرح المنصوص عليها في هذا القسم مكرر بالعقوبات المقررة للجنة ذاتها"، وبما أن لا عقاب على الشروع في الجرح إلا بنص، نجد المشرع الجزائري وسع من نطاق العقوبة لتشمل قدرا كبيرا من الأفعال الماسة بالأنظمة المعلوماتية، وجعل الشروع في إحدى هذه الجرائم معاقبا عليه بنفس العقوبة الخاصة بالجريمة التامة.

ويقوم الشروع على ركنين هما الركن المادي والركن المعنوي

أولاً: الركن المادي

لقيام الركن المادي في الشروع في الجرائم الإلكترونية، لابد من توافر عنصرين هما البدء في التنفيذ وعدم إتمام الجريمة لظروف خارجة عن إرادة الفاعل.

وغالبا ما يطرح التمييز بين المرحلة التحضيرية، ومرحلة البدء في التنفيذ إشكالا في الفصل بينهما، فتجهيز البرامج أو إدخال شيفرة غير صحيحة كل ذلك يعتبر أعمالا تحضيرية تسبق البدء في التنفيذ، كما أن البدء في التنفيذ يجب أن يكون أحد مكونات السلوك الإجرامي للجريمة، فالدخول إلى نظام غير مصرح به يعد بحد ذاته جريمة تامة، حتى ولو كانت في بدء تنفيذ جريمة أخرى، وهذا قد يحدث في كثير في الجرائم الإلكترونية، وعليه فإن البدء في تنفيذ الجريمة الإلكترونية يجب أن يكون بالشروع في أحد سلوكيات الجريمة المرتكبة، أما الأعمال التحضيرية فلا تعد ضمن سلوكيات الجريمة، إلا إذا كانت في حد ذاتها تعد جريمة تامة.¹

والبدء في تنفيذ الجريمة هو الفاصل بين الأعمال التحضيرية والتي لا يعاقب عليها القانون، حيث اختلف الفقه في وضع معيار ينظم مرحلة البدء في التنفيذ إلى مذهبين، المذهب الأول هو المذهب المادي الذي يمثلته الفقيه فيلي، يرى أن الفعل لا يدخل في دائرة التنفيذ، إلا إذا أصاب به الفاعل الركن المادي للجريمة كما عرفها القانون، أما المذهب الثاني فيبحث أنصاره في إرادة الجاني أي مدى دلالة أفعال الشخص على قصده²، وتبنى المشرع الجزائري المذهب الثاني أي الشخصي في تحديد البدء في

¹ - نائلة عادل محمد فريد قورة، المرجع السابق، ص 479 وما بعدها.

² - أحسن بوسقيعة، الوجيز في القانون الجزائي العام، دار هومة، الجزائر، ط8، 2009، ص 95.

التنفيذ متأثراً بالنهج الذي سلكه المشرع الفرنسي وباقي التشريعات، فالتساؤل الذي يمكن طرحه أي المعيارين يمكن الأخذ بهما في الجرائم الإلكترونية، فمن الوهلة الأولى نجد أن المعيار الشخصي لا يمكن الإعتماد عليه وذلك راجع إلى وحدة النشاط المادي في الجريمة الإلكترونية من ناحية، ومن ناحية أخرى يؤدي إلى إدخال الأعمال التحضيرية في دائرة التجريم¹، فالنشاط المادي يستلزم القيام بحركة مادية موحدة تعتمد على الحاسب الآلي واستخدام الأنترنت، مما يصعب من تحديد نوعية الجريمة المراد ارتكابها، فمثلاً من يشرع في تحميل صفحة أنترنت تحتوي على صور وأفلام مرتبطة بالاستغلال الجنسي للأطفال فقد لا يتم عمله، نتيجة لمراقبة عملية التحميل من قبل مزود الأنترنت، الذي يقوم بإبلاغ السلطات في الوقت الذي يمنع تقنيا مرتكب الجريمة من إتمام التحميل، هنا لا يمكن القول أن الجاني كان في حالة شروع، ليس بسبب عدم إتمام التحميل وهو النتيجة المطلوبة لتقرير مدى إمكانية توافر الجريمة في حالة الشروع، وإنما يعود السبب لعدم التحميل، ولكن يمكن إدانة الجاني بارتكاب جريمة حيازة بيانات ممنوعة مخزنة في الحاسوب.

أما المعيار المادي لم يبرز سوى الواقع وما توصلت إليه النظرة المادية للأمور، أما المعيار الشخصي فيتطلب الأمر محاولة الحصول على تسبب قد يخرج الأمور من مجراها الطبيعي، بحيث يمكن من خلال المعيار الشخصي نسبة وقائع تقنية إلى شخص لم يقيم واقعا ماديا على حدوثها أو ليس لها أساس فيه.²

مما يؤكد صعوبة التمييز بين الأفعال التحضيرية والبدء في التنفيذ في الجرائم الإلكترونية.

ثانياً: عدم إتمام الجريمة لظروف خارجة عن إرادة الفاعل

إن البدء في التنفيذ غير كاف لوجود شروع، إذ لابد من توافر العنصر الثاني وهو وقف التنفيذ أو خيبة أثر الأفعال نتيجة لظروف مستقلة عن إرادة مرتكبيها.

والشروع نوعان هما: الشروع التام وفيه يحقق الجاني النشاط الإجرامي كاملاً، لكن النتيجة لا تتحقق لأسباب لا دخل لإرادة الجاني فيها (الجريمة الخائبة) أما النوع الثاني هو الشروع الناقص حيث لا يكتمل

¹ - عمر محمد أبو بكر بن يونس، المرجع السابق، ص 279.

² - عمر محمد أبو بكر بن يونس، المرجع نفسه، ص 279.

النشاط الإجرامي لسبب خارج عن إرادة الجاني (الجريمة الموقوفة).¹

إذ يمكن تصور وتطبيق الشروع التام (الجريمة الخائبة) في مجال الجرائم الإلكترونية مثل لو قام الجاني بإدخال بطاقة إلكترونية إلى جهاز الحاسب الآلي، وأدخل الشفرة الخاصة بالجهاز إلا أن عملية تحويل الأموال لم تتم لعطل في الجهاز، كذلك إدخال برنامج فيروس في أحد نظم المعالجة الآلية بغرض تخريب بعض المعلومات، التي تحتويها إلا أن النتيجة لم تتحقق بسبب من أن النظام مشمول بحماية تدابير أمنية حالت دون ذلك.²

أما بالنسبة للشروع في الجريمة الموقوفة، فيمكن للجاني الدخول لأحد أنظمة المعالجة الآلية للمعطيات وبيدأ بالتلاعب بالمعلومات ثم عدل عن إتمام الجريمة لعدم رغبته في إكمال النشاط الإجرامي، أيا كان الباعث وراء العدول، في هذه الحالة يكون العدول منتجا لآثاره في عدم العقاب طالما لم يكن راجع لأسباب خارجية، أما إذا توافرت هذه الأسباب كما لو دخل الجاني بطريق الصدفة المحضة إلى نظام المعالجة الآلية، ثم استمر في البقاء في هذا النظام، وحدث أن قام العاملون على النظام باكتشاف دخوله فقام بقطع الإتصال عليه فإن الجريمة هنا قد وقفت عند حد الشروع.³

ثالثا: الركن المعنوي

الشروع جريمة عمدية يتخذ فيها الركن المعنوي صورة القصد الجنائي بعنصره العلم والإرادة، ولا يختلف هذا الركن الخاص بجريمة الشروع عن الركن المعنوي في الجريمة التامة وهو ما يقتضي اتجاه الإرادة إلى ارتكاب الجريمة لا إلى مجرد الشروع فيها.

وعلى ذلك يكون سلوك الجاني إراديا، وأن يتوافر علمه بكافة العناصر الجوهرية اللازمة لقيام الجريمة.

الفرع الرابع: الاتفاق الجنائي

هناك من يرى أن الاتفاق الجنائي هو جريمة خاصة وتامة، وليس مجرد عزم إجرامي، وتبرير المعاقبة عليه أنه يظهر العزم الجماعي الجنائي بمظهر خارجي مادي ملموس، لأن كل عضو يعلن

¹ - محمود نجيب حسني، المرجع السابق، ص 345.

² - رشيدة بوكري، المرجع السابق، ص 358.

³ - رشيدة بوكري، المرجع نفسه، ص 357.

عزمه إلى سائر الأعضاء فتتحد إرادتهم على ارتكاب الجريمة، وبالتالي فالإتفاق موجود ويمكن إثباته، ومن جهة أخرى فالإتفاق الجنائي ظاهرة خطيرة تهدد الأمن العام تهديدا فعليا.¹

الفقرة الأولى: تعريف الإتفاق الجنائي

لم يعرف قانون العقوبات المقصود بالإتفاق أو الجمعية، غير أن المسلم به أن الجمعية أو الإتفاق يقتضي إنعقاد إرادتين أو أكثر على ارتكاب الجريمة، أو على الأعمال المجهزة أو المسهلة لارتكابها، ولا يهم بعد ذلك مدة تشكيل الجمعية أو تأليف الإتفاق، والإتفاق والجمعية عبارتان تقيدان نفس المعنى تقريبا ولكن الجمعية أكثر هيكلية من الإتفاق.²

ولقد لجأت العديد من الدول إلى تجريمه، ومن بينه المشرع الجزائري واعتبرها جريمة مستقلة بذاتها، وكذلك تعاقب على مجرد الأعمال التحضيرية، فقد نصت المادة 176 من ق.ع.ج على أنه " كل جمعية أو إتفاق مهما كانت مدته أو عدد أعضائه تشكل أو تؤلف بغرض الإعداد لجناية أو أكثر، معاقب عليها بخمس (5) سنوات حبس على الأقل، ضد الأشخاص أو الأملاك تكون جمعية أشرار، وتقوم هذه الجريمة بمجرد التصميم المشترك على القيام بالفعل".³

وقد أثار هذا السلوك جدلا فقهيا كبيرا حول مدى ملائمة تجريم المشرع للإتفاق الجنائي من عدمه، حيث ظهر اتجاهان، فالأول ذهب إلى القول بأن الإتفاق الجنائي عزم إجرامي، وتجرمه لا يعتبر استثناء يرد على قاعدة "عدم العقاب على مجرد العزم الإجرامي" ويستند هذا الرأي على أن العقاب عليه في حد ذاته كجريمة خاصة وتامة، في حين يرى أصحاب الاتجاه الثاني أن هذه الحجج التي جاء بها الإتجاه الأول غير صحيحة، ويكفي لدحضها المقارنة بين خطورة الإتفاق الجنائي وخطورة الأعمال التحضيرية التي يسعى المجرم للقيام بفعله بمفرده، فالإتفاق مرحلة مبكرة بالنسبة للتحضير للجريمة، بينما يعاقب التحضير للجريمة هذه المرحلة النفسية، كما يضيف أصحاب هذا الرأي أنه لو صحت خطورة الإتفاق الجنائي تبريرا لمعاقبة المتفقيين في هذه المرحلة المبكرة من المراحل التي تمر بها الجريمة، لوجب على

¹ - محمد خليفة، دراسة نقدية لنصوص جرائم أنظمة المعاملة الآلية للمعطيات في قانون العقوبات الجزائري، المجلة النقدية للحقوق والعلوم السياسية، المجلد 13، العدد 01، جوان 2018، ص 70.

² - أحسن بوسقيعة، المرجع السابق، ص 472.

³ - المادة 176 من قانون العقوبات الجزائري.

المشرع أن يجرم مرحلة التحضير للجريمة من باب أولى.¹

وهذا ما تنبأه المشرع الجزائري من خلال اشتراطه أن يكون التحضير مجسدا بأفعال مادية، وليس مجرد العزم والتصميم على القيام بالفعل، وهذا ما جسده نص المادة 394 مكرر 5 من ق.ع.ج التي نصت على " كل من شارك في مجموعة أو اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية، يعاقب بالعقوبات المقررة للجريمة ذاتها. "

الفقرة الثانية: أركان الاتفاق الجنائي

يتضمن الإتفاق الجنائي في نطاق الجرائم الإلكترونية، شأنه في ذلك شأن أي جريمة يتكون من أركان ويقرر له جزاء وهذا ما سوف نتطرق إليه كما يلي:

أولاً: الركن المادي

يقوم الركن المادي لجريمة الاتفاق على ثلاثة عناصر هي:

1- فعل الاتفاق

يقوم هذا الركن على الإتفاق ذاته، وهو انعقاد إرادتين أو أكثر واجتماعهما على موضوع معين، وإذا كانت المادة 176 من ق.ع.ج تكتفي تجريمها للاتفاق العام بتلاقي الإرادات على إرتكاب الجريمة، فإن المادة 394 مكرر 05 من ق.ع.ج المتعلقة بالاتفاق في جرائم المعطيات لا تكتفي بذلك، وإنما تتطلب العقاب على الإتفاق أن يكون مجسدا بفعل أو عدة أفعال مادية، فهي تشترط إضافة إلى وجود العزم وتلاقي إرادات المتفقين على الجريمة، وجود مرحلة أخرى بعد هذا العزم هي مرحلة الأعمال التحضيرية، وهذه ليست مرحلة نفسية كسابقتها، وإنما يجب أن تظهر وتتجسد في أعمال وأفعال مادية يكون القصد منها التحضير والإعداد لإرتكاب الجريمة²، وإذا ارتكب العمل التحضيري المادي شخص واحد بمفرده وبمعزل عن غيره فلا يعاقب في هذه الحالة، فالعقاب لا يتقرر إلا في حالة اجتماع شخصين فأكثر.

¹- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، المرجع السابق، ص113.

²- نجاة بن مكي، المرجع السابق، ص205.

2- موضوع الاتفاق

يستمد الإتفاق صفته الإجرامية من موضوعه، فإذا كان الموضوع مشروعاً وليس له صلة بأي جريمة فلا يعد اتفاقاً جنائياً، والمادة 176 من ق.ع.ج نصت على الإتفاق العام في الجنايات ضد الأشخاص والأموال ويجرم الإتفاق المنصب على ارتكاب جريمة أو الإعداد لها، بينما نص المادة 394 مكرر 5 من ق.ع.ج موضوعه تجريم الإتفاق في جرائم الإعتداء على أنظمة المعالجة الآلية للمعطيات، هو الإتفاق على الإعداد لتلك الجرائم والتحضير لها، ولم ينص على الاتفاق على ارتكابها، فوفقاً لهذه المادة إذا كان موضوع الإتفاق أعمالاً تحضيرية والإعداد لتلك الجرائم، فإن الإتفاق يكسب صفة الجنائية ولو كانت الأعمال في ذاتها مشروعة¹، مثلاً الاتفاق على كيفية تصميم المعطيات وتجميعها ونشرها هو مشروع في الأصل، لكنه يصبح غير مشروع إذا كان الإتفاق على تعليم ذلك بغية إستعماله في الجرائم التي تنص عليها المادة 394 مكرر 2 فقرة 1 من ق.ع.ج²، أي يجب أن يكون هذا الاتفاق موجه نحو هدف محدد وهو التحضير لارتكاب جريمة من جرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات، ولكن ما يمكن ملاحظته أن المشرع الجزائري قد خص الإتفاق الجنائي إلا في الجرائم الماسة بأنظمة المعالجة الآلية دون غيرها من الجرائم، وهي تعتبر ثغرة قانونية وجب على المشرع التدخل، وجعل الإتفاق الجنائي يضم كل الجرائم المرتكبة عبر الحاسوب والأنترنت، مثلاً لا يعاقب الاتفاق الجنائي بهدف إرتكاب جنحة تقليد البرامج المعاقب عليها بنصوص حق المؤلف والحقوق المجاورة.³

3- التعدد الضروري للجناة

تتطلب جريمة الإتفاق تعدداً ضرورياً للجناة، والحد الأدنى لهذا التعدد شخصان، ويشترط أن يكون الجناة مسؤولين جنائياً، فإذا كان أحدهما غير مسؤول جنائياً كأن يكون صغيراً أو فاقداً للإرادة والتميز لتعاطيه مسكراً دون علم منه، أو مجنوناً فالإتفاق لا يقوم.⁴

ويستوي أن يكون أعضاء الإتفاق في صورة شركة، أو مؤسسة أو شخص معنوي، أو جماعة وسواء كانوا يعرفون بعضهم البعض أو لا، كما في العصابة أو مجرد مجموعة من الأشخاص، لا يعرف أحدهم

¹ - غنية باطلي، المرجع السابق، ص، ص 192 - 200.

² - محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، المرجع السابق، ص 115.

³ - رشيدة بوكري، المرجع السابق، ص 347.

⁴ - نجاه بن مكي، المرجع السابق، ص 206.

الآخر من قبل، وانتفوا على القيام بالنشاط الإجرامي¹.

الفقرة الثالثة: الركن المعنوي

تعتبر جريمة الإتفاق من الجرائم العمدية التي لابد من توافر القصد الجنائي من علم وإرادة.

أولاً: العلم

يجب توافر العلم لدى كل عضو من أعضاء الجماعة، بماهية الفعل أو الأفعال موضوع الاتفاق، فإذا انتفى العلم انتفت الجريمة، فمن ينظم اتفاقاً معتقداً أنه للإتجار في برامج نظام المعالجة الآلية للمعطيات عادية، فإذا به لإتجار في برامج خبيثة مثل البرامج الفيروسية، فإن القصد الجنائي غير متوافر لديه، فإذا كان الإتفاق بين شخصين فقط، وانعدم العلم لدى أحدهما بموضوع الإتفاق يؤدي إلى عدم قيام جريمة الإتفاق الجنائي وبالتالي انتفاء المسؤولية الجنائية.

ثانياً: الإرادة

إضافة إلى العلم لابد من وجود إرادة جادة لشخصين على الأقل للدخول أو الاشتراك فيه، أي إرادة كل واحد أن يكون طرفاً في هذا الإتفاق وأن يقوم بالدور الذي يستعد إليه، فإذا لم تكن الإرادة على هذا النحو، فكان المتفق غير جاد يسعى إلى الوشاية بأعضاء الاتفاق أو يريد مجرد استطلاع أمرهم دون الانضمام إليهم، ينتفي عنه القصد الجنائي، لانتهاء إرادته الخاصة².

¹ - آمال بن قارة، المرجع السابق، ص131.

² - تنص المادة 177 من ق.ع.ج على ما يلي "يعاقب على الاشتراك في جمعية الأشرار بالسجن المؤقت من خمس (5) إلى عشر (10) سنوات وبغرامة من 500000 دج إلى 1000000 دج إذا تم الإعداد لارتكاب الجنايات. وتكون العقوبة بالحبس من سنتين (2) إلى خمس (5) سنوات والغرامة من 100000 دج إلى 500000 دج إذا تم الإعداد لارتكاب الجنح.

وبيعاقب منظم جمعية الأشرار أو من يباشر فيها أية قيادة كانت بالسجن المؤقت من عشر (10) سنوات إلى عشرون (20) سنة وبغرامة من 1000000 دج إلى 5000000 دج".

ثالثا: العقاب على الإتفاق الجنائي

على خلاف المادة 177 من ق.ع.ج¹ التي حددت العقوبة للاتفاق على أساس خطورة الجريمة، نجد المشرع الجزائري في إطار تجريم الإعتداء على أنظمة المعالجة الآلية للمعطيات، قد حدد عقوبة الإتفاق بالعقوبة المقررة للجريمة ذاتها المعد لارتكابها والتحضير لها، وقد أحسن المشرع حيث جعل عقوبة الاتفاق الجنائي تتناسب وعقوبة الجرائم المتفق على ارتكابها وهو ما يتوافق وخصوصية هذه الجرائم وخطورتها، وذلك للسير على درب التشريعات العالمية، وتجسيد الإتفاقيات الدولية التي تم إرسائها في مجال مكافحة الجرائم الإلكترونية، وكذا مقررات المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات بشأن جرائم الكمبيوتر، وما تضمنه القرار الصادر عن مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة السجناء المتعلق بالجرائم ذات الصلة بالكمبيوتر، والتي خلصت في مجملها إلى مجابهة الإتفاق الجنائي وإيلاء الصرامة اللازمة في معاقبته.²

المطلب الثالث: طرفا الجريمة الإلكترونية

من المتعارف عليه دائما في العمل الإجرامي أن يكون لكل جريمة طرفان، الأول هو الجاني، والذي يطلق عليه المجرم الإلكتروني (المجرم المعلوماتي) أو (المجرم التقني)، لأن جريمتنا محل الدراسة هي الجريمة الإلكترونية، والثاني هو المجني عليه أو الضحية في الجريمة، إذ يعتبر المجرم الإلكتروني (المجرم المعلوماتي) أساس ارتكاب الجريمة في المجال المعلوماتي، وتتطلب السياسة الجنائية بداية التعرف على هذا النوع الخطير من المجرمين (الفرع الأول)، بالإضافة إلى الدوافع التي تؤدي بهم إلى ارتكاب هذه الجرائم، حتى يستطيع المشرع معرفة أسباب هذا الإجرام ومن ثم مكافحته (الفرع الثاني) ما يزيد من خطورة هذه الجريمة أن للضحية دورا مهما في ارتكابها (الفرع الثالث).

¹ - رشيدة بوكري، المرجع السابق، ص، ص 348 - 349.

² - زيدان زبيحة، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، الجزائر، د ط، 2011، ص، ص 105-106.

الفرع الأول: الجاني في الجريمة الإلكترونية¹

تقر دراسات علم الإجرام على التمييز بين الإجرام الطبيعي والإجرام الإصطناعي -المكتسب- ونادى بهذا التمييز عالم الإجرام الإيطالي "جاروفا لو"، ولقد ثار جدال فقهي يدور حول النوع الذي ينتمي إليه المجرم المعلوماتي²، وما يمكن القول في هذا الصدد أن المجرم المعلوماتي يمثل بالنسبة للمجموعات التقليدية أي (الإجرام الطبيعي) شخصية مستقلة قائمة بذاتها، مثال متفرد للمجرم الذكي ومن جهة أخرى إنسان اجتماعي بطبعه³، ومن خلال هذا الفرع نحاول دراسة شخصية المجرم المعلوماتي من حيث سماته وصفاته، ثم إبراز طوائفه وفئاته.

الفقرة الأولى: سمات المجرم المعلوماتي

إذا كان ارتباط الجريمة الإلكترونية بالحاسوب وشبكات المعلومات قد أسبغ على الجريمة الإلكترونية ذاتية خاصة تميزت بها عن غيرها من الجرائم التقليدية، فإن هذا الارتباط قد انعكس كذلك على مرتكب هذه الجريمة، حيث يتسم المجرم المعلوماتي بسمات خاصة تميزه عن غيره من المجرمين وذلك من حيث:

أولاً: الذكاء المعلوماتي

يتميز المجرم المعلوماتي وكأبرز صفة له بالذكاء العقلي في مجال المعلوماتية، ذلك أن التعامل مع النظام المعلوماتي والحاسب الآلي والأنترنت، لا يكون بطريقة المصادفة، بل يستلزم في الغالب نوعاً من المعرفة والدراية والمهارة في كيفية استخدام الكمبيوتر، وكيفية التعامل مع النظام المعلوماتي، وبالأخص فيما يتعلق بتجاوز جدران الحماية الأمنية للأنظمة المعلوماتية، وغيرها من العقبات المعلوماتية التي قد

¹ - الجاني في الجريمة الإلكترونية يطلق عليه مصطلح المجرم المعلوماتي وهو مصطلح قانوني يطلق على الشخص الذي له مهارات تقنية أو دراية بالتكنيك المستخدم في نظام الحاسب الآلي، أما المصطلح الإلكتروني يسمى "هاكر" "Hackers" ويطلق خبراء أمن المعلومات الإلكترونية اسم الهاكر على الشخص الذي يقوم بعمليات الاختراق والتخريب على شبكة الأنترنت، كما يطلق مصطلح "كراكرز" "Crackers" على المتخصصين بفك شفرات البرنامج وليس تخريب الشبكات، فهو نوع من الهاكرز المتخصص ويستخدم هذا المصطلح في المجال الإعلامي. للمزيد أنظر: هلال بن محمد بن حارب البورسعيد، الحماية القانونية والفنية لقواعد المعلومات المحسوبة - دراسة قانونية وفنية مقارنة-، دار النهضة العربية، القاهرة، ط1، 2009، ص38.

² - عبد الفتاح بيومي حجازي، نحو صياغة نظرية عامة في الجريمة والمجرم المعلوماتي، المرجع السابق، ص95.

³ - محمد سامي الشوا، المرجع السابق، ص49.

تعرض سبيل ارتكاب الجاني للجريمة الإلكترونية.¹

ومثل هذا الذكاء يكتسبه الجاني إما من خلال الدراسة المتخصصة لعلوم الكمبيوتر والأنظمة المعلوماتية أو من خلال التطبيق أو الخبرة العملية، أو من خلال اختلاطه إجتماعيا بالمتخصصين في علوم الكمبيوتر والأنترنت والأنظمة المعلوماتية، وهو يختلف من جان إلى آخر، ولكن المهم هو أن يصل إلى مستوى يمكن معه الجاني من ارتكاب الجريمة الإلكترونية التي يريد ارتكابها، فهناك جرائم إلكترونية يستلزم لإرتكابها أن تتوفر لدى الجاني، معرفة واسعة جدا بكيفية استخدام أصعب الأجهزة والبرامج في حين أن هناك جرائم إلكترونية أخرى، لا يتطلب ارتكابها سوى ضغط زر أو بضع ضغطات كمن يرسل رسالة إلكترونية إلى آخر يهدده فيها بالقتل، أو كمن يعطي الإيعاز لجهاز الحاسب الآلي العائد لغيره بمسح ملف أو ملفات معينة موجودة داخل الجهاز نفسه.²

ثانيا: عدم الاعتراف بالمسؤولية الجزائية

أثبتت الدراسات السيكلوجية التي أجريت على مجرمي المعلوماتية، بأن أغلب هؤلاء لا يشعرون بالمسؤولية الجزائية عن الأفعال التي يأتونها، فهم يعتبرونها أفعالا مباحة لا يستحقون العقاب عليها³، فمن خلال لقاء أجراه الأستاذ "دون باركر" "Don Parker" مع اثنين من مجرمي المعلوماتية حكم عليهما بالسجن لاستعمالهما غير المصرح به للكمبيوتر العائد لرئيسهما لتحقيق أغراضهما الشخصية، ذكر له المحكومان خلال اللقاء بأن السلوك الذي أقدموا عليه هو سلوك شائع ومقبول في أوساط العاملين في المؤسسات اللتين كانا يعملان لديها، وأن أغلب العاملين في المؤسسات كانوا يقدمون على هذه الأفعال سواء لتحقيق الربح المادي أو لمجرد التسلية في أوقات الفراغ.⁴

ثالثا: الجاني إنسان اجتماعي

المجرم المعلوماتي هو عادة إنسان اجتماعي قادر على التكيف في بيئته الاجتماعية، بل إن بعضهم يتمتع بثقة كبيرة في مجال عمله، فالمجرم المعلوماتي يتميز بأنه لا يضع نفسه في حالة عدا مع

¹ - هلال بن محمد بن حارب البورسعيدى، المرجع السابق، ص47.

² - رشاد خالد عمر، المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية- دراسة تحليلية مقارنة -، المكتب الجامعي الحديث، د.م.ن، دط، 2013، ص49.

³ - أيمن عبد الله فكري، المرجع السابق، ص114.

⁴ - نائلة عادل محمد فريد قورة، المرجع السابق، ص60.

المجتمع الذي يحيط به بل إنه إنسان قادر على التوافق والتصالح مع مجتمعه¹، فهو شخص مرتفع الذكاء مما يساعده على عملية التكيف مع المجتمع، فالذكاء في نظر الكثيرين ليس سوى القدرة على التكيف، وهذا الأمر لا يقلل من شأن المجرم، بل بالعكس فإن خطورته الإجرامية تزداد كلما زاد تكيفه الإجتماعي مع توافر الشخصية الإجرامية لديه.²

رابعاً: الجاني يتمتع بالسلطة تجاه النظام المعلوماتي

ويقصد بالسلطة الحقوق أو المزايا التي يتمتع بها المجرم المعلوماتي التي تمكنه من ارتكاب جريمته، فكثير من مجرمي المعلوماتية لديهم سلطة مباشرة أو غير مباشرة في مواجهة المعلومات محل الجريمة، وقد تتمثل هذه السلطة في الشفرة الخاصة بالدخول إلى النظام الذي يحتوي على المعلومات التي تعطي الفاعل مزايا متعددة، كفتح الملفات وقراءتها وكتابتها ومحو المعلومات أو تعديلها، وقد تتمثل هذه السلطة في الحق في استعمال الأنظمة المعلوماتية أو إجراء بعض التعاملات أو مجرد الدخول إلى الأماكن التي تحتوي على هذه الأنظمة.³

خامساً: الجاني مجرم غير عنيف

المجرم المعلوماتي من المجرمين الذين لا يلجؤون إلى العنف بتاتا في تنفيذ جرائمهم، وذلك لأنه ينتمي إلى إجرام -الحيلة- فهو لا يلجأ إلى العنف في ارتكاب جرائمه، وهذا النوع من الجرائم لا يستلزم أي قدرا من العناء للقيام به.⁴

سادساً: الجاني يبرر ارتكاب جريمته

يوجد شعور لدى مرتكب فعل الإجرام المعلوماتي أن ما يقوم به لا يدخل في عداد الجرائم، أو بمعنى آخر لا يمكن لهذا الفعل أن يتصف بعدم الأخلاقية، وخاصة في الحالات التي يقف فيها السلوك عند قهر نظام الحاسوب وتخطي الحماية المفروضة حوله، حيث يفرق مرتكبو هذه الجرائم بين الإضرار بالأشخاص الأمر الذي يعدونه غاية في اللاأخلاقية، وبين الإضرار بمؤسسة أو جهة في استطاعتها إقتصاديا تحمل

¹ - نهلا عبد القادر المومني، المرجع السابق، ص 79.

² - غنية باطلي، المرجع السابق، ص 36.

³ - تركي عبد الرحمن الموشير، المرجع السابق، ص 29.

⁴ - عبد العال الديربي، محمد صادق اسماعيل، المرجع السابق، ص 59.

نتائج تلاعبهم.¹

فهؤلاء الأشخاص لا يدركون أن سلوكهم يستحق العقاب، ويبدو أن الاستخدام المتزايد للأنظمة المعلوماتية قد أنشأ مناخا نفسيا موائما لتصور إستبعاد فكرة الخير والشر، وقد ساعد على عدم وجود احتكاك مباشر بالأشخاص، ومما لا شك فيه أن هذا التباعد في العلاقة الثنائية بين الفاعل والمجني عليه يسهل المرور إلى الفعل غير المشروع، ويساعد على إيجاد نوع من الإقرار الشرعي الذاتي بمشروعية هذا الفعل.²

ففي كثير من الأحيان يقوم العاملون بالمؤسسات المختلفة باستخدام أجهزة الحاسوب لأغراض شخصية بوصفه سلوكا شائعا بين الجميع ولا ينظر إليه بوصفه فعلا إجراميا.³

إلا أن ذلك لا يعني أن عدم الشعور بعدم أخلاقية هذه الأفعال الإجرامية لدى فئة كبيرة من مرتكبيها ينفي وجود مجرمين يرتكبون الإجرام المعلوماتي وهم على علم وإدراك بعدم مشروعية الفعل، فهناك فئة لديها إتجاه إجرامي خطير وسوء نية واضح وهم على إدراك بخطورة أفعالهم.⁴

ويتميز المجرم المعلوماتي كذلك بمجموعة من الخصائص التي تميزه بصفة عامة عن غيره من المجرمين ويرمز إليها الأستاذ Parker بكلمة S.K.R.A.M وهي تعني المهارة، المعرفة، الوسيلة، السلطة، وأخيرا الباعث.⁵

ومجمل القول أن الإجرام المعلوماتي هو إجرام الذكاء، ولا يحتاج إلى استخدام القوة والعنف، وهذا الذكاء هو مفتاح المجرم المعلوماتي لاكتشاف الثغرات وإختراق البرامج المحصنة، ويمكن إجمال القواسم المشتركة بين هؤلاء المجرمين في عدة صفات وهي شبه اتفاق بين الكثير من الفقهاء شأنها شأن سمات العالم الافتراضي نذكر منها:

¹ - نهلا عبد القادر المومني، المرجع السابق، ص78.

² - تركي بن عبد الرحمان المويشير، المرجع السابق، ص28.

³ - نائلة عادل محمد فريد قورة، المرجع السابق، ص55.

⁴ - تركي بن عبد الرحمن المويشير، المرجع السابق، ص28.

⁵ - وللمزيد من الإطلاع أنظر في ذلك عبد الكريم رشيد توبة، جرائم تكنولوجيا المعلومات، دار المستقبل، ط1، 2008، ص، ص 151-152. وكذلك أنظر عبد العال الديربي، المرجع السابق، ص60.

- عادة ما تتراوح أعمار تلك الفئة من المجرمين ما بين 18-45 عاما.
- المهارة والإلمام الكامل والقدرة الفنية الهائلة في مجال نظم المعلومات.
- إنتماؤهم إلى طبقة المثقفين والمتعلمين.
- الثقة الزائدة بالنفس والإحساس بإمكانية ارتكابهم لجرائمهم دون افتضاح أمرهم.
- إلمامهم التام بمسرح الجريمة وبأدواته، مما يجنبه فجائية المواقف التي تؤدي إلى إفشال مخططاتهم.¹

الفقرة الثانية: طوائف وفئات الجاني

أمام التطور السريع والتغير في أنماط الجريمة الإلكترونية وصورها فقد يكون من الصعب وضع تصنيف ثابت لطوائف مجرمي المعلوماتية، ولكن يمكننا وفقا لما توصلت له الدراسات والأبحاث التي تناولت مجرمي المعلوماتية أن نبين بعض الأنماط لهؤلاء المجرمين، وما تجدر الإشارة إليه أن هذه التصنيفات لا تعني أن كل مجرم معلوماتي يندرج تحت فئة محددة دون غيرها من الفئات المذكورة، بل يمكن أن يكون المجرم الواحد مزيجا من أكثر من طائفة أو فئة.

أولا: فئة صغار مجرمي المعلوماتية

أو كما يسميهم البعض صغار نوابغ المعلوماتية (pranksters)²، وتضم هذه الطائفة الأشخاص الذين يرتكبون الجرائم الإلكترونية، بغرض التسلية والمزاح دون أن تكون لديهم نية إحداث أي ضرر بالمجني عليه، وذلك عن طريق إستخدام آلية محمولة خاصة بهم، أو حاسبات آلية خاصة بمدارسهم، ومن بينهم فئة لم تبلغ بعد سن الأهلية مفتونين كثيرا بالتقنيات الرقمية، وهم غالبا ما يكونون في مرحلة المراهقة، وعلى الرغم من صغر سنهم إلا أنهم قادرون على اقتحام كافة أنواع الأنظمة المعلوماتية.³

ثانيا: فئة القراصنة أو المحترفون

قراصنة المعلومات هم في الغالب مبرمجون من أصحاب الخبرة، يهدفون إلى الدخول إلى أنظمة

¹ - محمد علي قطب، المرجع السابق، ص14.

² - le terme "phreaking provient de la contraction de deux mots anglais "phone" (Téléphone) et freak (monstre) le phreaker désigne l'auteur d'une fraude informatique constituée par l'utilisation des lignes téléphoniques, voir Mohamed Chawki , op.cit. , p 34.

³ - نعيم سعيداني، المرجع السابق، ص53.

المعلوماتية وكسر الحواجز الأمنية المحيطة بالأنظمة، ويمكن تصنيفها إلى صنفين هما:

1- القراصنة الهواة العابثون (Hackers)

ويطلق على هذه الطائفة مصطلح (Hacker's)¹ ويعني المتطفل، وهو ذلك الشخص الذي يتميز بقدر عال من الكفاءة التقنية، ويتفخرون بإلمامهم بعلوم الحاسوب، وبقدرتهم على إختراق شبكات الحاسوب وبجهدهم الذاتي، ودون الإستعانة بأي تعليمات من أي مصادر، وأغلبهم من صغار السن²، كما أنهم يدعون أنه لا توجد هناك دوافع تخريبية وراء أعمالهم، بل يكون الفضول وحب المعرفة والتعمق في عمل الأنظمة المعلوماتية هو دافعهم الأول، ومجرمو هذا الصنف هم عادة أشخاص عاديون يشغلون مناصب محل ثقة، ولديهم الكفاءة والمعرفة والمهارة المطلوبة في مجال الحواسيب والشبكات.³

وأهم سمة مميزة لهذه الفئة من القراصنة، ألا وهي تبادلهم المعلومات فيما بينهم، وتحديدًا التشارك في وسائل الإختراق، كما ساهم هؤلاء القراصنة في كشف العديد من الفجوات الأصلية للأنظمة المعلوماتية في المؤسسات المالية، الأمر الذي ساهم في تطوير نظم الأمن ضد الاختراقات الأمنية التي يقوم بها مجرمو المعلوماتية.

2- القراصنة المحترفين (Crackers)

تعرف هذه الفئة بالمجرمين البالغين أو الهاكر الخبيث أو المحترف أو المخترق ذو النوايا الإجرامية أو العنكبوت Araignées⁴، ويتميز أفراد هذه الطائفة بالتخصص العالي في مجال الحاسوب، وتعد هذه الطائفة من أخطر مجرمي المعلوماتية، حيث تهدف إعتداءاتهم بالأساس إلى تحقيق الكسب المادي لهم،

(1) - le terme "hacker" provient du verbe anglais « "to hack into" » qui signifie « "entrer par effraction » ". le hacker peut être considéré comme « "une personne qui prend du plaisir à explorer en détail un système, un programme, et qui cherche sans cesse à étendre ses connaissances dans ce domaine" » en pratique le hacker exploite les failles dans une procédure d'accès pour casser un système informatique et en violer l'intégrité, afin d'y dérober, d'altérer, ou détruire de l'information ou encore de copier frauduleusement des logiciels ou des données. Voir: romain Boos, la lutte contre la cybercriminalité au regard de l'action des états, Thèse de doctorat de droit privé et sciences criminelles, Université de lorraine, France, 2017, p33.

² - محمود أحمد عابنة، المرجع السابق، ص41.

³ - وليد الزيدي، القراصنة على الأنترنت والحاسوب، دار أسامة للنشر، عمان، ط1، 2003، ص41.

⁴ - Le cracker se cache dans l'ombre, laissent des traces déplaisantes de leur passage et peuvent être dangereux on les appelle araignées (Spiders) voir Mohamed Buzabar, la criminalité informatique sur l'internet, journal Law, n°20, 2002, p47.

مشار إليه لدى نبيلة هبة هروال، جرائم الأنترنت، المرجع السابق، ص53.

أو للجهات التي كلفتهم وسخرتهم لارتكاب جرائم نظم المعلومات عامة والجرائم الإلكترونية خاصة، كما تهدف إعتداءات بعضهم إلى تحقيق أغراض سياسية، والتعبير عن موقف فكري أو نظري أو فلسفي¹ ويتصف أفراد هذه الطائفة بالتكتم خلافا للطائفة الأولى، فلا يتبادلون المعلومات بشأن أنشطتهم، بل يطورون معارفهم الخاصة، ويحاولون ما أمكن عدم كشف طرقهم التقنية لإرتكاب جرائمهم.

ويتشابه مرتكبو هذه الأفعال المجرمة مع المجرمين ذوي الياقات البيضاء،² من حيث كونهم من أصحاب التخصصات العالية، ولهم الهيمنة الكاملة مع تقنية الإلكترونية وعلى قدر من الذكاء.³

ثالثا: فئة الحاقدين

إن الرغبة في الثأر والانتقام هو الطابع الغالب على تصرفات هذه الفئة، كما أن أعضاء هذه الفئة لا تتسم بالمعرفة التقنية الاحترافية، ويغلب على أنشطتهم من الناحية التقنية إستخدام الفيروسات، والبرامج وتعطيل النظام، أو الموقع المستهدف وإتلاف كل أو بعض معطيات الأنظمة الخاصة بالحاسب الآلي إن كان من مواقع الأنترنت.⁴

رابعا: مجرمو المعلوماتية أصحاب الآراء المتطرفة

هذه الفئة تضم كل من الجماعات الإرهابية أو المتطرفة التي تتكون من مجموعة من الأشخاص لديهم معتقدات وأفكار اجتماعية، أو سياسية أو دينية، ويرغبون في فرض هذه المعتقدات باللجوء أحيانا إلى النشاط الإجرامي، وترتكز هذه الفئة نشاطها بصفة عامة في استخدام العنف ضد الأشخاص، من أجل لفت الأنظار إلى ما يدعون إليه، وبدأ إهتمام هذه الجماعات وخاصة تلك التي تتمتع بدرجة عالية من التنظيم يتجه إلى نوع جديد من النشاط الإجرامي ألا وهو الجريمة الإلكترونية.

فهذه الجماعات تدافع عن قضية أو معتقد معين ولا تهدف الى تحقيق الربح المادي، وفي هذا

¹ - أيمن عبد الله فكري، المرجع السابق، ص110.

² - مصطلح المجرمين ذوي الياقات البيضاء، مصطلح حديث نسبيا أول من أطلقه عالم الاجتماع "Suther land" حيث وضح أن هذه الجرائم ترتكب من قبل الطبقة الراقية في المجتمع ذوي المناصب الإدارية الكبيرة وتشمل أنواعا مختلفة من الجرائم، كغسيل الأموال، تجارة الرقيق وتزوير العلامات التجارية وغيرها من الجرائم وهم جالسون في مكاتبهم.أنظر: عبدالفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والأنترنت، دار الكتب القانونية، مصر، 2007.

³ - سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الأنترنت، دار الفكر الجامعي، الاسكندرية، د ط، 2007، ص54.

⁴ - نسرین عبد الحمید نبیہ، المرجع السابق، ص43.

تختلف هذه المنظمات المتطرفة عن المنظمات الإجرامية المنظمة، حيث تهدف الأخيرة إلى تحقيق مصالحها الشخصية المباشرة وتحديدًا تحقيق الربح المادي.¹

وأبرز سمات وخصائص هذه الطائفة أن المجرم المتطرف لا يسعى لتحقيق هدف شخصي، أو الحصول على نفع مادي له، بل يعمل على تغيير المجتمع ليتماشى مع ما يعتقد صحته من الأفكار والمعتقدات.

ومن أمثلة ذلك قيام جماعات تنتمي إلى منظمات إرهابية دولية من اليمين المتطرف واليسار مثل جماعة الألوية الحمراء الإيطالية، ومنظمة (LECLODO) وهي منظمة فرنسية متخصصة في تدمير نظم المعلومات وغيرها من المنظمات الأخرى بارتكاب أفعال اعتداء على أنظمة المعلومات، المنتشرة في أوروبا ابتداءً من عام 1978.

وقد تعرضت وزارات وجامعات ومؤسسات مالية لهجمات الألوية الحمراء، فأصدرت هذه المنظمة منشورا في فبراير 1998 شرحت فيه استراتيجيتها وأهدافها من الهجوم على النظم المعلوماتية.²

خامسا: الموظفون العاملون في مجال الأنظمة المعلوماتية

بحكم طبيعة عمل هؤلاء الموظفين، ونظرا لأن النظام المعلوماتي هو مجال عملهم الأساسي، ونظرا للمهارات والمعرفة التقنية التي يتمتعون بها، فإنهم يقتربون بعض الجرائم المعلوماتية التي من الممكن أن تحقق أهدافهم الشخصية وأهمها الكسب المادي، فالعلاقة الوظيفية التي تربط بين الموظف والمجني عليه، تجعل عملية ارتكابه للجريمة الإلكترونية أسهل، نظرا للثقة التي يتمتع بها.

سادسا: مجرمو المعلوماتية في إطار الجريمة المنظمة

ويجتمع تحت لواء هذا الصنف مجرمو المعلوماتية المنتمون إلى منظمات إجرامية كالمافيا الروسية، كارتل المخدرات الكولومبي، عصابات كاليفورنيا، بحيث يشتغلون على استغلال شبكة الأنترنت من أجل

¹ - نهلا عبد القادر المومني، المرجع السابق، ص، ص 85-86.

² - ويبدأ المنشور الذي أصدرته الألوية الحمراء بالتعريف بالمحور الاستراتيجي للمنظمة وهو مهاجمة الهيئات متعددة الجنسيات تلك الموجودة على وجه الخصوص في الولايات المتحدة الأمريكية فهي عدوها الأول وتغزو المنظمة إلى أجهزة الحاسوب نجاح هذه الهيئات ويعتبرون الحاسوب سلاحا خطيرا بفضل قدرته على حفظ المعلومات ومقارنتها، أنظر: نهلا المومني، المرجع نفسه، ص86.

العمل على نهب الأموال، وتحويلها بطرق مشروعة لحساباتهم، إضافة إلى تبييضها، وقد قدر مكتب Lexy قيمة الأموال التي تم تبييضها سنة 2006 ما بين 640 مليار دولار و1.6 تريليون دولار.¹

سابعا: الإهمال الجنائي

وتتضمن أهم المشكلات التي تتصل بإساءة استخدام الحاسبات الآلية ألا وهي الإهمال، ومما لا شك فيه أن في مجال الحاسوب تترتب نتائج خطيرة قد تصل إلى حد إزهاق الأرواح، فعلى سبيل المثال ما وقع في نيوزيلندا بحيث قام شخصان، من مبرمجي الحواسيب الإلكترونية بتغيير أحد البرمجيات التي تعمل على تحديد خطوط سير الطائرات في السماء، ولم يتمكنوا من الإتصال بقائد الطائرة بعد هذا التغيير مما تترتب عليه تحطم الطائرة لاصطدامها بأحد الجبال، وقتل 60 راكبا كانوا على متن الطائرة وتمت محاكمتهم حينها على أساس القتل الخطأ.²

وما يمكن ذكره أن هناك اتفاق بين الخبراء والمتخصصين أن مجال الجريمة الإلكترونية يمثل تحديا جديدا في عالم الجريمة وذلك للأسباب التالية:

- صعوبة التعرف على هوية الجاني، فهو لا يترك أثرا لجريمته.
- وجود عقبات في محاكمة الجاني، حال اكتشاف هويته إذا كان من بلد لا يعتبر ما قام به جرما.
- اتساع شريحة الجناة لتشمل صغار مستخدمي الأنترنت لسهولة استعمال الوسائل والبرامج المستخدمة في عملية التخريب.
- نقص الوعي بسلبية الاستخدام السيء للأنترنت، مما يجعل البعض ينظر للأعمال التخريبية كاختراق المواقع عمل بطولي.³

الفرع الثاني: أسباب ودوافع ارتكاب الجريمة الإلكترونية

تختلف الجريمة الإلكترونية عن الجريمة التقليدية في محلها وخصائصها، لذا لا بد أن تكون الدوافع لارتكابها مختلفة عن أسباب ودوافع الجريمة التقليدية، ويأتي في مقدمة هذه الأسباب والدوافع غاية التعلم

¹ - تركي بن عبد الرحمان المويشير، المرجع السابق، ص33.

² - نائلة عادل محمد فريد قورة، المرجع السابق، ص63.

³ - عبد العال الديربي، محمد صادق اسماعيل، المرجع السابق، ص63.

التي تتمثل في استخدام الحاسوب والإمكانات المستحدثة لنظم المعلوماتية، وكذا وجود رغبة هؤلاء المجرمين في تحقيق الثراء السريع، بالإضافة إلى الإنبهار والشغف بالإلكترونيات والإنجاز التقني، كما قد تكون الأسباب الشخصية دافعا لانتشار هذا النوع من الجرائم.¹

لذا فثمة دوافع عديدة تحرك مجرمي المعلوماتية لإرتكاب أفعال الإعتداء المختلفة المنطوية تحت مفهوم الإجرام المعلوماتي، ويمكن تلخيص هذه الدوافع فيما يلي:

الفقرة الأولى: الدوافع الشخصية

ويمكن رد الدوافع الشخصية لدى مرتكب الجرائم الإلكترونية إلى دوافع مالية ودوافع ذهنية وهما أهم الدوافع لدى المجرم المعلوماتي في إرتكاب مثل هذه الجرائم.

أولاً: الدوافع المادية

تعد الدوافع المادية من أهم البواعث على إرتكاب الجرائم الإلكترونية، لما تحققه من ثراء فاحش²، حيث يرجع إرتكابهم لها إلى الديون الناتجة عن المشاكل العائلية، أو الخسائر الضخمة من ألعاب القمار أو إدمان المخدرات، وقد تكون جميع الوسائل بالنسبة إلى البعض مشروعة في مثل هذه الحالات الغاية تبرر الوسيلة.³

يلجأ الجاني لإرتكاب الجريمة الإلكترونية وذلك لتحقيق المكاسب المادية، إما يستعمل المساومة على البرامج أو المعلومات المتحصلة بطريقة الاختلاس من جهاز الحاسوب، أو عن طريق إستعمال بطاقة سحب آلي مزورة أو منتهية الصلاحية وغير ذلك، ولقد أشارت مجلة Sécurité informatique وهي مجلة متخصصة في الأمن المعلوماتي أن 43% من حالات الغش المعلن عنها قد تمت من أجل اختلاس الأموال و23% من أجل سرقة المعلومات و19% أفعال إتلاف و15% سرقة وقت الآلة

¹ - Meriem Quémener et J. Ferry, cybercriminalité, défi mondial, 2^{ème} édition, Economica, paris, 2009, p69.

² - ومن أمثلة ذلك ما حدث في فرنسا سنة 1986، حيث كان العائد من ارتكاب جنائية سرقة مع حمل السلاح هو 70000 فرنك فرنسي، في حين أن جريمة الغش في مجال المعالجة الآلية للمعلومات حصل منها الجاني على 670.000 فرنك فرنسي أي ما يعادل أكثر من 38 مرة. أنظر ذلك في:

Rose Philipe, la criminalité informatique, Que sais-je?, 1^{ère} édition, PuF 1988, p490.

³ - أحمد خليفة الملط، المرجع السابق، ص100.

لأغراض شخصية.¹

إن نجاح المجرم المعلوماتي في ارتكاب جريمته الإلكترونية، فإن ذلك يجعله يتحصل على أرباحا طائلة في زمن قياسي، ويمكن أن نوضح ذلك من خلال إحدى الدراسات الواردة بالتقرير السادس لمعهد أمن المعلومات حول الجرائم الإلكترونية، حيث أجريت هذه الدراسة بمشاركة 538 مؤسسة أمريكية تضم وكالات حكومية، وبنوك ومؤسسات مالية ومؤسسات صحية وجامعات، والتي أظهرت حجم الخسائر الناجمة عن الجرائم الإلكترونية، فقد تبين أن 85% من المشاركين تعرضوا لإختراقات الأنظمة المعلوماتية، وأن 64% لحقت بهم خسائر مادية جراء هذه الإعتداءات.²

ثانيا: الدوافع الذهنية أو النمطية

غالبا ما يكون الدافع لدى مرتكب الجرائم الإلكترونية، هو الرغبة في إثبات الذات وقهر النظام، أو لمجرد الدعاية والتسلية.

1- الرغبة في إثبات الذات

إن الرغبة في قهر النظام يعد أهم دافع لإرتكاب الجريمة الإلكترونية، أكثر من الرغبة في الحصول على الربح، فيميل مرتكبو الجرائم الإلكترونية إلى إظهار تفوقهم من خلال التحدي الفكري أثناء استخدامه للحاسب الآلي، وإثبات قدرته على إختراق الأنظمة، وكسر الحواجز الأمنية، والرغبة في تحدي وقهر النظام، والتفوق على تعقيدات وسائل التقنية، لذلك فإن أغلب من يقومون بتلك الأفعال، هم فئة صغار نوابغ المعلوماتية، لأنهم يسعون دائما إلى إكتشاف ما هو جديد ومحاولة التعامل مع هذه البرامج الجديدة وإثبات تفوقهم العلمي.³

2- إرتكاب الجريمة كوسيلة للتسلية والدعاية

يعتبر دافع المزاح أو الدعاية من الدوافع التي تجعل الشخص يقوم بتصرفات، وإن كان لا يقصد من وراءها إحداث جرائم وإنما بغرض المزاح فقط، ولكن هذه التصرفات قد تنتج عنها نتائج ترقى إلى درجة

¹ - نهلا عبد القادر المومني، المرجع السابق، ص 90.

² - نعيم سعيداني، المرجع السابق، ص 61.

³ - أيمن عبد الحفيظ، الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، مطابع الشرطة، د.م.ن، د ط، 2005، ص 19.

الجريمة، لأنه من الطبيعي أن الشخص الذي يقوم بمسح مجموعة ملفات من جهاز شخص آخر، وكانت هذه الملفات تحتوي على معلومات مهمة فلا يمكن القول بأن هذا التصرف مجرد دعاية، بل إن هذا التصرف في حقيقته هو جريمة إتلاف وتخريب متعمد.¹

ثالثاً: الدوافع الخارجية

الإنسان بطبعه مخلوق هش من الناحية السيكولوجية، حيث أنه يمكن في بعض المواقف أن يتأثر بالموثرات الخارجية، أو أن يحدث نتيجة سلوكه المخادع لدوافع عديدة ارتكابه تلك الجرائم² ومثال هذه الدوافع.

1- دافع الانتقام من رب العمل وإلحاق الضرر به

دافع الانتقام من أخطر الدوافع التي تدفع بالجاني لإرتكاب الجريمة، وغالبا ما يصدر من شخص يملك معلومات كبيرة عن المؤسسة أو الشركة التي يعمل بها، وغالبا ما يكون أحد موظفيها فكثير من الأفراد يفصلون تعسفيا أو بغير حق من شركة أو منظمة حكومية أو حتى مصرف، لذلك يرتكب الجاني جريمة رغبة منه في الانتقام ليجعل الشركة أو المؤسسة تتكبد الخسائر المالية الكبيرة من جراء ما يسببه لها من ضرر يحتاج إصلاحه إلى وقت لا بأس به.³

حيث يقوم بزرع برنامج، يحمل تعليمات بمسح كافة البيانات في حالة عدم وجود إسمه في كشف الموظفين بالشركة، ويقوم عند فصله بالانتقام من هذه المؤسسة عن طريق تشغيل هذا البرنامج، وكذلك عن طريق احتفاظه بكلمة السر لكي يتمكن من الدخول على نظام الحاسوب الخاص بالمؤسسة، وإرتكاب أي من الجرائم، أو إعطائها لشركة أخرى منافسة لكي تتمكن من الدخول إلى أنظمة تلك الشركة والتجسس على بياناتها.⁴

كمثال على ذلك استطاعت مجموعة من القراصنة إختراق موقع جريدة "نيويورك تايمز" تسمى بـ (H.F.G) "Hacking For Girilies"، بحيث غيرت الصفحة الرئيسية للجريدة إنتقاما من أحد محرري

¹ - خالد ممدوح إبراهيم، الجريمة المعلوماتية، المرجع السابق، ص 141.

² - أحمد خليفة الملط، المرجع السابق، ص 101.

³ - محمد أمين الرومي، جرائم الكمبيوتر والانترنت، دار المطبوعات الجامعية، عمان، د ط، 2004، ص 25.

⁴ - خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص 140.

الجريدة الذي كان يكتب مقالات كثيرة، يناشد فيها بإدانة أكبر مجرم معلوماتي المسمى "كيفين منتك"¹ والملقب بـ"الكوندور"، بحيث كانت هذه المجموعة تطالب بإطلاق صراح كيفين منتيك من السجن.

2- دافع جنون العظمة أو الطبيعة التنافسية

التي تدفع العاملين داخل المنشأة لإظهار قدراتهم الفنية لإدارة المنشأة، فيؤدي ذلك إلى إرتكاب مثل هذه الجرائم حتى ينافس زملاءه للوصول إلى المراكز المرموقة.

3- دافع التعاون والتواطؤ على الأضرار

هذا النوع كثير التكرار في الجرائم الإلكترونية، وغالبا ما يحدث من متخصص في الأنظمة المعلوماتية يقوم بالجانب الفني من المشروع الإجرامي، وآخر من المحيط أو خارج المؤسسة المجني عليها لتغطية عمليات التلاعب وتمويل المكاسب المادية إليه، وعادة ما يمارسون التلصص على الأنظمة، وتبادل المعلومات بصفة منتظمة حول أنشطتهم.²

رابعا: دوافع أخرى

الدوافع السابقة التي تناولناها بالدراسة ليست هي الوحيدة، بل يوجد هناك دوافع أخرى تدفع لإرتكاب الجريمة الإلكترونية، فالتنافس السياسي والإقتصادي قد يكون دافعا لارتكاب مثل هذه الأفعال، فقد قام بعض القراصنة المتواجدين على الأراضي الروسية، بإختراق نظم حاسبات حكومية في الولايات المتحدة الأمريكية مدة عام كامل، حيث قاموا بسرقة معلومات غير سرية لكنها حساسة من أجهزة الحواسيب العسكرية الأمريكية.

كما يعد التسابق الفضائي والعسكري بين الدول دافعا لهذه الجريمة، فقد قام القراصنة بالإغارة على

¹ - كيفين منتك من أشهر وأقوى الهاكرز ومخترقي الأنظمة المعلوماتية على الإطلاق ويطلق عليه اسم كوندور أو نسر أمريكا، تم اعتقاله من قبل مكتب التحقيقات الفدرالي الأمريكي FBI وقضى ما يقارب الخمس سنوات في السجن منها 8 أشهر بالحبس الانفرادي لخطورته ما بين سنتي 1995 و 2000، وذلك عقابا على الهجمات التي قام بها والتي طالت قاعدة Pacific Bell وكذلك أنظمة كل من Fujitsu, Motorola, Nokia و Sun Microsystems، حيث منع كيفن منتك من استخدام أي شكل من تكنولوجيا الاتصالات أو أي نشاط يتعلق بالكمبيوتر ولو كان هذا النشاط مجرد الحديث أو الكتابة. أنظر في ذلك: مصطفى محمد موسى، أساليب إجرامية بالتقنية الرقمية ماهيتها ومكافحتها، دار الكتب القانونية، مصر، د ط، 2005، ص، ص 31 - 32.

² - أحمد خليفة الملط، المرجع السابق، ص 102.

شبكات معلوماتية تابعة لوكالة الفضاء ناسا، ومواقع أسلحة ذرية لحكومة الولايات المتحدة الأمريكية. كما أن المنافسة التجارية أو التجسس العسكري أو الصناعي قد يكون من البواعث التي قد تدفع إلى ارتكاب الجرائم الإلكترونية ليس من قبل الأفراد فحسب بل حتى من قبل الدول.¹

الفرع الثالث: المجني عليه في الجريمة الإلكترونية

يساهم المجني عليه في الجريمة التقليدية بقدر كبير في الكشف عنها، مما يترتب عليه إمكانية الوقوف على حجم الظاهرة الإجرامية في الجرائم التقليدية، ومن ثم إمكانية إرساء القواعد القانونية اللازمة لملاحقة الجناة ومكافحتها، ولكن الأمر يختلف بالنسبة للجرائم الإلكترونية، إذ من الصعب تحديد نطاق ضحايا هذه الجرائم على وجه الدقة، لأن هؤلاء الضحايا لا يعلمون شيئا عليها إلا بعد أن تقع فعلا، أو يكون ذلك بمحض الصدفة، وإذا تم مشاهدة أثر الجريمة فغالبا ما يلجأ المجني عليه في الجريمة الإلكترونية إلى الإحجام عن الإبلاغ عنها، خوفا على السمعة والثقة كما في المؤسسات المالية الكبرى² المجني عليها، ويمكن أن يكون الضحية في الجرائم الإلكترونية شخصا طبيعيا أو معنويا، مع أن الغالبية العظمى من الجرائم تقع على الأشخاص المعنوية، ويمكن تقسيم المجني عليهم في مجال الجرائم الإلكترونية إلى ما يلي:

أولا: المؤسسات المالية والجهات الحكومية

إن المؤسسات المالية كالبنوك والشركات المالية، من أكثر الأماكن المستهدفة من قبل مرتكبي جرائم السرقة والنصب والإحتيال، وتعد القطاعات الحكومية هي الهدف الذي يقصده الجواسيس. ويظهر هذا بصورة أكبر في القطاعات الخاصة بالقوات المسلحة نظرا لطبيعة وأهمية المعلومات التي تحتويها تلك القطاعات، ولا شك أن مرتكبي جرائم الإحتيال قد يقصدون المؤسسات المالية والقطاعات الحكومية على السواء.³

كما تعتبر البنوك من أهم القطاعات الأكثر تضررا إذ بلغت النسبة فيها 19% من مجموع الجرائم المرتكبة، بالإضافة إلى قطاعات المال، وتزداد رقعة الجريمة لتشمل الشركات الخاصة كشركات التأمين،

¹ - نهلا عبد القادر المومني، المرجع السابق، ص 93.

² - أحمد عبد اللاه المراغي، المرجع السابق، ص 117.

³ - خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص 150.

فقد شهدت لوس أنجلوس أشهر الجرائم في هذا النوع عندما تمكن أحد موظفي شركة تأمين كبرى بإستخدام نظامها الحاسوبي من خلق عملاء وهميين مؤمن عليهم، وتمكن من تحويل 46.000 بوليصة تأمين إلى شركة مناظرة.¹

ثانيا: المؤسسات العسكرية

لم تقتصر حدود ثورة المعلومات على القطاع المدني، بل كان لها أكبر أهمية في تطوير أنظمة الحرب الحديثة، وأدت إلى ظهور ما يسمى بحرب المعلومات.

حيث يستهدف هذا النوع من الإجرام الأهداف السياسية، فبالرغم من ندرة حدوثه عادة، إلا أنه موجود على أرض الواقع، وأفضل مثال عن ذلك نجاح الإنجليزي "نيكولاس أندرسون" من إختراق موقع البحرية الأمريكية وسرقة كلمات السر الخاصة المستخدمة في الهجوم النووي، وأيضا نجاح الألماني "هيس لأندر" في إختراق قاعدة بيانات البنتاجون وإستطاع الحصول على 29 وثيقة متعلقة بالأسلحة النووية.²

وأصبحت الدولة التي تملك المعلومات هي الدولة الأقوى، ولذلك بدأ الإهتمام ينصب على الجاسوسية العسكرية، وأصبح إطلاق الأقمار الصناعية من الجهات العسكرية هو المحور الذي يقوم عليه الإتجاه في تطوير الأجهزة والمعدات العسكرية، مما إستتبع ظهور حروب جديدة تسمى بحرب المعلومات بين الدول، وأصبحت المعلومات من خلال هذه الحرب هي السلاح الرئيسي، وبالتالي أدى تطوير صياغة التنظيمات الهجومية والدفاعية لحرب المعلومات، مما يجعل منظومة القوات المسلحة في الحروب المستقبلية والدفاعية لحرب المعلومات تتكون من قسمين رئيسيين هما:

1- التواجد الفعلي للقوات المسلحة في مسرح العمليات.

2- ظهور حرب في إتجاه آخر هي حرب المعلومات، المعنية بتجميع المعلومات وتيسير سبل الحصول عليها وتوزيعها، بالإضافة إلى إحتكارها بشكل مطلق والسيطرة على تدفق المعلومات لقوات الخصم.

¹ - هلال بن محمد بن حارب البورسعيدى، المرجع السابق، ص 49.

² - يوسف صغير، الجريمة المرتكبة عبر الأنترنت، مذكرة لنيل شهادة الماجستير في القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، الجزائر، 2013، ص 28.

وتعتمد آليات هذه الحرب على شبكات الحاسبات الآلية في نقل المعلومات، عن طريق الشبكات ومن خلال الأقمار الصناعية، حيث يؤدي ذلك بدوره إلى تعاظم دور القوات المسلحة، ونظم المعلومات في أنظمة التسليح، نظرا لاحتمية وأهمية تخزين البيانات وسرعة معالجتها وعرضها بصورة مناسبة أمام القادة لإتخاذ القرار المناسب على أساس أهمية تلك المعلومات.

وهذا ما جعل الدول تبادر إلى القيام بالتجسس على الدول الأخرى للحصول منها على المعلومات التي تجعلها قادرة على مواجهتها في أي وقت.¹

ثالثا: الأشخاص الطبيعيون

لا يقتصر تصنيف ضحايا الجرائم الإلكترونية على الأشخاص المعنوية، بل يتعدى أيضا إلى الأشخاص الطبيعيين، وبالتالي فإن كثيرا من الأشخاص يتعرضون لجرائم النصب، والسرقة والإتلاف، ومن الطبيعي أن تكون شبكة الأنترنت المجال الخصب لإرتكاب تلك الجرائم.

حيث أصبحت ملايين الأسرار المتعلقة بالناس، سواء كانوا أفرادا عاديين أو في مراكز معينة في متناول كل من يستطيع إختراق شبكة المعلومات التي تتطوي عليها كل هذه الأسرار.

وتعتبر جرائم الإتلاف عن طريق الفيروسات، من أكثر الجرائم التي يتعرض لها الأشخاص الطبيعيون عبر البريد الإلكتروني، والذي يعتبر من أهم البوابات التي يقفز منها القراصنة إلى أجهزة الحواسيب الخاصة بالأشخاص.

وخير مثال على ذلك وقوع الكثير من الشعب الأمريكي ضحية لجريمة النصب، من قبل الأشخاص مستغلين الحادث الإرهابي، الذي حدث في الولايات المتحدة الأمريكية في الحادي عشر من سبتمبر سنة 2001، حيث قامت العديد من الجهات بإنشاء عدة مواقع على شبكة الأنترنت بغرض جمع تبرعات للضحايا.²

وعلى هذا الأساس قامت حكومة الولايات المتحدة من تحذير رعاياها من الوقوع ضحايا لتلك العمليات الإجرامية.

¹ - خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص 102.

² - خالد ممدوح إبراهيم، المرجع نفسه، ص 103.

وفي الأخير ما يمكن استخلاصه أن شخصية المجرم المعلوماتي (المجرم الإلكتروني) تتم بخطورة إجرامية خطيرة، وذلك من خلال السمات والخصائص التي يتميز بها عن المجرم التقليدي، إذن فشخصيته متميزة ومن نوع خاص، وأمام الموقف السلبي للمجني عليه والمتمثل في إحجامه عن الإبلاغ عن الجرائم التي يرتكبها المجرم المعلوماتي، لذا يجب إتخاذ الإجراءات والتدابير اللازمة لردعه عن طريق سن قوانين صارمة لمواجهة هذه الشخصية الفريدة من نوعها.

المطلب الرابع: مبررات الحماية

إن التقدم التكنولوجي والعلمي حقق مزايا عديدة ومتنوعة في جميع ميادين الحياة، والفضل يرجع إلى ظهور الحاسوب وشبكة الأنترنت، لكن في المقابل خلفت جملة من الإنعكاسات السلبية والخطيرة جراء سوء إستخدام هذه التقنية، مما نتج عنها ظهور جرائم مستحدثة وخطيرة، تختلف جذريا عن الجرائم التقليدية، مما يستدعي التصدي لهذا النوع من الإجرام، ويمكن أن نقف على جملة من المبررات التي تقف وراء إقرار الحماية الجنائية لهذه الجرائم ويمكن إيجازها فيما يلي:

الفرع الأول: خطورة الجرائم الإلكترونية

تتميز الجرائم الإلكترونية بخطورتها في مختلف مجالات الحياة، منها الاقتصادية، والاجتماعية والنفسية، والصحية والعسكرية والأمنية، والسياسية لذا سوف نتناول هذا الفرع كما يلي:

أولاً: الأخطار الاقتصادية

تخلف الجرائم الإلكترونية خسائر كبيرة وضخمة من الناحية الاقتصادية، لوقوعها في معظم الأحوال على معلومات وبرامج ذات قيمة اقتصادية، سواء في ذاتها أو لارتباطها بأموال قيمة، مما يؤدي في الغالب إلى خسائر مادية فادحة، إذ يستخدم المجرم المعلوماتي الذكاء والتقنية في عملياته الإجرامية بدلا من الأسلحة، فإنه لا يتردد في القضاء على مؤسسة اقتصادية، بمجرد التعرف على رقم حسابها أو رقمها السري، ليستولي على مبالغ طائلة تفوق بكثير عما يستولي عليه المجرم التقليدي، فمثلا معدل ما يسرقه اللص العادي في الولايات المتحدة الأمريكية ما دون الـ (10) آلاف دولار، بينما أن معدل ما يسرقه المجرم المعلوماتي هو حوالي (45) ألف دولار.¹

¹ - رشاد خالد عمر، مرجع السابق، ص، ص 36 - 37.

وأما على صعيد الدول العربية، فإنه وبمقتضى دراسة أجرتها منظمة Soft Alliance Business في الشرق الأوسط، تبين بأن مجموع الخسائر المالية الناجمة عن الجرائم الإلكترونية في كل من المملكة العربية السعودية، والإمارات العربية المتحدة معا تقدر بـ 30 مليون دولار سنويا، وفي لبنان بـ 1.40000 دولار سنويا.¹

وأما في الجزائر وكغيرها من دول العالم ليست بمنأى عن الجرائم الإلكترونية، فقد كشفت إحصائيات قدمها مركز البحوث القانونية والقضائية التابع لوزارة العدل، إذ وصل عدد الهجمات اليومية على مختلف المواقع الإلكترونية منها مواقع رسمية وخاصة، مواقع هيئات وجرائد وطنية ومن بينها موقع جريدة "الشروق" الذي استعمل لبيع قطع أثرية لولاية عنابة وعرض صور خليعة عبر الأنترنت، كما تم اختراق منظومة البنك الجزائري والجمارك الوطنية من طرف شاب لديه خبرة ومهارة في مجال الإعلام الآلي وينحدر من ولاية أم البواقي إلى 3000 هجمة في الشهر.²

وقد قدرت خسائر الجزائر بـ 30 مليون دولار نتيجة قطع الأنترنت لمنع الغش في إمتحانات البكالوريا.

ثانيا: الأخطار الاجتماعية

إن خطورة الجريمة الإلكترونية لا تتوقف عند حدود الإقتصاد بل تتخطاها لتشمل النواحي الاجتماعية للأفراد والمجتمعات كآتي:

- المساس بالآداب والأخلاق العامة للمجتمع من خلال نشر الصور والأفلام الجنسية (الإباحية) على شبكة الأنترنت، فالعالم المعاصر يعيش ثورة جنسية طاغية تجاوزت كل الحدود والقيود، وقد قال جيمس رستون الصحفي في جريدة "نيويورك تايمز" بأنها ستكون في النهاية أشد فتكا من الطاقة النووية في خطورتها على المجتمعات البشرية، والسبب يرجع إلى بروز شبكة الأنترنت، التي لعبت دورا كبيرا في ربط العالم بأسره مع بعضه البعض، وجعلته بالأخص أمريكا وأوروبا يعيش جنونا جنسيا محموما في عالم الأزياء والأفلام والصور الجنسية الفاضحة، حتى أمسى الجنس هو الشغل الشاغل لعقول أغلب المجتمع

3- عبد الرحمان جلم حمزة، جرائم الأنترنت من منظور شرعي وقانوني، ظافر للتصميم والطباعة، بغداد، د ط، د.س.ن، ص22.

2- نبيلة هبة هروال، الأطروحة مرجع سابق، ص34.

البشري¹، فتمثل هذه الشبكة واحدة من الوسائل التي لها فاعلية وجاذبية لنشر الإباحية، واقتحامها لجميع البيوت والمكاتب، ولذلك فقد لجأ مروجو تجارة الجنس والإباحية إليها من أجل الحصول على أرباح طائلة.²

وبلا شك أن هذه المواقع والمواد الإباحية لها آثار سلبية على المجتمع والأفراد، فمن يتعرض لمشاهدة هذه المواقع فإنه في بادئ الأمر قد يرتاد على الموقع من حيث الفضول أو الخطأ، ومن ثم يبدأ بالإدمان عليها، وقد يصل به الأمر إلى ارتكاب الجرائم الجنسية والأخلاقية، ولهذا ذهب رأي فريق من الباحثين إلى أن هناك علاقة طردية ما بين مشاهدة هذه المواد، وارتكاب بعض الجرائم التقليدية، كالإعتداء على الآباء والأولاد جنسيا.³

وما يزيد من خطورة الأمر أن الوصول إلى هذه المواقع الخاصة بالإباحية، أصبح سهلا بشكل يمكن معه حتى للمراهقين والأطفال الوصول إليها.

- المساس بخصوصيات حياة الأفراد عن طريق المعالجة الإلكترونية للبيانات الشخصية، قصد إستغلالها في غير الذي جمعها من أجله أو نتيجة إختراق أجهزة الكمبيوتر والبريد الإلكتروني، وغيرها من الجرائم التي تشكل تهديدا، لخصوصيات وأسرار حياة الأفراد الشخصية والعائلية، وسواء أحدث هذا الإختراق من قبل الأفراد أو من قبل جهات حكومية، فإنها تعتبر بلا شك خرقا لأحد المبادئ الدستورية أو من قبل جهات حكومية.⁴

- المساس بسمعة وشرف وإعتبار الأفراد، عن طريق نشر صور مشينة لسمعتهم وشرفهم، سواء كانت تلك الصور حقيقية أو مزيفة، من خلال برامج تعديل الصور، أو عن طريق السب والشتم والتشهير عبر الأنترنت.⁵

¹- رشاد خالد عمر، المرجع السابق، ص38.

²- حسن طاهر داود، المرجع السابق، ص93.

³- عبد الوهاب ملياني، أمن المعلومات في بيئة الأعمال الإلكترونية، أطروحة لنيل شهادة الدكتوراه في القانون العام، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، الجزائر، 2016-2017، ص76.

⁴- رشاد خالد عمر، المرجع السابق، ص39.

⁵- علي بن عبد الله العسيري، المرجع السابق، ص47.

ثالثا: أخطار نفسية وصحية

تترك الجريمة بصفة عامة آثارا سلبية على نفسية ضحاياها، إلا أن الآثار السلبية التي توقعها الجريمة الإلكترونية على نفسية ضحاياها، في الغالب أشد وقعا من تلك التي توقعها الجرائم التقليدية، ومن أهم هذه الآثار:

- شعور المجني عليه بعدم الإرتياح النفسي، وذلك بضياح حقوقه وعدم إمكانية استرجاعها، لأن المجرم المعلوماتي يكون في الغالب مجهول الهوية، ويصعب إكتشافه وحتى وإن اكتشف فإنه لا يمكن إثبات جرائمه، كما يشعر المجني عليه دائما بأنه معرض لخطر هذه الجرائم الخطيرة، وأن خصوصياته وأسراره الشخصية والعائلية معرضة لخطر الإفشاء والإطلاع عليها من مستعملي شبكة الأنترنت، أو أن أمواله عرضة للسرقة والإختلاس، مما يجعله يشعر بعدم الثقة فيمن حوله من أصدقائه وزملائه في العمل، ممن يستعملون الحاسوب وشبكة الأنترنت.¹

كما أن خطورة هذه الجرائم لا تقف عند الحدود النفسية، بل تتعداها لينتج عنها أخطار صحية قد تؤدي أحيانا بحياة الأبرياء، ولعل أبرز مثال على ذلك ما قام به أحد المجرمين المعلوماتيين عند إختراقه لنظام معلوماتي لإحدى المستشفيات في الولايات المتحدة الأمريكية، حيث أنه قام بالعبث بملفات النظام، مما أدى إلى وفاة أحد المرضى بالمستشفى.²

رابعا: الأخطار العسكرية والأمنية والسياسية

- أما على الصعيد العسكري فإن الخطر الحقيقي لهذه الجرائم يتمثل، في جرائم التجسس الإلكتروني حيث بات بإمكان الكثير من الدول التي تملك التكنولوجيا أن تقوم بالتجسس، على المواقع والمنشآت العسكرية (السرية أو غير السرية) للدول الأخرى، من خلال أقمار صناعية، أو أجهزة تقنية متطورة ومعدة خصيصا لذلك.³

- على صعيد المخاطر الأمنية فإن بعضا من الجرائم الإلكترونية كالإرهاب الإلكتروني، وجرائم

1 - رشاد خالد عمر، المرجع السابق، ص41.

² - صالح بن محمد المسند، عبدالرحمان بن راشدا لمهيني، جرائم الحاسب الآلي كالخطر الحقيقي في عصر المعلومات، المجلة العربية للدراسات الأمنية والتدريب، أكاديمية نايف العربية للعلوم الأمنية، المجلد 15، العدد29، 1421، ص 174.

3- رشاد خالد عمر، المرجع السابق، ص 42.

غسيل الأموال عبر الأنترنت وغيرها، من الجرائم المنظمة أمست تشكل تهديدا حقيقيا للدول المعاصرة، خصوصا بعد أن أصبح هناك نوع من الارتباط الطبيعي ما بين الجريمة وشبكة الأنترنت، والذي هو ارتباط قابل للازدهار والتطور يوما بعد يوم، ذلك أن هذه الشبكة توفر للجريمة المنظمة القنوات والأهداف في آن واحد، وكذلك توفر لها أفضل الفرص لإستغلال هذه القنوات والأهداف، في سبيل تحقيق أكبر قدر ممكن من الأرباح، بأقل قدر ممكن من الخسائر والمخاطرة.¹

وعلى وجه العموم فإن جرائم الإرهاب الإلكتروني تعد من أخطر هذه الجرائم، فوسائل الإتصال الحديثة كالهواتف النقالة التي ترتبط بالأقمار الصناعية، وأنظمة المعلومات الإلكترونية الحديثة كالحاسب الآلي وشبكة الأنترنت، شائعة الإستعمال من قبل الجماعات الإرهابية مما ساعدتها على زيادة أنشطتها، كما أدت إلى زيادة في نطاق الإرهاب العابر للحدود، وذلك من خلال ضمانها لعنصر السرية الضرورية لأعمال هذه الجماعات، وعنصر الديمومة الضرورية لنقل أفكارها وتسهيل إتصالها بالجماهير، وكذا تمكنت من خلال الشبكة من تجنيد العديد من الأشخاص على وجه الخصوص الأحداث والمراهقين، كما ساعدتها على نشر عملياتها بالصوت والصورة، وفي التحريض على القتل والإرهاب، والحصول على التمويل اللازم لمواصلة عملياتها الإرهابية.²

- وأما المخاطر السياسية لهذه الجرائم فتتمثل في جرائم التشهير برؤساء ومسؤولي الدول ورموزها السياسية والقيادية، وذلك من خلال نشر أقوال وإشاعات بديئة وسيئة لسمعتهم، أو نشر صور مشينة لهم سواء أكانت هذه الصور حقيقة أو مزيفة، وذلك من أجل إضعاف ثقة مواطني دولهم بهم، وإضعاف نفوذهم على الصعيد الدولي.³ وكذلك من أجل زرع الفتن والإضطرابات والإخلال بالاستقرار السياسي في دول الضحايا، حتى باتت هناك مواقع إلكترونية متخصصة بالسب والقذف والتشهير عبر شبكة الأنترنت.

¹ - عبد الله عبد الكريم عبدالله، جرائم المعلومات والأنترنت (الجرائم الالكترونية)، منشورات الحلبي الحقوقية، بيروت، ط1، 2007، ص 42.

² - رشاد خالد عمر، المرجع السابق، ص، ص 42 - 43.

³ - منير محمد الجنيبي وممدوح محمد الجنيبي، جرائم الأنترنت والحاسوب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، د ط، 2006، ص 34.

الفرع الثاني: قصور القوانين التقليدية

قلبت الجريمة الإلكترونية العديد من المفاهيم القانونية السائدة، سواء على المستوى الموضوعي من حيث التجريم والعقاب، بفعل إزدواجية طبيعتها بين جريمة إلكترونية محضة تستهدف الأنظمة والبيانات الإلكترونية في حد ذاتها، أو كجريمة عادية مرتكبة بواسطة تقنية المعلومات لتنفيذ المشاريع الإجرامية، أو على مستوى القانون الإجرائي، بفعل تغلبها على القواعد الإجرائية المقررة لملاحقة الجرائم العادية، مما يتعين القول بأن الإجماع المعلوماتي قد أحدث ثورة في فلسفة التجريم والعقاب وقوانين الإجراءات الجزائية.¹

أولاً: عدم كفاية القوانين العقابية التقليدية

إن الطبيعة الفنية للجريمة الإلكترونية تجد صعوبة في تطبيق القواعد القانونية التقليدية، بمعنى عدم ملائمة القوانين القائمة بتطبيقها على هذا النوع من الجرائم، بسبب أن القانون الجنائي لا يتطور بنفس السرعة التي تتطور بها التكنولوجيا أو مهارة الذهن البشري في تسخير المبتكرات للاستخدام السيء²، ومن ثم فإن القانون الجنائي التقليدي لا يكفي من حيث المبدأ لمواجهة هذا الشكل الجديد من الإجرام، وخاصة أن النصوص التقليدية قد وضعت لتطبيق وفقاً لمعايير معينة (منقول مادي)³، فثمة أفعال ترتكب بالوسائل التقنية، لا يمكن خضوعها للقوانين العقابية التقليدية، على الرغم من تهديدها للمصالح العامة والنظام العام، كأفعال إنتهاك حرمة أو خصوصية الغير، أو الإطلاع على البيانات ونسخها⁴ كما أن الدخول إلى حاسب مملوك للغير، وسرقة المعلومات منه لا تعتبر جريمة بمفهوم القوانين التقليدية، بإعتبار السرقة ترد على المال المنقول، بعكس سرقة المعلومات التي تعتبر أفكار معنوية بحتة، زيادة على ذلك أن فعل السرقة يعني تجريد الغير من ماله في حين إختلاس المعلومات يتمثل في أخذ نسخة منها مع الإبقاء بأصلها عند صاحبها، إذا فهي مستبعدة من التجريم المقرر لجرائم الأموال، والشيء نفسه

¹ - عبد الرحمن اللمتوني، الإجرام المعلوماتي بين ثبات النص وتطور الجريمة، سلسلة ندوات محكمة الاستئناف بالرباط، العدد 7، 2014، ص48.

² - تركي بن عبد الرحمن المويشير، المرجع السابق، ص88.

³ - مريم محمد آل علي، وقائع الجرائم الإلكترونية المتعلقة بالآداب العامة عبر الأنترنت - دراسة ميدانية-، مركز البحوث الشارقة، الشارقة، د ط، 2009، ص64.

⁴ - لينا محمد الأسدي، المرجع السابق، ص147.

قيل في عدم وقوع جريمة الإلتلاف على الكيانات غير المادية للوسائل الإلكترونية كالبيانات والبرنامج.¹ ومن جهة أخرى فإن هذه الجرائم قد تمس بأهم مبدأ في القانون، وهو مبدأ الشرعية الجزائية الذي ينص على "لا جريمة ولا عقوبة إلا بالنص" بحيث يمكن تعريض القضاء لأن يسير في أحد الاتجاهين، إما أن يطبق النص التقليدي على هذا النوع من الجرائم، فيقع في القياس المحذور، أو أن يقف مكتوف الأيدي أمام هذا النوع من الجرائم في ظل عدم قدرته، على خلق جرائم وعقوبات إعمالاً بمبدأ الشرعية،² مما يؤدي إلى إفلات الجاني من العقاب، ومن أمثلة ذلك ما وجده القضاء المغربي عندما طرحت عليه قضايا تتعلق بالجرائم الإلكترونية، تتمثل في قضية تتعلق بحائز لبطاقة الائتمان والأداة استعمالها بصورة تعسفية، وذلك استناداً للفصلين 540 و 574 من مجموعة القانون الجنائي المتعلقين بالنصب وخيانة الأمانة، حيث تمت إدانته بثلاث سنوات حبساً، لكن القضاء الاستئنافي برأ ساحة المتهم بحجة أن العناصر المكونة لهذه الجرائم لا تتوفر في القضية المعروضة على القضاء.³

لذا إن عدم مواكبة القوانين العقابية للتطورات الحاصلة في مجال الجرائم الإلكترونية، يؤدي إلى إتخاذ سبيل التفسير الموسع للنصوص التقليدية التي يجب أن تتم صياغتها واضحة ودقيقة، ليبعد عنها الغموض الذي قد يعتريها⁴، وبالتالي فتحمل النص أكثر من الدلالة التي يبتغيها المشرع يعتبر خروجاً عن مبدأ الشرعية الجنائية، وكذلك الخروج عن مبدأ التفسير الضيق للنصوص العقابية بإعتباره أحد نتائج مبدأ الشرعية، إذ ترك الأمر بيد القضاء لتفسير هذه النصوص القائمة على نحو أوسع من الذي وضعت من أجله، لأن تفسير النصوص تفسيراً ضيقاً يمنع إمتداد هذه القواعد إلى الجرائم الإلكترونية، على إعتبار أن هذه الجرائم لم تتطرق إلى ذكر هذه الطائفة من الجرائم، بإعتبارها أحد صور الجرائم المنصوص عليها في قانون العقوبات، هذا العجز الذي أثبتته القوانين العقابية التقليدية في مواجهة هذه الجرائم المستحدثة، حاولت بعض الدول المتقدمة إستدراك الوضع بسن تشريعات تتلاءم مع هذه الجرائم فمنها من فضلت

¹ - جمال إبراهيمي، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة لنيل شهادة الدكتوراه في العلوم، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، الجزائر، 2018، ص 221.

² - أحمد أسامة حسينة، الجريمة الإلكترونية بين الشرعية الجنائية والإجرائية، مجلة جامعة الأزهر، غزة، المجلد 19، عدد خاص بمؤتمر كلية الحقوق الخامس المحكم، 2017، ص 19.

³ - أمين عزان، الجريمة المعلوماتية، ورقة علمية قدمت للمؤتمر العلمي المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، ليبيا، المنعقد في الفترة من 28-29/10/2009، ص 3.

⁴ - أحمد أسامة حسينة، المرجع السابق، ص 21.

تعديل قوانينها العقابية وإضافة نصوص جديدة إليها لسد الفراغ التشريعي، ومنها من قامت بإستحداث نصوص جديدة خاصة بهذا النوع المستجد من الإجرام، غير أن الملاحظ في هذه القوانين لا تشمل كافة الأفعال غير المشروعة المرتكبة بواسطة الوسائل التقنية، كما أن بعض الدول ما زالت تطبق القوانين القائمة رغم ثبوت قصورها.¹

ثانيا: عدم ملائمة الإجراءات التقليدية

بعدما تعرضنا للمشكلات الموضوعية التي تثيرها الجرائم الإلكترونية، عند تطبيق القواعد التقليدية نجد قصورا كذلك في القوانين الإجرائية، إذ معظم الإجراءات التي تتضمنها التشريعات التقليدية لا تتلاءم وطبيعة الجريمة الإلكترونية، لأنها ترتكب في مسرح إلكتروني أو مجال مفرغ يختلف كليا عن المسرح التقليدي الذي ترتكب فيه الجريمة التقليدية، حيث يتم الإستدلال عليها وضبطها وإثباتها بالوسائل التقليدية المتمثلة في إجراءات الإستدلال والتحقيق²، فهي إجراءات صيغت لضبط وإثبات جرائم ترتكب في عالم ملموس ماديا، يلعب فيه السلوك المادي الدور الأكبر، بعكس الجريمة الإلكترونية ترتكب في عالم إفتراضي غير ملموس، أما إذا ارتكبت عبر شبكة الأنترنت تزداد العقبات القانونية صعوبة، لأننا سنقف أمام مشكلات إجرائية لضبط الجريمة وإثباتها، لأنها تتعلق ببيانات معالجة إلكترونيا وكيانات منطقية غير مادية، مما يصعب كشف هذه الجرائم، إضافة إلى دقة وسرعة تنفيذ هذا النوع من الجرائم، مع إمكانية محو آثارها، وإخفاء الأدلة المتحصلة عنها عقب التنفيذ مباشرة، مما يخلق صعوبات أمام الجهات القائمة بالتفتيش وجمع الأدلة، هذه الأخيرة تتعلق ببيانات مخزنة في أنظمة أو شبكات إلكترونية، موجودة خارج الدولة التي يجري التحقيق فيها للدخول إليها، ومحاولة جمعها وإجراء التحقيق بشأنها، أو مشكلات تتعلق بسيادة الدولة أو الدول الأخرى التي توجد لديها هذه البيانات، وفي هذه الحالة يحتاج الأمر إلى تعاون دولي في مجال البحث والتفتيش وجمع الأدلة وتسليم المجرمين³، فكل هذه المشاكل التي تثيرها الجريمة الإلكترونية نتناولها في الباب الثاني من هذا البحث.

¹ - جمال براهيم، المرجع السابق، ص 223.

² - رحاب عميش، الجرائم المعلوماتية، بحث مقدم إلى المؤتمر الأول حول "المعلوماتية والقانون"، "أكاديمية الدراسات العليا، طرابلس، ليبيا، المنعقد في الفترة بين 28-29/ 10/ 2009، ص 25.

³ - لينا محمد الأسدي، المرجع السابق، ص 184.

المبحث الثاني: المرجعيات المؤطرة¹ للجرائم الإلكترونية وتأثر المشرع بها

أصبحت الجرائم الإلكترونية حقيقة خطيرة تهدد العالم بأسره، وأمام الصعوبات الكبيرة التي واجهت الدول في مكافحة هذه الجرائم عبر قوانينها الداخلية، وفي مواجهة أصعب خاصية لها كونها جريمة عابرة للحدود²، وإزاء ذلك كان من الضروري أن توحّد الجهود في مواجهة الإجرام المعلوماتي، وذلك من خلال العمل على إنشاء أرضية قانونية تعمل على دعم الجهود الدولية لمكافحة الجريمة الإلكترونية³، فتكللت الجهود ببروز منظمات دولية وإقليمية، مهمتها عقد المؤتمرات والاتفاقيات في هذا الخصوص، والجزائر على غرار الدول الأخرى تأثرت بالتطورات الحاصلة في مجال مكافحة الجريمة الإلكترونية، فأثرت منظومتها التشريعية عن طريق المصادقة على مجموعة من الاتفاقيات الدولية والإقليمية، لذا سيتم تقسيم هذا المبحث إلى دراسة الجهود الدولية في مكافحة الجريمة الإلكترونية (المطلب الأول) والجهود الإقليمية في (المطلب الثاني) وتأثر الجزائر بالجهود الدولية في (مطلب ثالث).

1 - أيوب اللبار، السياسة الجنائية في مواجهة جرائم المس بنظم المعالجة الآلية للمعطيات، كلية العلوم القانونية والاقتصادية والاجتماعية، جامعة سيدي محمد بن عبد الله، فاس، منشور على الموقع: droit.entrprise.com أطلع عليه يوم 2020/10/13 على الساعة 10h:30.

2 - أيوب اللبار، المرجع نفسه، د ت ص.

3 - فيصل بدري، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، أطروحة لنيل شهادة دكتوراه علوم، كلية الحقوق، جامعة الجزائر 01، 2017-2018، ص 8.

المطلب الأول: الجهود الدولية لمكافحة الجريمة الإلكترونية

حظيت مكافحة الجريمة الإلكترونية بإهتمام دولي، وباعتبارها من الجرائم العابرة للحدود، مما أكسبها الطابع العالمي، ما أدى بأعضاء المجتمع الدولي إلى التصدي لها سواء، من خلال جهود الأمم المتحدة التي بدلت جهودا لا يستهان بها في مجال محاولة التصدي للجرائم الإلكترونية، وذلك من خلال إشرافها على عقد المؤتمرات الدولية الخاصة بمنع الجريمة ومعاملة المجرمين، ومن خلال الوكالات والمنظمات العاملة تحت لوائها.¹

الفرع الأول: جهود الأمم المتحدة لمكافحة الجريمة الإلكترونية

لقد نظمت الأمم المتحدة عدة مؤتمرات دولية، محاولة تقديم توصيات توضح من خلالها المخاطر الناجمة عن استخدام المعلوماتية، وتبين الإجراءات التي يجب على الدول الأخذ بها قصد مواجهة هذه الجرائم وأبرز هذه الجهود تتمثل فيما يلي:

أولا: مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين هافانا 1990

في عام 1955 كلف مؤتمر الأمم المتحدة السابع الذي انعقد في ميلانو بإيطاليا، لجنة الخبراء العشرين بدراسة موضوع حماية نظم المعلومات والإعتداء على الحاسب الآلي، فأقرت مجموعة من المقترحات والتوصيات لمكافحة الظواهر الإجرامية المتعلقة بالحاسب الآلي، وقد تبنى مؤتمر هافانا الثامن من العام 1990 هذه التوصيات بعد أن أدخل عليها بعض التعديلات، أضاف عليها بعض المقترحات، وقد أكد هذا الأخير على ضرورة الاستفادة من التطورات العلمية والتكنولوجية، في مواجهة هذه الحركة، وأشار إلى مسألة الخصوصية واختراقها بالإطلاع على البيانات الشخصية، المخزنة داخل نظم الحاسوب، وضرورة اعتماد ضمانات لصون سريتها، كما أكد على ضرورة تشجيع التشريعات الحديثة التي تتناول هذه الجرائم بصفاتها نمطا من أنماط الجريمة المنظمة²، وأهم توصيات مؤتمر هافانا تتمثل: في تحديث القوانين الجنائية الوطنية بما في ذلك التدابير المؤسسية، وتحسين أمن الحاسب الآلي و التدابير المنعوية، واعتماد إجراءات تدريب كافية للموظفين و الوكالات المسؤولة عن منع الجريمة الإقتصادية و الجرائم المتعلقة بالحاسب الآلي و التحري والإدعاء فيها، وكذا اعتماد سياسيات تعالج المشكلات المتعلقة بالمجني

¹ _محمود أحمد عبانة، المرجع السابق، ص 155.

² _محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي القانون الجزائري، المرجع السابق، ص 53.

عليهم في تلك الجرائم، مع التأكيد على زيادة التعاون الدولي من أجل مكافحة هذه الجرائم.

ثانيا: المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات

انعقد هذا المؤتمر في البرازيل "ريو دي جانيرو"، في الفترة الواقعة من 4 إلى 9 أكتوبر عام 1994 وقد خرج بالعديد من التوصيات، منها ما يتعلق بوضع قائمة بالحد الأدنى للأفعال المتعين تجريمها وإعتبارها من قبيل جرائم الكمبيوتر، كجريمة الإحتيال والغش المرتبط بالكمبيوتر، من خلال إتلاف ومحو المعطيات، وأيضا ما يعرف بالتزوير المعلوماتي ويشمل إتلاف ومحو البرامج والبيانات وتعطيل وظائف الكمبيوتر ونظام الاتصالات أو الدخول غير المصرح به عن طريق انتهاك إجراءات الأمن.¹

أما من الناحية الإجرائية فإن القرار الصادر عن المؤتمر الدولي العاشر للجمعية الدولية لقانون العقوبات، تضمن جملة من القواعد الإجرائية في بيئة الجرائم الالكترونية، من بينها القيام بإجراء التفتيش والضبط في بيئة تكنولوجيا المعلومات، وأيضا تفتيش شبكات الحاسب الآلي، وكذا التعاون الفعال بين المجني عليهم والشهود وكذا مستخدمي من أجل إتاحة استخدام المعلومات للأغراض القضائية، إلى جانب إعتراض الإتصالات داخل نظام الحاسب الآلي ذاته وممارسة الرقابة عليها.²

ثالثا: المؤتمر العاشر

إن تزايد الجرائم الإلكترونية وما تثيره من مشاكل، أدى إلى عقد الإتفاقية الخاصة بمكافحة إساءة إستعمال التكنولوجيا لسنة 2000، أين أكدت على الحاجة إلى تعزيز التنسيق والتعاون بين الدول في مكافحة إساءة استعمال التكنولوجيا لأغراض إجرامية، والعمل على إتخاذ تدابير مناسبة للحد من أعمال القرصنة.³

¹ _ ليندة شرايشة، السياسية الدولية والإقليمية في مجال مكافحة الجريمة الالكترونية والاتجاهات الدولية في مكافحة الجريمة الالكترونية، دراسات وأبحاث، المجلد 1، العدد 1، 2009، ص 246.

² _ عبد الله عبد الكريم عبد الله، المرجع السابق، ص 114.

³ _ اتفاقية مكافحة استعمال تكنولوجيا المعلومات لأغراض إجرامية، رقم 155/63، الصادرة عن هيئة الأمم المتحدة، الجلسة العامة 81 ديسمبر 2000.

رابعاً: المؤتمر الثاني عشر لمنع الجريمة والعدالة الجنائية لعام 2010

عقد هذا المؤتمر في سلفادور بالبرازيل، من 17-19 أبريل 2010 تحت عنوان "استراتيجيات شاملة لتحديات عالمية"، حيث ناقشت فيه الدول الأعضاء بتعمق مختلف التطورات الأخيرة في استخدام العلم والتكنولوجيا، من جانب المجرمين والسلطات المختصة الجريمة، بما في ذلك الجريمة الإلكترونية حيث احتل هذا النوع من الجرائم إهتماماً بارزاً في جدول أعمال المؤتمر، وذلك تأكيداً على خطورتها والتحديات التي تطرحها.¹

وعليه تبدل الأمم المتحدة مجهودات جبارة من خلال المؤتمرات الدولية التي تنظمها، كمحاولة منها للتصدي للجرائم الإلكترونية، مؤكدة على وجوب تعزيز التعاون بين الدول من الحد من انتشار هذا النوع من الإجرام، فهي تعمل على صياغة معاهدة دولية جديدة لمكافحة الجرائم الإلكترونية، بعد أن وافقت الجمعية العامة على هذا القرار رغم إعتراض كل من الإتحاد الأوروبي والولايات المتحدة الأمريكية ودول أخرى، وينشئ القرار لجنة خبراء تمثل جميع مناطق العالم لوضع إتفاقية دولية شاملة لمكافحة استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية.²

الفرع الثاني: دور المنظمة العالمية للملكية الفكرية

تعد المنظمة العالمية للملكية الفكرية³، إحدى الوكالات التابعة للأمم المتحدة، وقد إهتمت هذه المنظمة في دعم الملكية الفكرية في جميع أنحاء العالم، بهدف تشجيع النشاط الإبتكاري، وتطوير إدارة

¹ مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية، البند الثامن من جدول الأعمال المؤقتين التطورات الأخيرة في استخدام العلم والتكنولوجيا من جانب المجرمين والسلطات المختصة في مكافحة الجرائم الإلكترونية، المنعقد بالبرازيل 12-19 أبريل 2010 رقم A/conf.213/09

² بنهاية عام 2019 أقرت الجمعية العامة للأمم المتحدة مشروع قرار بخصوص صياغة معاهدة دولية جديدة لمكافحة جرائم الانترنت، وينص هذا القرار على إجتماع اللجنة لمدة 3 أيام في اغسطس وآب 2020 في مدينة نيويورك للاتفاق على الخطوط العريضة لأنشطتها وعلى خطة وإجراءات عملها في المستقبل، حيث تم التصويت على هذا القرار بأغلبية 79 صوتاً مقابل 60... صوتاً وإمتناع 33 عن التصويت. للمزيد من التفصيل أنظر جريدة العين الإخبارية. مقال بعنوان هل المجتمع الدولي بحاجة إلى تشريع جديد بخصوص الجرائم السيبرانية، موجود على الموقع: www.united-ain.org/article. Com nat.... أطلع عليه في 2020/03/15 على الساعة 10.00.

³ تأسست هذه المنظمة بموجب إتفاقية ستوكهولم سنة 1967م، وأصبحت إحدى الوكالات المتخصصة التابعة للأمم المتحدة إعتباراً من 17 ديسمبر عام 1974 ويرمز إليها بمصطلح "wipo" world intellectual property organization مقرها جنيف.

الإتحادات المنشأة في مجالات حماية الملكية الصناعية وحماية المصنفات الأدبية والفنية.¹

وإهتمت هذه المنظمة في المجال المعلوماتي بتوفير الحماية القانونية لبرامج الحاسب الآلي، وقواعد البيانات بإعتبارها من المصنفات الأدبية والفنية، والتي تنبئ عن إبداع فكري لمصمميها أو مبتكريها، بعد أن استقر الرأي بعدم إمكانية توفر الحماية في تشريعات براءات الاختراع، ثم الإتفاق بتوفيرها بواسطة الإتفاقيات العالمية وخاصة إتفاقية "تريبس"² وبرن³، اللتان حثتا فيهما الدول الأعضاء على ضرورة تطوير تشريعاتها، خاصة تشريعات حق المؤلف، وكذلك وضع عقوبات على كل أعمال تزوير في العلامات التجارية والقرصنة المتعمدة والمركبة في إطار تجاري، ويعتبر الأنترنت من الأماكن الخصبة، لهذا النوع من التصرفات والتي وفرت بموجبها الحماية القانونية للبرامج وقواعد البيانات المعلوماتية.⁴

وقد نصت المادة 4 من معاهدة المنظمة العالمية للملكية الفكرية والمعتمدة في سنة 1996 على أنه: «تتمتع برامج الحاسوب بالحماية بإعتبارها مصنفات أدبية في معنى المادة الثانية من إتفاقية برن، وتطبيق تلك الحماية على برامج الحاسوب أيا كانت طريقة التعبير عنها أو شكلها» وتتص المادة الخامسة على أنه: «تتمتع مجموعات البيانات أو المواد الأخرى بالحماية بصفتها هذه أيا كان شكلها إذا كانت تعتبر ابتكارات بسبب اختيار محتوياتها أو ترتيبها».⁵

¹ محمد أحمد عبانبة، المرجع السابق، ص 159.

² تشكل الاتفاقية المتعلقة بالجوانب التجارية للملكية الفكرية المعروفة اختصارا باتفاقية ترس أبرز مظاهر التقنية الموحد لقوانين الملكية الفكرية بشقيها، الملكية الادبية والفنية والملكية الصناعية والتجارية، ويرى البعض أنها صيغت بهدف عولمة الاقتصاد وإزالة العراقيل التي كانت تحول دون المضي في تحرير التجارة الدولية وابرمت هذه الاتفاقية بمدينة مراكش سنة 1994 وهي ملحق للاتفاقية المنشئة للمنظمة العالمية للتجارة wto للمزيد من التفصيل انظر: نجاه بن مكي، المرجع السابق، ص 96 وما بعدها.

³ أبرمت إتفاقية برن في سبتمبر 1886، وكملت في باريس 1896، وعدلت في برلين في 13 نوفمبر 1908، ثم كملت في برلين 20 مارس 1994م، والمعدلة في روما في جوان 1928م وبروكسل سنة 1948 وستوكهولم في جويلية 1967 وباريس 1971 وكان عدد اعضاء الدول المنظمة إليها 140 دولة منها 10 دول عربية.

وانضمت الجزائر إلى اتفاقية برن بموجب المرسوم الرئاسي رقم 431/97 المتضمن انضمام الجزائر بتحفظ إلى اتفاقية برن لحماية المصنفات الأدبية والفنية، الجريدة الرسمية، عدد 61، الصادرة بتاريخ 14/09/1997.

⁴ يوسف صغير، المرجع السابق، ص 98.

⁵ عبد الله عبد الكريم عبد الله، الحماية القانونية لحقوق الملكية الفكرية على شبكة الانترنت دراسة في الأطر القانونية للحماية مع شرح النظام القانوني للملكية الفكرية في التشريعات المصرية والاردنية والاوربية والأمريكية ومعاهدي الانترنت، دار الجامعة الجديدة، الإسكندرية، د ط، 2008، ص 263.

ساد الإتجاه لدى أغلب الدول الصناعية ودول العالم الثالث إلى الميل إلى خضوع برامج الحاسب الآلي لقوانين حماية حق المؤلف، ومنذ ذلك العام حتى الآن عدلت معظم الدول تشريعاتها الخاصة بحق المؤلف، وأضافت برامج الحاسب الآلي إلى المصنفات الأدبية المحمية وفقا للقانون، وذلك نتيجة لإستمرار لجان الخبراء في دراسة الأسلوب المناسب لحماية البرامج الخاصة بالحاسب الآلي ومسائلهما الفنية عبر الإجتماعات المتكررة وبالتعاون ما بين الويبو واليونسكو.¹

الفرع الثالث: الإتحاد الدولي للاتصالات

يلعب الإتحاد الدولي للاتصالات بوصفه وكالة متخصصة داخل منظمة الأمم المتحدة، دورا بارزا بشأن تقييس وتنمية الاتصالات، كما يوفر الإتحاد الدولي للاتصالات الذي يضم 192 دولة و 700 شركة من القطاع الخاص والمؤسسات الأكاديمية، منبرا استراتيجيا للتعاون بين أعضائه، ويعمل الإتحاد على مساعدة الحكومات في الإتفاق على مبادئ مشتركة تفيد الحكومات والصناعات التي تعتمد على تكنولوجيا المعلومات والبنية التحتية للاتصالات²، وله دور كبير لمكافحة الإجرام المعلوماتي من خلال دوره الرائد في عقد العالمية لمجتمع المعلومات، والذي جاء عبر مرحلتين الأولى في جنيف بسويسرا سنة 2003 وعقد الآخر في تونس العاصمة سنة 2005، وقد وضع الإتحاد الدولي للاتصالات مخططا لتعزيز الأمن يتكون من سبعة أهداف رئيسية هي:³

-وضع إستراتيجية لتطوير نموذج مشترك للتشريعات السيرانية يكون قابلا للتطبيق وطنيا وعالميا.
-تهيئة الأرضية الوطنية والإقليمية المناسبة لوضع الهياكل التنظيمية والسياسات المتعلقة بالجرائم الالكترونية.

-وضع آلية عالمية للمراقبة الإلكترونية والإنذار والرد المبكر مع ضمان التنسيق عبر الحدود.
-إنشاء نظام هوية رقمي عالمي وتطبيقه، مع تحديد الهياكل التنظيمية اللازمة لضمان الإعراف

¹ _محمد أحمد عبانية، المرجع السابق، ص 161.

² _جورج لبكي، المعاهدات الدولية للإنترنت حقائق وتحديات، مجلة الدفاع الوطني اللبناني، عدد 83، بيروت، 2014، ص، ص 12-13.

³ _فهم الجريمة السيرانية دليل البلدان لنامية، مشروع أبريل 2009، الإتحاد الدولي للاتصالات شعبة تطبيقات تكنولوجيا المعلومات والاتصالات والأمن السيرافي، دائرة السياسات والاستراتيجيات، ص 3، منشور على الموقع www.itu.int/itu-d/cyb/cybersecueity/legislation.html أطلع عليه يوم 2018/11/12 على الساعة 14h 30.

بالوثائق الرقمية للأفراد عبر الحدود الجغرافية.

-تطوير إستراتيجية عالمية للإسراع في رفع المؤهلات البشرية والمؤسسية وتعزيز المعرفة والدراسة والتحسيس في مجال الاجرام المعلوماتي.

-اعتماد إطار استراتيجي عالمي لجميع الفاعلين والمهتمين بالإجرام الإلكتروني من أجل التعاون والحوار، تبادل المعارف والخبرات، والتنسيق على كل المستويات في هذا المجال.

المطلب الثاني: الجهود الإقليمية لمواجهة الجريمة الإلكترونية

إن خطر الجريمة الإلكترونية وشدة انتشارها جعل الدول تكتف جهودها على مستوى أقاليمها، خاصة الأوروبية منها، وبرزت على المستوى الإقليمي عدة جهود لمكافحة الجريمة الإلكترونية، من أجل وضع قواعد للحد من هذه الجرائم، وسوف نتناول بالدراسة في هذا المطلب، كلا من جهود المجلس الأوروبي الذي يحاول تكريس وجوب التعاون بين أعضاء الاتحاد لمواجهة هذا النوع المستحدث من الإجرام، سواء فيما بينهم أو بالتنسيق مع هيئات ومنظمات دولية أخرى، وكذا الجهود العربية المبذولة لمواجهة هذه الجرائم.

الفرع الأول: دور المجلس الأوروبي في مكافحة الجريمة الإلكترونية

لعب المجلس الأوروبي دورا مهما في مكافحة الجرائم الإلكترونية، حيث إهتم بمخاطر الحاسب الآلي منذ نهاية الستينيات، فعبر وزراء الدول الأعضاء في المجلس المشاركون في مؤتمره المنعقد عام 1968، عن اهتمامهم بمسألة حماية الخصوصية ضد مخاطر الحاسب الآلي، وصدر في عام 1973 القرار رقم 22-73 الخاص بحماية الحياة الخاصة، من أخطار بنوك المعالجة آليا في القطاع الخاص، وانطوى على توجيهات بشأن وجوب توفير قواعد تكفل حماية للبيانات الشخصية من مخاطر المعالجة الإلكترونية¹، واستمر جهد المجلس بهذا الخصوص ففي 17 سبتمبر 1980 قام بتوقيع معاهدة مجلس أوروبا والمتعلقة بحماية الأشخاص من مخاطر المعالجة الآلية للبيانات ذات الطبيعة الشخصية، وقد وضعت هذه الاتفاقية للتوقيع في جانفي 1981، وقد بدأ العمل الفعلي بها في أكتوبر 1985 ويقتصر نطاق تطبيق هذه الإتفاقية على الأشخاص الطبيعيين، وتسري على القطاعين الخاص والعام بشأن

¹ _لمى عبد الباقي محمود، المرجع السابق، ص 299.

الملفات المعدة آليا، إذ تحظى بإلزامية أحكامها لتحقيق حماية البيانات الشخصية المعالجة آليا.¹

كما صدر عن المجلس الأوروبي العديد من التوصيات لتؤكد على توسيع الحماية لتشمل قطاعات الأنشطة الخاصة بالبيانات الطبية والبحثة والإحصائية، ومن أبرز تلك التوصيات، التوصية رقم 80/13 R لسنة 1980 الخاصة بتبادل المعلومات القانونية المتصلة بحماية البيانات الطبية المعالجة آليا في بنوك المعلومات، والتوصية رقم R 83/10 عام 1983 والخاصة بحماية البيانات الشخصية المستعملة للبحوث العلمية.²

بالإضافة إلى ما سبق، فقد صدر عن المجلس الأوروبي العديد من القواعد التوجيهية في مجال جرائم الحاسب الآلي، تضمنت وجوب تجريم العديد من السلوكيات التي تعد من الجرائم، كالغش المعلوماتي وتزوير المعلومات، وسرقة الأسرار المخزنة والتوصل غير المصرح به، وسرقة منفعة الحاسب، كذلك تضمنت هذه القواعد عددا من الإجراءات الفنية التي يتوجب اتخاذها، بهدف الحيلولة دون الوصول غير المرخص به إلى المعلومات المخزنة، كحماية كلمة السر المستخدمة في النهايات الطرفية وحماية الأوامر الخاصة بالتشغيل وترميز المعلومات الشخصية وأسماء من تتعلق بهم.³

غير أن الحدث الرئيسي الذي توج به المجلس الأوروبي جهوده، تقديم اللجنة الأوروبية لمشكلات الجريمة ولجنة الخبراء في مجال جرائم التقنية سنة 2000 بمشروع اتفاقية الجرائم الالكترونية، وخضعت مواد الاتفاقية المقترحة للمناقشة، وتبادل الآراء خلال الفترة من إصدار مشروعها الأول حتى إعداد مسودتها النهائية، التي أقرت لاحقا في بودابست 2001 وعرفت باتفاقية بودابست 2001.⁴

الفقرة الأولى: إتفاقية بودابست

إن إتفاقية مجلس أوروبا للجريمة الإلكترونية، تعد أول مبادرة عالمية وأبرز وأنجح ثمرات التعاون الدولي في هذا المجال حتى الآن، وتعد هذه الإتفاقية دعوة موجهة إلى دول العالم، إلى تبني سياسة جنائية مشتركة من أجل مكافحة الجريمة الإلكترونية، واستلهاهم الدول قوانينها الداخلية من هذه الاتفاقية، وهذا ما فعله المشرع الجزائري لوضع إستراتيجيته لمكافحة الإجرام الإلكتروني، فمعظم قوانينه مستقاة من

¹ -محمود أحمد عبانبة، المرجع السابق، ص 220.

² - لمى عبد الباقي محمود، المرجع السابق، ص 300.

³ -محمود احمد عبانبة، المرجع نفسه، ص 164.

⁴ -نجاة بن مكي، المرجع السابق، ص 121.

هذه الإتفاقية، على الرغم أنه لم يصادق عليها حتى الآن.

فمنذ 1996 قرر مجلس أوروبا إنشاء لجنة الخبراء¹، مهمتها صياغة وسيلة قانونية متعلقة بمكافحة الجرائم الالكترونية، لكن هذه الاتفاقية لم تظهر إلى الوجود إلا بتاريخ 25 ماي 2001².

وأقرت اللجنة الوزارية لمجلس أوروبا في دورتها رقم 109 بتاريخ 8 نوفمبر 2001 الاتفاقية الأوروبية للجريمة الالكترونية وتم فتح التوقيع للانضمام إلى هذه الاتفاقية في مؤتمر دولي في مدينة بودابست المجرية في 23 نوفمبر 2001³، وفي هذا التاريخ وقعت على الاتفاقية ثلاثون دولة منها دول أعضاء في المجلس الاوروبي، إضافة إلى الولايات المتحدة الأمريكية، كندا، اليابان، وجنوب إفريقيا ولكن لم تدخل حيز التنفيذ حتى عام 2004⁴.

فالإتفاقية هي في الأصل أوروبية الميلاد، إلا أنها تحمل الطابع الدولي، لأنها مفتوحة لكل الدول التي تريد الإنضمام إليها من غير الدول الأوروبية، إلا أن هذه الدعوة للانضمام لا تسلخ عنها أنها اتفاقية ثم اعدادها في إطار المجموعة الأوروبية⁵.

وبالرغم من أهمية الإتفاقية في مكافحة الجرائم الالكترونية، ما يمكنه ملاحظة وجود تباطؤ من حيث التصديق عليها وإدخالها حيز النفاذ، سواء كان من طرف الدول الأعضاء في مجلس أوروبا⁶ أو الدول

¹ - أنشئت لجنة الخبراء المعنية بالجريمة في الفضاء الالكتروني بموجب القرار رقم 583(97)/déc. 583(97)/cm/del/déc. الصادر في 4 فبراير 1997، وتعرف هذه اللجنة بالاختصار الإنجليزي (PC-cyy) ..

⁽²⁾ _Emmanuelle Matignon, la cybercriminalité-un focus dans le monde des Télécoms ; mémoire de Master en droit numérique Administrations, école de droit , université de Sorbonne , paris 1, 2011-2012, p34.

³ _مجمع البحوث والدراسات اكاديمية السلطان قابوس لعلوم الشرطة، المرجع السابق، ص 60.

⁽⁴⁾ _Caprioli Eric A, Règlement des litiges internationaux et droit applicable dans le commerce électronique, édition du juris-classeur, litec, paris, 2002, p 78.

⁵ _عمر بن يونس، المرجع السابق، ص 216.

⁶ _تعتبر دول أوروبا الشرقية الأسبق من حيث التصديق على اتفاقية بودابست وإدخالها حيز النفاذ خلال الفترة الممتدة من 2002/02/20 إلى 2005/5/1 كإستونيا، هنغاريا، رومانيا، ليتوانيا، سلوفينيا، بلغاريا، مالطا، في حين أن الدول الغربية والمتقدمة تكنولوجيا اختلفت في التصديق على هذه المعاهدة مثلا فرنسا صادقت عليها في 2006/1/10 أما النفاذ كان بتاريخ 2006/5/1، ألمانيا في التصديق بتاريخ 2009/03/9 ونفاذ الاتفاقية كان يوم 2009/7/1 إيطاليا صادقت على الاتفاقية بتاريخ 2008/06/5 ودخلت حيز التنفيذ بتاريخ 2008/10/1.

غير الأعضاء¹، وهذا أكدته مجمع البحوث والدراسات الأكاديمية السلطان قابوس لعلوم الشرطة من خلال الإحصائيات والدراسات التي قام بها، حيث أن 30 % من الأعضاء صادقوا عليها ونفذوها بعد مرور 5 إلى 8 سنوات من فتحها للتوقيع، وأن 30% أخرى من الأعضاء صادقوا عليها وأدخلوها حيز النفاذ بعد مرور 9 إلى 13 سنة من التوقيع على الاتفاقية، مما يؤكد أن التوقيع على هذه الاتفاقية كانت بالنسبة لبعض الدول، عبارة عن تظاهرة دولية للعلاقات العامة وأعقبها تقاعس متعمد في التصديق عليها وإنفاذها، ففي هذه الفترة إستفحلت الجرائم الإلكترونية، وانتشرت في جميع أرجاء العالم وكلفت خسائر فادحة وكبيرة بلغت مليارات الدولارات، مما أدى إلى التحرك الدولي المكثف لتفعيل الاتفاقية بداية من عام 2010 بعدما أن طالت الهجمات البنيات التحتية في القطاع العام والخاص ومعلومات وبيانات الأفراد²، وخلفت آثارا إقتصادية بالغة الخطورة على المستوى العالمي.

و تسعى إتفاقية بودابست للعمل على توحيد الجهود الدولية لمواجهة الجريمة الإلكترونية، وذلك من خلال التنسيق بين القوانين الوطنية وقوانين الدول الأخرى، وتجسيد الأهداف المسطرة في الإتفاقية والتي³ تتمثل فيما يلي:

-السعي لتحقيق وحدة التدابير التشريعية بين الدول الأوروبية والدول المنظمة للاتفاقية من غير الدول الأوروبية.

-التأكيد على أهمية التعاون الإقليمي والدولي في ميدان مكافحة جرائم الكمبيوتر والإنترنت، وإيجاد مرجعية ودليل إرشادي للتدابير التشريعية الوطنية في ميدان مكافحة جرائم الكمبيوتر والإنترنت.

-ضرورة فعالية خطط العمل لمكافحة الأنشطة التي تستهدف سرية وسلامة وتوفير المعلومات،

¹ _ ولا يختلف الأمر كذلك بالنسبة للدول غير الأعضاء لمجلس أوروبا الموقعة على الاتفاقية لم يكن لها نفس الحماس على التصديق والنفاذ، فالولايات المتحدة الأمريكية صادقت على الاتفاقية في 2006/09/29 ودخلت حيز التنفيذ 2006/7/1 اليابان صادقة عليها بتاريخ 2011/07/3 ودخلت حيز النفاذ بتاريخ 2012/11/1 أما كندا صادقت عليها بتاريخ 2012/11/30 ودخلت حيز النفاذ 2013/03/1 فيما يخص جنوب افريقيا لم تصادق عليها حتى الآن.

من المزيد اطلع على كتاب الجريمة الالكترونية، مجمع البحوث والدراسات الأكاديمية السلطان قابوس لعلوم الشرطة المرجع السابق، ص 64.

² _مجمع البحوث والدراسات الأكاديمية السلطان قابوس لعلوم الشرطة، المرجع نفسه، ص 65.

³ _عبد الله عبد الكريم عبد الله، المرجع السابق، ص 127.

وأنظمة الكمبيوتر وشبكات الكمبيوتر وأنشطة إساءة استخدام الكمبيوتر والشبكات، بما في ذلك تحديد الإطار الموضوعي لهذه الأنشطة والإطار الإجرائي المتصل بالتحقيق والتحري، والمقاضاة في ميدان جرائم الكمبيوتر على المستوى الدولي والوطني.

-تحقيق التوازن بين حماية حقوق الإنسان الأساسية وتحديد حقوق الأفراد بالوصول إلى المعلومات وتكون هذه الاتفاقية من 48 مادة موزعة على أربعة فصول وهي:

الفصل الأول: تضمن تعريفا للمصطلحات الأساسية (المادة 1).

الفصل الثاني: وجاء تحت عنوان الخطوات الواجب إتخاذها على الصعيد الوطني وهو مؤلف من ثلاثة أقسام: الأول يضم المواد من 2 إلى 13 التي تعالج النصوص الموضوعية لجرائم الحاسوب، والثاني يضم المواد من 14 إلى 21 وتتعلق بالقواعد الإجرائية، والثالث يشمل المادة 22 ويتعلق باختصاص، أما الفصل الثالث فجاء بعنوان "التعاون الدولي" ويشمل المواد من 23 إلى 35.

الفصل الرابع: ويتضمن الاحكام الختامية من المادة 36 إلى 48.

وبعد هذا التمهيد للاتفاقية الأوروبية، سنلقي الضوء على أبرز الأحكام الموضوعية والأحكام الإجرائية التي جاءت بها الإتفاقية.

أولاً: الأحكام الموضوعية

فيما يتعلق بالأحكام الموضوعية، فقد تضمنت الاتفاقية أربع طوائف رئيسية لجرائم الحاسوب، وطائفة خامسة تتعلق بقواعد المساهمة بالجريمة والعقوبات المفروضة لهذه الطوائف الأربعة وهذه الطوائف هي على النحو التالي:

الطائفة الأولى: الجرائم التي تستهدف عناصر أمن المعلومات.

وهي الجرائم ضد السرية والسلامة ووجود بيانات الحاسوب، وتشمل جريمة الدخول غير المشروع (المادة 2) وجريمة المراقبة أو الإعتراض غير المشروع (المادة 3)، وجريمة التدخل في المعطيات (المادة 4) وجريمة اتلاف أو تعديل نظام الحاسب الالى (المادة 5)، وجريمة إساءة استخدام الأجهزة (المادة 6).

الطائفة الثانية: الجرائم المرتبطة بالحاسوب، وتتمثل في التزوير المعلوماتي (المادة 7)، كما توجب الإتفاقية على الدول إدراج ما يضمن العقاب عليه في تشريعاتها، مع ترك الباب مفتوحاً للدول في حرية تنظيم مسألة القصد الإجرامي.

وفي المادة الثامنة الخاصة بالغش المعلوماتي (الإحتيال المتصل بالحاسب الآلي) أوجبت الإتفاقية على الأعضاء وجوب إدراج الإحتيال، الذي يتم إما بإدخال أو تغيير أو حذف أي معطيات والتدخل في وظائف الحاسب الآلي بقصد تحقيق منفعة إقتصادية للشخص أو للغير¹.

الطائفة الثالثة: وتشمل الجرائم المتصلة بالمواد الإباحية للأطفال²، وذلك من خلال المادة التاسعة، حيث تسعى الإتفاقية إلى تدعيم الإجراءات التي تحمي الأطفال خاصة حمايتهم ضد الاستغلال الجنسي من خلال تحديث قانون العقوبات بطريقة أكثر فعالية، تشمل على استخدام نظم الحاسب الآلي في إطار ارتكاب الجرائم الجنسية ضد الأطفال³.

الطائفة الرابعة: الجرائم المرتبطة بحق المؤلف والحقوق المجاورة

وتتضمن الجرائم المتصلة بالإعتداءات الواقعة على الملكية الفكرية والحقوق المجاورة، حيث أشارت المادة العاشرة فقرة 1 إلى وجوب تبني الدول في تشريعاتها، نصوصاً قانونية رادعة لإعادة إنتاج أو توزيع أي مواد محمية بقوانين حماية الملكية، من خلال الإعتداءات التي يمكن أن تقع عليها بواسطة الحاسب الآلي بالشكل المخالف لإتفاقية برن بشأن المصنفات الأدبية والفنية، وفي الفقرة الثانية حقوق التأليف المحمية في الدول المجاورة كما ورد في إتفاقية الويبو (wipo)⁴، من خلال نص هذه المادة تبين أنها تهتم بتوفير الحماية الجنائية للملكية الفكرية، في شكلين أحدهما مباشر بالنص صراحة على الجرائم المتصلة بانتهاك حق المؤلف والحقوق المتصلة به، وذلك في المادة 10 من الإتفاقية، والثاني في مسألة حقوق

¹ _محمود أحمد عبانية، المرجع السابق، ص، ص 166-167.

² _تصنف الجرائم المتعلقة بدعارة الاطفال من جرائم المحتوى، فهي ليست الصورة الوحيدة للأفعال المجرمة المتصلة بمحتوى مواقع المعلوماتية، بالرغم أن عدد من التشريعات اتجهت إلى تجريم أفعال أخرى كجرائم المقاومة على الشبكة أو إثارة الاحقاد والفتن وغيرها، للمزيد انظر عبد الله عبد الكريم عبد الله، المرجع السابق، ص134.

³ _عبد اللاه أحمد هلال، اتفاقية بودابست معلقاً عليها، دار النهضة العربية، القاهرة، ط1، 2008، ص113.

⁴ _محمود أحمد عبانية، المرجع السابق، ص، ص 167-168.

الملكية الفكرية بشكل غير مباشر وفي نصوص موضوعية.¹

الطائفة الخامسة: وخصصت للمساهمة والمسؤولية والعقوبات، فتناولت المادة 11 من الإتفاقية على وجوب الدول الأعضاء إتخاذ تدابير تشريعية للنص على المسؤولية عن الشروع، والتدخل والتحريض في ارتكاب هذه الجرائم أو ما تختاره الدولة منها، وكذلك النص على المسؤولية الخاصة بالأشخاص المعنوية، عن الأفعال التي يرتكب لمصلحة الشخص المعنوي من قبل الشخص الطبيعي، بشرط أن يكون مرتكب الجريمة ممثلاً قانونياً للمؤسسة، ويملك سلطة إتخاذ القرار إذا تم ارتكاب الجريمة بتكليف منهم.²

بالنسبة للعقاب على هذه الجرائم فقد أشارت إليها المادة 13 الخاصة بالعقوبات، على أن العقوبات التي تفرض على مرتكبي الجرائم، يجب أن تكون عقوبات سالبة للحرية والغرامات المالية بالنسبة للأشخاص المعنوية.

ثانياً: الأحكام الإجرائية

نصت المواد من 14 حتى 21 من الإتفاقية الأوروبية للجرائم الإلكترونية على الأحكام الإجرائية، وقد تضمنت هذه المواد إلزام كل طرف في هذه الإتفاقية، بتهئية تشريعية داخلية لتقرير السلطات والإجراءات اللازمة في مجال التحقيق بالجرائم المنصوص عليها في الاتفاقية.³

كما ألزمت هذه الإتفاقية الدول الأطراف، عند سنها تشريعاتها الداخلية المتعلقة بالجرائم الإلكترونية، أن تراعي الإتفاقيات الدولية لحقوق الإنسان، كالإتفاقية الأوروبية لحماية حقوق الإنسان والحريات الأساسية لسنة 1950، والميثاق الدولي حول الحقوق المدنية والسياسية لسنة 1966 (المادة 15 من الاتفاقية).⁴

وقد تضمنت الإتفاقية مجموعة من القواعد الإجرائية الخاصة بالبحث والتحري من خلال المواد من 16 إلى 21 ويمكن إجمالها فيما يلي:

¹ _نجاة بن مكي، المرجع السابق، ص 127.

² _محمد أحمد عابنة، المرجع السابق، ص 168.

³ _محمد أبو بكر عمر بن يونس، الاتفاقية الأوروبية حول الجريمة الافتراضية (المذكرة التفسيرية)، مؤسسة آدم للنشر والتوزيع، مالطا، ط2، 2008، ص 113.

⁴ _محمد طارق عبد الرؤوف الخن، جريمة الاحتيال عبر الانترنت -الأحكام الموضوعية والأحكام الاجرائية -، منشورات الحلبي الحقوقية ببيروت، ط1، 2012، ص 123.

سرعة التحفظ على بيانات الكمبيوتر المخزنة، إجبار مقدمي الخدمات على التزويد بالمعلومات المطلوبة، تفتيش وحجز بيانات الكمبيوتر وإمكانية اعتراض هذه البيانات.

كما تضمنت قواعد إجرائية متعلقة بالإختصاص القضائي وذلك بموجب المادة 22¹، منها ضوابط سريان الإختصاص القضائي على الجريمة الإلكترونية، مؤكدة على ضرورة إعتداد الدول الأطراف ما يلزم من تدابير تشريعية وتدابير أخرى لإقرار الإختصاص القضائي على الجرائم الواردة في الإتفاقية، فالمادة 22 وضعت مجموعة من المعايير، التي بمقتضاها تتسق الأطراف المتعاقدة حدود صلاحيتها المتعلقة بالجرائم الواردة في الإتفاقية، وذلك عندما ترتكب الجريمة في إقليم الدولة أو على متن إحدى السفن التي ترفع علمها، أو على إحدى الطائرات المسجلة بموجب قوانينها، وكذا على كل جريمة مرتكبة من جانب أحد مواطنيها، إذا كانت الجريمة معاقب عليها بموجب القانون الجنائي بمكان إرتكابها، أو في حالة إرتكاب الجريمة خارج الإختصاص القضائي لآية دولة، كما نصت الإتفاقية على إستبعاد الإختصاص الجنائي الذي ينص عليه أحد الأطراف، وفقا لقانونه الوطني ومطالبة الدول الأطراف في الإتفاقية بالتشاور حول الإختصاص القضائي الأكثر ملائمة لمحاكمة مجرمي المعلوماتية، في حالة تعدد المطالبة من طرف الأطراف بإختصاصه القضائي حول الواقعة.²

أما بالنسبة للتعاون الدولي فقد خصصت الإتفاقية عدة مبادئ تلزم الدول الأعضاء بوجوب التعاون لإتخاذ الإجراءات والتشريعات الكفيلة بتحقيق التعاون وتطبيق التشريعات الدولية، في مجالات التحقيق وسرقة المعلومات وجمع الأدلة الإلكترونية، وفقا لما جاء في نص المادة 20 من الإتفاقية الأوروبية، أما المادة 21 تتعلق بتسليم المتهمين، كما تضمنت عدة مواد قانونية تتعلق بالتعاون المتبادل، وتبادل المعلومات إذا كانت تحت سلطة دولة أخرى ومخزنة ضمن نطاقها، وكذا تسليم المعلومات ووجوب إلزام

¹_Art 22 convention.

Chaque partie adopte les mesures législatives et autres qui se révèlent nécessaire pour établir sa compétence à l'égard de toute infraction pénale établie conformément aux articles 2 à 11 de la présente convention, lorsque l'infraction est commise :

a-sur son Territoire, ou.

b-à bord d'un navire battant pavillon de cette partie, ou.

c-à bord d'un aéronef immatriculé selon les lois de cette partie, ou.

d-par un de ses ressortissants, si l'infraction est punissable pénalement là où elle a été commise ou si l'infraction ne relève de la compétence Territoriale d'aucun état.

² يوسف قجاج، الإطار الإجرائي الدولي في مجال البحث عن الجريمة الالكترونية، موقع العلوم القانونية، Maroc droit،

منشور على الموقع www.maroc.droit.ampprojet.com اطلع عليه يوم 2019/07/25 على الساعة

كل طرف بتعيين نقطة اتصال على مدار الساعة، وفي أيام العطل لإستقبال طلبات التحقيق في الإعتداءات التي تطل معطيات الحاسب الآلي والمعلومات أو لجمع الأدلة الإلكترونية.¹

فمن خلال ما سبق عرضه تعد الإتفاقية الأوروبية المبرمة ببودابست، بمثابة دليل إرشادي للدول بهدف تطوير تشريعاتها الوطنية من أجل مواجهة الجريمة الإلكترونية، والحث على التعاون بين الدول لصد هذا النوع من الإجرام، كما تجدر الإشارة إليه، أن الجزائر لم توقع أو تصادق حتى الآن على هذه الإتفاقية على غرار المشرع المغربي الذي صادق عليها بتاريخ 29 يونيو 2018 ودخلت حيز النفاذ بتاريخ 1 أكتوبر 2018، فندعو المشرع الجزائري الإسراع إلى الإنضمام والتصديق على هذه المعاهدة.

الفقرة الثانية: البروتوكول الإضافي لاتفاقية مجلس أوروبا

تقدمت كل من فرنسا وألمانيا، بإقتراحات تتعلق بتجريم الأفعال ذات الطبيعة العنصرية وكراهية الأجانب التي ترتكب عبر أنظمة الكمبيوتر، ووجدت هذه الإقتراحات معارضة كل من الولايات المتحدة الأمريكية، اليابان، كندا بحجة المساس بمبدأ حرية التعبير.²

وبهدف إكمال مضامين إتفاقية بودابست، ثم إعتقاد بروتوكول إضافي من طرف مجلس أوروبا بمدينة ستراسبوغ (Strasbourg) الفرنسية بتاريخ 07 نوفمبر 2004، وتم فتح التوقيعات الخاصة بالبروتوكول في 28 جانفي 2003 للتوقيع عليه من طرف الدول الأعضاء في الإتفاقية، وذلك بمناسبة الدورة الأولى للجمعية البرلمانية لمجلس أوروبا لسنة 2003.⁽³⁾

وتضمن هذا البروتوكول تجريم التمييز العنصري وكراهية الأجانب، والتي أصبحت منتشرة في مختلف دول العالم والتي تؤدي إلى أخطار كبيرة.

ويتضمن هذا البروتوكول على 17 مادة، وقد ورد ضمن أحكام الفصل الثالث من البروتوكول المعنون "بالعلاقة بين الإتفاقية وهذا البروتوكول" في المادة الثامنة إلى أن القواعد الاجرائية المضمنة

¹ _ محمد أحمد عابنة، المرجع السابق، ص، ص 168-169.

² _Emmanuelle Matignon Rapport, op, cit, p35.

³ _M.Robert Del picchia, rapport projet de loi autorisant l'approbation de convention sur la cybercriminalité et du protocole additionnel à cette convention relatif à l' incrimination d'actes de nature raciste et xénophobe commis par le brais de système informatique sénat, session ordinaire de 2004-2005, Annexe au procès de la séance du 4 mai 2005, sp, publier sur le sité.www.senat.fr, vu le 30/07/2019 à 13h 30.

بإتفاقية بودابست تطبق على الجرائم المشار عليها في هذا البرتوكول، وذلك فيما يخص أحكام الإختصاص المشار إليها في المادة 22 من إتفاقية بودابست مع ما قد يلزم من تعديل.¹ "Mutatis mutandis"²، وكذا أحكام المواد من 14-21 المتعلقة بنطاق تطبيق القواعد الإجرائية والشروط والضمانات المرتبطة بها والقواعد الاجرائية، المتعلقة بسرعة التحفظ على بيانات الكمبيوتر المخزنة وإصدار الأوامر وتفتيش وحجز بيانات الكمبيوتر والتجميع الفوري لها.³

وإلى جانب هذه الجهود، هناك العديد من المؤتمرات التي عقدت في عام 2000 ومن بينها مؤتمر الجرائم المعلوماتية الذي عقد بالنرويج بمدينة أوسلو⁴، في الفترة الممتدة من 29-31 ماي بمشاركة العديد من الدول النامية والهيئات والمنظمات الدولية، ومن أهم المواضيع التي تناولها هذا المؤتمر، تتمثل في بحث أنواع الجرائم الإلكترونية والتحديات القانونية التي تعيق مواجهة هذه الجرائم، كما أكد المؤتمر على الجهود الدولية وخاصة جهود المجلس الأوروبي التي تمثلت في مسودة الإتفاقية الأوروبية.⁵

وكذلك من القرارات الهامة الصادرة عن المجلس الأوروبي القرار رقم Jal/222/2005 حول الإعتداءات التي تشن على نظم المعلومات، إذ بمقتضاه ألزم المجلس الدول الأعضاء بتوحيد نصوصها الجنائية التي تجرم وتعاقب على أفعال الاعتداء التي تمس الأنظمة المعلوماتية كأفعال القرصنة، كشف كلمات المرور، كما أكد على ضرورة التعاون الدولي في مجال هذه الجرائم على المستوى الأوروبي، ووضع أرضية أوروبية للتكوين والتدريب الجيد لرجال العدالة الجنائية وإنفاذ القانون في هذا المجال.⁶

كما وضع المجلس الأوروبي في الفترة ما بين 2010 و2014 مخططا شاملا مشتركا، فحدد إستراتيجية تشريعية وأمنية، التي يجب على الدول الأعضاء إتباعها سواء على المستوى الوطني أو على

¹ يوسف قجاج، المرجع السابق، ص د ت.

² les articles 1,2,13,22,41,45,46 de la convention s'appliquent mutatis mutandis à ce protocole.

³ يوسف قجاج، المرجع السابق، ص د. ت.

⁴ وكان انعقاد هذا المؤتمر بسبب الهجمات التي تعرضت لها مواقع عديدة في فيفري 2000 مثل موقع Yahoo و Cnn، كما ظهر في تلك الفترة فيروس الحب الذي الحق أضرارا بالغة بأجهزة الحواسيب في كافة انحاء العالم.

⁵ نجاة بن مكي، المرجع السابق، ص 129.

⁶ جمال إبراهيمي، المرجع السابق، ص 286، / كذا قرار المجلس رقم Jal/222/2005، مؤرخ في 24 فبراير 2005، يتعلق بالهجمات التي تشن على نظم المعلومات، الجريدة الرسمية لاتحاد الأوروبي 16 مارس 2005.

المستوى الأوروبي لمواجهة الجرائم الإلكترونية¹، ومنها القرار رقم E 2011/92/4 الصادر بتاريخ 13 ديسمبر 2011 يتعلق بالاستغلال الجنسي للأطفال عبر الأنترنت والذي يعدل القرار 2004/68/Jai لمجلس ويهدف هذا القرار للمواجهة الدولية لاستغلال الجنسي للأطفال عبر الأنترنت، ويسط حماية خاصة للأطفال مع سن نصوص التجريم والوقاية لهذا النوع من الأفعال غير المشروعة، فشدد هذا القرار من العقوبة، كما دعا الدول الأعضاء إلى التمسك بالمسؤولية الجنائية للأشخاص المعنوية في مجال هذه الجرائم، مع وضع إجراءات خاصة لوقاية الأطفال ضحايا هذا النوع من الإجرام²، ولقد ساهم هذا المخطط بشكل كبير في توحيد السياسة الجنائية التشريعية بين دول الاتحاد الأوروبي في مواجهة تحديات الجرائم الإلكترونية، وخلق مناخ للتعاون المشترك فيما بينها في هذا الشأن.³

الفقرة الثالثة: جهود مجموعة الدول الثمانية (G 8)

أنشأت مجموعة الدول الثمانية G8 فريقاً فرعياً للجرائم الإلكترونية الفائقة التقنية عام 1997، وفي إجتماع لها عقد في واشنطن سنة 1997 إعتمدت هذه المجموعة، عشرة مبادئ لمكافحة الجرائم الإلكترونية ومن بينها عدم إتاحة ملاذات آمنة للمعتدين على تكنولوجيا المعلومات، و التنسيق بين جميع الدول المعنية في ملاحقة مرتكبي جرائم الانترنت ومحاكمتهم بغض النظر عن مكان حدوث الضرر، مع تدريب الموظفين المكلفين بتنفيذ القوانين وتجهيزهم بالمعدات الضرورية للتعامل مع الجرائم ذات التقنية العالمية.⁴

وقد صدر بيان مشترك عن مجموعة الدول الثمانية G8، الذي ضم وزراء العدل والداخلية في واشنطن بتاريخ 10/11/2004، حيث حث هذا البيان على مواصلة تعزيز القوانين المحلية لبناء القدرات العالمية لمكافحة الاستخدامات الارهابية والاجرامية للأنترنت، وأوجب على جميع الدول أن تواصل تحسين القوانين التي تجرم إساءة استخدام الشبكات الحاسوبية والتي تسمح بسرعة التعاون في التحقيقات المتصلة بالأنترنت، ومع دخول إتفاقية مجلس أوروبا للجريمة الإلكترونية حيز النفاذ في 1 أوت 2004 يجب على الدول الأعضاء اتخاذ خطوات لتشجيع اعتماد المعايير القانونية التي تتضمنها على قاعدة واسعة.⁵

¹-Myriam quémener , Yves charpenl, op. cit, p231.

²_Emmanuelle Matignon, op, cit, p38.

³ _ جمال إبراهيمي، المرجع السابق، ص 286.

⁴ _جورج لبكي، المرجع السابق، ص 08.

⁵ _مركز معلومات G8 متاح على الموقع الإلكتروني: <http://www.cybercrime law.net/g8.html> أطلع عليه يوم 2018/03/15 على الساعة 17h : 45.

وترى دول G8 أن الحماية الفعالة ضد الجرائم الإلكترونية، تتطلب الإتصال والتنسيق والتعاون داخليا ودوليا، وبناء على ذلك إلترمت الدول الثمانية بتدريب جميع العاملين في مجال تطبيق القانون، وتجهيزهم بالمعدات الضرورية لمكافحة الجرائم الإلكترونية، وكذا مساعدة جميع البلدان الأعضاء على إقامة مراكز اتصال تعمل على مدار 24 لساعة سبعة أيام في الأسبوع.¹

وبالإضافة إلى ما سبق، أصدرت مجموعة الدول الثمانية عدة توصيات بخصوص الجرائم الإلكترونية لحث الدول الأعضاء على ما يلي:

-السهر على توحيد تشريعاتها العقابية والإجرائية الوطنية، فيما يتعلق بجرائم التكنولوجيا الحديثة والجرائم ذات الصلة بالحاسب الآلي.

-تكتيف سبيل التعاون الدولي لمكافحة الجرائم الإلكترونية، والتنسيق بين الدول لتجاوز العقبات ومعالجة المشاكل المتعلقة بالتحقيقات القضائية في هذه الجرائم.

- إتخاذ تدابير وقائية وأخرى ردعية لمنع الجريمة الإلكترونية.

-العمل الدؤوب على إقتناء التكنولوجيا الملائمة والتطوير المستمر للخبرات والقدرات الفنية في مجال التحقيق والإدعاء العام، وتشجيع البحث العلمي والتطبيقي في هذا المجال، من أجل زيادة فعالية تقنيات تطبيق القانون.

-تشجيع التعاون في مجال تطوير الاستراتيجيات المناسبة لرفع الوعي العام في هذا الشأن مع التقييم المستمر لبرامج مكافحة والوسائل القانونية المتبعة.²

الفرع الثاني: جهود الدول العربية في مكافحة الجريمة الإلكترونية

بالرغم أن الجريمة الإلكترونية لم تستفحل في الدول العربية كما عليه في دول العالم الأخرى، إلا أن هذا لا يمنع من إتخاذ الإجراءات اللازمة للحد من إنتشارها، حيث سعت الدول العربية من خلال بعض القوانين أو المؤتمرات إلى الحث على مكافحتها، وهذا ما يتم التعرف عليه من خلال إبراز جهود الدول العربية لمكافحة الجريمة الإلكترونية وذلك كما يلي:

¹ _جورج لبكي، المرجع السابق، ص 8.

² _جمال إبراهيمي، المرجع السابق، ص 293.

أولا-قانون الإمارات العربي الإسترشادي لمكافحة جرائم تقنية المعلومات

يعد القانون العربي النموذجي لمكافحة الجريمة الإلكترونية خطوة فعالة في مجال مكافحة الجريمة الإلكترونية، ومسلكا منطقيا وضروريا لا بد من اتخاذه، لأن المجتمعات العربية ليست بمنأى عن هذه الجرائم الجديدة والمستحدثة¹، اعتمدت جامعة الدول العربية عبر الأمانة الفنية لمجلس وزراء العرب، ما يسمى بقانون الإمارات العربي الإسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها، نسبة إلى مقدم هذا المقترح وهو دولة الإمارات العربية المتحدة، حيث تم إعماله في الدورة التاسعة عشرة بالقرار رقم 495-ج-19 (2003/10/8-19)²، بحيث يمثل هذا القانون القواعد الأساسية الإرشادية التي يمكن أن يستعين بها المشرع في الدول العربية، عندما يريد أن يسن نصوصا وطنية بخصوص الجرائم الإلكترونية، سواء باستحداث قوانين خاصة بذلك أو تحيين قوانينه القائمة.³

وقد تضمن هذا القانون 27 مادة موزعة على أربعة أبواب، تناول الباب الأول الجرائم الإلكترونية والعقوبات المقررة لها، وتم النص عليها في المواد من 2 إلى 22 ويمكن تلخيصها في:

-جريمة الولوج غير المشروع الى موقع أو نظام معلوماتي، والتلاعب في بياناته

-جريمة تزوير المستندات المعالجة في نظام معلوماتي واستعمالها.

-جريمة الإدخال المؤدي إلى إيقاف أو تعطيل نشاط الشبكة المعلوماتية، أو إتلاف البرامج فيها.

-جريمة التصنت وإعتراض المراسلات عبر الشبكة المعلوماتية.

-الجرائم المخلة بالآداب العامة والنظام العام وأمن الدولة عبر الشبكة المعلوماتية.⁴

أما الباب الثاني تطرق إلى التجارة والمعاملات الإلكترونية، فيما تناول الباب الثالث تدابير حماية حقوق الملكية الفكرية عبر الوسائل الإلكترونية، في حين تناول الباب الرابع الجوانب الجرائية المتعلقة

¹ _يدري فيصل، المرجع السابق، ص 33.

² _متاح على الموقع الإلكتروني: [http://arabic.justice.dz/ligue arabe / loi .emir ar crimtech inf. .PDF](http://arabic.justice.dz/ligue%20arabe%20loi%20emir%20ar%20crimtech%20inf.%20PDF).

³ _جمال إبراهيمي، المرجع السابق، ص 292.

⁴ _عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والأنترنت في القانون العربي النموذجي، دار المكر الجامعي، الإسكندرية، د ط، 2006، ص 10.

بالجريمة الالكترونية.¹

وما تجدر الإشارة إليه أن القانون العربي الإسترشادي لمكافحة جرائم تقنية المعلومات، كان موفقا إلى حد ما في أحكامه الموضوعية، حيث شملت معظم الجرائم التي يمكن أن ترتكب عن طريق الحاسب الآلي أو عبر الأنترنت، لكن يؤخذ على هذا القانون عدم تعرضه للأحكام الإجرائية الضرورية لملاحقة هذه الجرائم، كإجراءات التفتيش والضبط، ما جعل هذا القانون لم يلق إهتمام معظم الدول العربية بسبب تركيزه على الجوانب الموضوعية للجريمة الإلكترونية.

ولتدارك الفراغ الذي تخلله الجانب الإجرائي للقانون العربي الإسترشادي اجتهدت الدول العربية لإيجاد إطار قانوني أكثر ملاءمة للتصدي ومواجهة الجرائم الإلكترونية، توج بإبرام إتفاقية عربية تعمل على توحيد الجهود العربية في هذا المجال.

ثانيا: الإتفاقية العربية لمكافحة جرائم تقنية المعلومات

بادرت الدول العربية إلى وضع اتفاقية عربية لمكافحة الجرائم الإلكترونية، وذلك في إطار مواكبة الجهود المبذولة على المستوى الدولي، بهدف تعزيز التعاون بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات، وتم إبرام هذه الإتفاقية بعد الموافقة عليها من طرف مجلس وزراء الداخلية والعدل العرب في إجتماعهما المشترك المنعقد بمقر الأمانة العامة لجامعة الدول العربية بالقاهرة بتاريخ 2010/12/21، وتسري هذه الإتفاقية بعد مضي ثلاثين يوما من تاريخ إيداع وثائق التصديق عليها أو قبولها أو إقرارها من سبع دول عربية بموجب الفقرة 3 من الأحكام الختامية للاتفاقية².

وجاء مضمون الإتفاقية العربية مطابقا لأحكام إتفاقية بودابست، خاصة على مستوى القواعد الإجرائية، سواء من حيث نطاق التطبيق أو طبيعة هذه القواعد³، وكانت الجزائر من الدول الأعضاء الموقعة على هذه الإتفاقية والتي صادقت عليها بالمرسوم الرئاسي رقم 252/14.⁴

¹ _جمال إبراهيمي، المرجع السابق، ص 293.

² _ عبد المالك صاولي، تشريعات الجريمة الإلكترونية في البيئة الإعلامية العالمية، مجلة الحقوق والعلوم السياسية، العدد 10، 2018، ص 467.

³ _هشام ملاطي، خصوصية القواعد الإجرائية للجرائم المعلوماتية، محاولة المقاربة مدى ملائمة القانون الوطني مع المعايير الدولية، سلسلة ندوات محكمة الاستئناف بالرباط، العدد السابع، 2014، ص 83.

⁴ _مرسوم رقم 252/14 مؤرخ في 8 سبتمبر 2014، يتضمن التصديق على الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، الجريدة الرسمية للجمهورية الجزائرية، عدد 57، الصادرة بتاريخ 2014.

واحتوت هذه الإتفاقية على خمسة فصول، خصص الفصل الأول لتعريف بعض المصطلحات وتحديد نطاق تطبيق أحكام هذه الإتفاقية، وموقفها إتجاه سيادة الدول الأطراف في الاتفاقية¹، فيما خصص الفصل الثاني الذي جاء تحت عنوان "التجريم"، لحصر والنص على مجموعة من الجرائم الإلكترونية، المساهمة الجنائية والتشديد على توقيع العقوبة، من خلال المواد من 05 إلى 21، أما الفصل الثالث فقد تضمن أهم إجراءات التحقيق والإثبات الجنائي كإجراءات التفتيش عن بعد، وكذا إجراءات الضبط، وإجراءات إعتراض ومراقبة المراسلات الإلكترونية، التسجيل الفوري لبيانات المحتوى وبيانات المرور المتعلقة بالاتصالات عبر وسائل تقنية المعلومات.²

بينما تناول الفصل الرابع أحكام التعاون القانوني والقضائي بين الدول الأطراف، وقد تضمن عدة صورة منها الاختصاص القضائي، المساعدة الفنية المتبادلة لأغراض التحقيق وجمع الأدلة في الجرائم الإلكترونية، فيما إشمئل الفصل الخامس والأخير الأحكام الختامية، وأصبحت الاتفاقية سارية المفعول بعد تصديق الرئيس المصري عليها سنة 2015 ليكتمل نصاب الدول السبع المطلوبة لسريانها.³

ثالثاً: المكتب الاقليمي العربي لاتحاد للاتصالات⁴

عقد محضر الإجتماع الأول في الجزائر يومي 25 و 26 فيفري 2013 تم تشكيل فريق العمل حول حماية الأطفال على الانترنت في المنطقة العربية ويهدف إلى تنسيق الجهود وتوحيد الرؤية في المنطقة العربية من أجل التوصل إلى وضع مبادئ توجيهية لإطار قانوني لحماية الطفل على الانترنت في المنطقة العربية وتم الاتفاق على أن تكون مهمة الفريق كالتالي:

- تحديد الأفعال التي تشكل خطراً على الأطفال في الفضاء السيبراني.

- وضع المبادئ التوجيهية للإطار القانوني الإقليمي، لحماية الأطفال في الفضاء السيبراني في إطار

¹ _ المواد من 01 إلى 14 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

² _ المواد من 22 إلى 29 من الاتفاقية العربية.

³ _ أحمد بن خليفة، حفظة الأمير عبد القادر، الجريمة الإلكترونية وآليات التصدي لها، مجلة الامتياز لبحوث الاقتصاد والإدارة، المجلد 01، العدد 01، 2017، ص 162.

⁴ _ فاروق خلف، الآليات القانونية لمكافحة الجريمة المعلوماتية، ورقة علمية مقدمة في إطار الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، مخبر الحقوق والحريات في الانظمة المقارنة، جامعة بسكرة، المنعقد بين 16-17/11/2015، ص 8.

التعاون والتنسيق الاقليمي في المنطقة العربية.

-تقديم توصيات عامة حول الإسترشاد بالمبادئ التوجيهية، على المستوى الوطني لكل دولة عند صياغة قوانينها الخاصة.

الفرع الثالث: جهود الاتحاد الافريقي في مكافحة الجريمة الإلكترونية

طلب المؤتمر الإستثنائي لوزارة الاتحاد الإفريقي المسؤولين عن تكنولوجيا المعلومات والاتصالات، المنعقد في جنوب افريقيا من 02 إلى 05 نوفمبر من مفوضية الاتحاد الإفريقي القيام بالاشتراك مع لجنة الأمم المتحدة الاقتصادية لإفريقيا بإعداد إتفاقية حول مواجهة الجريمة الالكترونية¹، وبالفعل تم إعتقاد إتفاقية الاتحاد الإفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي سنة 2014، وفي جانفي 2020 وقعت من طرف 14 دولة إفريقية من أصل 55 دولة عضوا في الاتحاد الإفريقي.²

وقد نص الفصل الثالث الذي جاء تحت عنوان " تعزيز الأمن الالكتروني ومكافحة الجريمة الإلكترونية"، وحيث حثت الدول الأعضاء في الاتحاد الإفريقي إلى تأمين الفضاء الإلكتروني وذلك بإتخاذ تدابير تشريعية لمكافحة هذه الجريمة، ونشر ثقافة الأمن الإلكتروني بالإضافة إلى تفعيل هياكل لرصد تأمين الفضاء الإلكتروني، وكذلك تبني تعاون الدول في مجال مكافحة هذا النوع من الجرائم، كما نصت على بعض الجرائم ذات الصلة بتكنولوجيا المعلومات والاتصال.³

المطلب الثالث: تأثير الجزائر بالجهود الدولية في مجال الجريمة الالكترونية

إن الجهود المبذولة سواء من هيئة الأمم المتحدة، أو المجلس الاوروبي لعب دورا كبيرا في إقرار تشريعات قانونية تتعلق بالإجرام المعلوماتي، فيمكن إعتبارها الملهم الحقيقي للمشرع الجزائري في هذا

¹ -فاروق خلف، المرجع السابق، ص 08.

² -تقرير الإنتربول بتاريخ 2020/08/14 يحذر من أن الجريمة الالكترونية في إفريقيا تشكل تهديدا أشد خطر من أي وقت مضى، منشور على الموقع الإلكتروني www.interpol.int/Ar/1/1/2020/36; أطلع عليم يوم 2020/12/15 على الساعة 14h00.

³ -إتفاقية الاتحاد الإفريقي بشأن أمن الفضاء الالكتروني وحماية البيانات ذات الطابع الشخصي.

المجال خاصة إتفاقية بودابست، ولضرورة مواكبة المشرع للتطورات الدولية والإقليمية في هذا الميدان، وكذا بإعتبار الإتفاقيات الدولية الموقعة من الجزائر تسمو على القوانين الداخلية، مما تدعو المشرع إلى تعديل القوانين الداخلية بما يتماشى مع هذه الإتفاقيات أو سن قوانين جديدة لمواكبة هذه التشريعات¹، قبل الخوض في ذكر التعديلات المتعلقة بالمنظومة التشريعية الجزائرية، لابد أولا من تناول بعض النماذج من التشريعات المقارنة الرائدة والسباقة في مواجهة الجريمة الإلكترونية كالتشريع الفرنسي، وتشريع الولايات المتحدة الأمريكية.

الفرع الأول: جهود الدول الغربية

خطت بعض الدول خطوات واسعة في مجال إعداد تشريعات خاصة بالجرائم الإلكترونية، بعد فشل القوانين التقليدية وعدم ملائمتها للإعتداءات الحاصلة في نظم المعلومات، سوف نتناول فيما يلي جهود التشريع الفرنسي (أولا) والتشريع في الولايات المتحدة الأمريكية (ثانيا).

أولا: التشريع الفرنسي

بداية من عام 1980 لا توجد تشريعات خاصة في مجال مكافحة الجريمة الإلكترونية في التشريع الفرنسي، وكانت أولى محاولات لمد سلطان قانون العقوبات حماية المال المعلوماتي بفرنسا من طرف وزيرها للعدل عام 1985، عندما تقدم بمشروع قانون عقوبات جديد، أضاف بموجبه بابا رابعا للكتاب الثالث منه بعنوان "الجرائم في المادة المعلوماتية" *les infractions en matière informatique* يتكون من ثماني² مواد من 1/307 إلى 8/307 تناولت بالتجريم الموضوعات التالية:

-إلتقاط البرامج أو المعطيات أو أي عنصر آخر من النظام المعلوماتي عمدا.

-إستخدام أو نقل أو إنتاج برنامج أو معطيات أو أي عنصر من عناصر النظام المعلوماتي دون موافقة من لهم حق فيه.

-تخزين أو عرقلة أداء كل أو جزء من نظام المعالجة الآلية للمعطيات.

¹ _محمد السعيد زنائي، الجريمة الإلكترونية في ظل التشريع الجزائري والإتفاقيات الدولية، مجلة اليزي للبحوث والدراسات، العدد 2، 2017، ص 38.

2 - محمد خليفة، جريمة التواجد غير المشروع في الأنظمة المعلوماتية، المرجع السابق، ص 48.

لكن هذا المشروع لم يطبق على أرض الواقع ولم يلق نجاحا، إلى أن تقدم النائب jacques Godfrain بتاريخ 1986/08/05 ونواب آخرون إلى الجمعية الوطنية باقتراح مشروع قانون عن الغش المعلوماتي " fraude informatique " حاول من خلاله تطويع بعض النصوص القائمة في قانون العقوبات، والتي تتناول جرائم تقليدية كالسرقة وخيانة الأمانة، والتزوير والإتلاف والإخفاء وذلك ليشمل العدوان المال المعلوماتي¹، وبعد المناقشات في البرلمان أسفرت عن قانون، يختلف عن المشروع الذي قدم لأول مرة بل تشابه مع المشروع الأول، الذي قدمه الوزير الأول للعدل سنة 1985، فصدر بذلك القانون رقم 19/88² بتاريخ 05 جانفي 1988 المتعلق بحماية نظم المعالجة الآلية للمعطيات، وتم إدراجه في قانون العقوبات الفرنسي، ليشكل الباب الثالث من الكتاب الثالث من القسم الثاني منه، وذلك في المواد من 2/462 إلى 9/462 وتتمثل في الجرائم التالية:³

-الدخول أو البقاء غير المشروع في نظام معالجة آلية للمعطيات أو جزء منه وتثديد العقوبة في حالة محو أو تعديل المعطيات الموجودة داخل هذا النظام أو إفساد وظيفته.

-إدخال معطيات في النظام أو محو أو تعديل المعطيات الموجودة فيه عمدا وبدون مراعاة حقوق الغير، سواء تم ذلك بطريقة مباشرة أو غير مباشرة.

-كل فعل من شأنه أن يعرقل أو يفسد عمدا وبدون مراعاة حقوق الغير اداء النظام لوظيفته.

-تزوير المستندات المعالجة آليات أيا كان شكلها، وإستعمال هذه المستندات.

-الشروع في إرتكاب الجرائم السابقة.

- الإتفاق الجنائي على إرتكاب الجرائم السابقة.

وفي سنة 1994 تم تعديل قانون العقوبات الفرنسي، حيث استغنى المشرع الفرنسي عن عبارة "دون مراعاة حقوق الغير واستعمل عبارة "الغش"، كما قام أيضا بتعديل المادة 1/441 من ق.ع.ف المتعلقة بتزوير المعلوماتي، لتصبح جريمة تزوير المستندات المعلوماتية وإستعمالها، بعد ما كانت جريمة تزوير

¹ _محمد خليفة، جريمة التواجد غير المشروع في الأنظمة المعلوماتية، المرجع نفسه، ص 49.

² _loi 88/19, 5 janv. 1988, relative a fraude informatique, J06 janv., p 231, dite loi Godfrain

³ _أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، الحماية الجنائية للحاسب الآلي، دراسة مقارنة، دار النهضة العربية، القاهرة، دط، 2000م، ص 262.

المستندات المعالجة آليا فحسب، بذلك أخرجت هذه الجريمة من نطاق جرائم الإعتداء على النظم المعلوماتية بسبب إختلاف المصلحة المحمية.

وبحلول عام 2004 أضاف المشرع الفرنسي، جريمة أخرى وهي جريمة التعامل في الوسائل التي تصلح أن ترتكب بها جريمة الدخول أو البقاء غير المصرح بها أو جريمة التلاعب بالمعطيات، أو جريمة إعاقة وإفساد أنظمة المعالجة الآلية للمعطيات ويعرف بقانون المتعلق بالثقة في الإقتصاد الرقمي.¹

فالتشريع الفرنسي كان له الأثر الكبير في إرساء قواعد قانونية ساعدت على مكافحة الجريمة الإلكترونية خاصة على التشريع الجزائري.

ثانيا: تشريع الولايات المتحدة الأمريكية

قبل صدور التشريعات الفيدرالية المتعلقة بالجرائم الإلكترونية²، كان القضاء الأمريكي يستعين بنصوص قانون العقوبات التقليدية وتطبيقها على بعض أفعال السرقة والإتلاف وخطوط الهاتف³، بعد إنتشار هذه الجرائم وفداحة الخسائر الناتجة عنها، تعالت الأصوات لضرورة إقرار تشريعات خاصة لمواجهة هذه الجرائم، فيعد قانون فلوريدا الصادر عام 1978 أول قانون في الولايات المتحدة الأمريكية يخص الجريمة الإلكترونية، فينص هذا القانون على كل دخول إلى الحاسب الآلي غير مصرح به هو بمثابة جريمة، حتى ولو لم تكن نية عدائية للدخول⁴، أما على الصعيد الفيدرالي فقد صدر سنة 1984 قانون الإحتيال وسوء إستخدام الكمبيوتر " computer fraud and Abuse act " وتم تعديله عام 2001، وذلك بموجب القانون الوطني المؤرخ في 2001/10/26، وتم إدراجه في القسم 1030 من هذا القانون كل من يقوم بالدخول عمدا إلى حاسوب مشمول بالحماية دون أن يكون مصرحا له بذلك أو يتجاوز

(1) _Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, plus connue sous le nom de LCEN, voir Myriam quémener, Yves charpente, op cit, p30.

² _بدأ إهتمام الولايات المتحدة الأمريكية بمكافحة الجريمة الإلكترونية سنة 1966 في أول قضية Hancock ustate تعرض لموضوع إساءة إستخدام الحاسبات الآلية وتتلخص وقائع هذه القضية في اتفاق مبرمج لحاسبات آلية بإحدى الشركات، بالاتفاق مع صديق له يعمل بشركة أخرى على أن يقوم الأول بطبع المعلومات التي يحتوي عليها 59 برنامجا ملكا للشركة التي يعمل بها والتي هي ذات أهمية كبيرة وتسليمها للشركة الأخرى، مقابل تلقيه 5 ملايين دولار وأثناء التسليم، ثم القبض عليه وقدم للمحاكمة بتهمة السرقة. أنظر: نائلة عادل محمد فريد قوره، المرجع السابق، ص 147.

³ _سامية عبد الرزاق خلف، جريمة اختراق أنظمة المعلومات-دراسة مقارنة-، مجلة كلية القانون، جامعة البصرة، د.ع، ص 11.

⁴ _محمد طارق عبد الرؤوف الخن، المرجع السابق، ص 104.

التصريح الممنوح له إذا كان الغرض من هذا الدخول هو الحصول على شيء ذي قيمة عن طريق الاحتيال¹.

وما يمكن الإشارة إليه أن التشريع الفيدرالي الأمريكي قبل عام 1986 لم يجرم إتلاف المعلومات والبرامج، وإنما إقتصر التجريم على إعاقة أنظمة الحاسبات الآلية، فقد جرمت المادة 1030 الفقرة الثالثة من القانون الفيدرالي لجرائم الحاسب الآلي الصادر سنة 1984 إتلاف المعلومات التي يترتب عليه إعاقة الحكومة عن استعمال أنظمة الحاسبات الآلية، وقد وجهت عدة إنتقادات لهذا القانون، لكن تم تعديله في عام 1986 وأصبحت الفقرة الثالثة من المادة 1030 تتناول فقط الدخول غير المصرح به إلى الحاسب الآلي تستعمله الحكومة متى أعاق الدخول هذا الاستعمال، إلى جانب ذلك أضيفت فقرة خامسة للمادة 1030، تتناول جريمة الإتلاف العمدي وغير المصرح به لمعلومات يحتوي عليها حاسب آلي تابع للحكومة وإدارتها أو حاسب آلي غير تابع للحكومة، إلا أنه يتم إستخدامه من طرفها أو لصالحها، أو إعاقة هذا الحاسب عن أداء المهام المختلفة التي تباشرها الحكومة بواسطته، وفي عام 1996 تم إصدار قانون حماية بنية المعلومات القومية أين تم تعديل المادة السابقة، وقد شمل هذا التعديل التوسع في نطاق حماية أنظمة الحاسبات الآلية، فوفقا للفقرة الثانية من المادة 1030 لم تعد الحماية مقصورة على الحاسبات الآلية التابعة للحكومة وإدارتها أو التي يتم استخدامها من قبلها، وإنما إتسعت لتشمل الحماية لجميع الحاسبات التي يتم إستخدامها من قبل المؤسسات الإقتصادية والتي تستخدم في التجارة والاتصالات وهو ما أطلق عليه بالحسابات التي تتمتع بالحماية².

الفرع الثاني: التشريع الجزائري

واكب المشرع الجزائري التشريعات المقارنة في مجال مكافحة الجريمة الإلكترونية، وكانت مواجهته للجرائم الإلكترونية إحدى بنود إتفاق مؤسس لشراكة بين الجزائر والإتحاد الأوروبي عقد بتاريخ 22 أبريل 2002 وضمنت المادة 86 منه³، ونظرا لخطورة هذه الجرائم سواء على الأفراد أو على مؤسسات الدولة،

¹ _نعيم سعيدي، المرجع السابق، ص 82.

² _نعيم سعيدي، المرجع نفسه، ص، ص 82 - 83.

³ _ نصت المادة 86 من هذا الاتفاق على مايلي: prévention et lutte contre la criminalité organisée:

1-les parties conviennent de coopérer afin de prévenir et de combattre la criminalité organisée notamment dans les domaines du trafic de personne, de l'exploitation à des fins sexuelles du trafic illicite de produits prohibés ,contrefaits ou pirates et de transactions illégales concernant

أدت بالمشروع الجزائري إلى التفكير إلى ضرورة التصدي لها وقمعها، ولتدارك الفراغ التشريعي الذي عرفه مجال الإجرام المعلوماتي، أسرع إلى تعديل وإعادة النظر في العديد من التشريعات الوطنية وعلى رأسها قانون العقوبات كقانون عام، إضافة إلى إستحداث قوانين أخرى خاصة لم تكن معروفة من قبل، وكذا إبرامه لإتفاقيات عربية ودولية وسوف نتناول هذه القوانين دون تفصيلها وذلك كما يلي:

أولاً: تعديل قانون العقوبات

أصدر المشرع الجزائري سلسلة من النصوص القانونية، وكان أول نص تشريعي تمثل في القانون رقم 09/01 المؤرخ في 26 جوان 2001¹، المعدل والمتمم لقانون العقوبات في القسم الأول تحت عنوان "الإهانة والتعدي على الموظفين ومؤسسات الدولة" وذلك بموجب المواد 144 مكرر-144 مكرر 2 وكذا المادة 146 من ق.ع.ج وتعلق بجريمة القذف والسب والإهانة ضد رئيس الدولة ومؤسسات الدولة، وفيما يخص دين الإسلام (الرسول وباقي الانبياء وما هو معلوم من الدين) فأدرج لأول مرة مصطلح... وسيلة إلكترونية أو معلوماتية... والتي تفيد بتجريم الأفعال السابقة في محيط المعلوماتية والانترنت. ثم جاء تعديل آخر لقانون العقوبات تمثل بالقانون رقم 15/04 المؤرخ في 10/11/2004 والذي نص على حماية جزائية لأنظمة المعالجة آليا للمعطيات، من خلال تجريم كل أنواع الإعتداءات التي تستهدف هذه الأنظمة فخص القسم السابع مكرر تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات" والتي تحتوي على ثمانية مواد من المادة 394 مكرر إلى المادة 394 مكرر 7.

ففي سنة 2006 أدخل المشرع الجزائري تعديلا آخر على قانون العقوبات، بموجب القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006، فمس التعديل مرة أخرى القسم السابع مكرر والمتعلق بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، من خلاله تم تشديد العقوبة المقررة لهذه الأفعال دون المساس

notamment les déchets industriels ou du matériel radio actif ,de la corruption du trafic de voitures volées ,du trafic d'armes à feu et des explosifs ,de la criminalité informatique, et du trafic de bien culturels.

Les parties coopérèrent étroitement afin de mettre en place les dispositifs et les normes appropriés.

2- la coopération technique et administrative dans ce domaine pourra inclure la formation, et le renforcement de l'efficacité des autorités et de structures chargées de combattre et de prévenir la criminalité et la formation de mesures de prévention du crime.

¹ _ القانون رقم 09/01 المؤرخ في 26/06/2001 يعدل ويتم الأمر رقم 156/66 المؤرخ في 08/06/1966 والمتضمن قانون العقوبات، الجريمة الرسمية للجمهورية الجزائرية، عدد 34، الصادرة بتاريخ 27/06/2001.

النصوص الموجودة في هذا القسم، وذلك نظرا لخطورة هذا النوع المستحدث من الجرائم وتأثيره على الاقتصاد الوطني.¹

ونظرا للانتشار الواسع لوسائل الإتصال خاصة شبكة الأنترنت، ومالها من أخطار كبيرة على الحياة الخاصة للأفراد، بادر المشرع الجزائري إلى تجريم المساس بحرمة الحياة الخاصة للأفراد بعد إصداره للقانون رقم 06-23 المؤرخ في 20 ديسمبر 2006 المعدل لقانون العقوبات، فجرم من خلال المواد من 303 مكرر إلى 303 مكرر²، إلتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية بغير إذن صاحبها أو رضاه، أو تسجيل أو نقل صورة لشخص في مكان خاص بغير إذن صاحبها أو رضاه.

ولإنجاح سياسته الجنائية لمكافحة الجريمة الإلكترونية واصل المشرع في تعديل قانون العقوبات ومنها القانون رقم 01/14/ المؤرخ في 2014/02/4³، فأضاف المشرع المادة 333 مكرر 1 بهدف حماية الأطفال عبر الأنترنت في القسم السادس "إنتهاك الآداب العامة" من الفصل الثاني الجنائيات والجناح ضد الأسرة والآداب العامة من الباب الثاني «الجنائيات والجناح ضد الأفراد» والتي جاءت لتعاقب كل من صور وبأي وسيلة كانت قاصرا لم يكمل 18 سنة وهو يمارس أنشطة جنسية بصفة حقيقية أو غير حقيقية، أو صور الأعضاء الجنسية لقاصر لأغراض جنسية، أو قام بإنتاج أو توزيع أو نشر أو ترويج أو استيراد أو تصدير أو عرض أو بيع أو حيازة مواد إباحية متعلقة بالقصر.

وفي سنة 2016 وفي إطار تكيف المشرع الجزائري وتحيين منظومته التشريعية مع التطورات القانونية الدولية⁴، خاصة ما تعلق منها بمكافحة جرائم الإرهاب والتي يعتمد مجرموها على هذه التقنية في تنفيذ أفعالهم الإرهابية، فقام المشرع الجزائري مرة أخرى بتعديل قانون العقوبات وإصدار القانون رقم 16-

¹ _ فضيلة عاقل، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، ورقة علمية مقدمة في إطار المؤتمر الدولي الرابع عشر حول الجرائم الإلكترونية، طرابلس، لبنان، المنعقد بين 24-25 مارس 2017، ص 127.

² _ القانون رقم 06-23 المؤرخ في 20/10/2006، يعدل ويتم الأمر رقم 66-156 المؤرخ في 08/06/1966، والمتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، عدد 84، الصادرة بتاريخ 2006/12/24.

³ _ القانون رقم 14-01 المؤرخ في 04/02/2014 يعدل ويتم الأمر رقم 66-156 المؤرخ في 08/06/1966 ويتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، العدد 7، الصادرة بتاريخ 2014/02/16.

⁴ _ محمد السعيد زناي، المرجع السابق، ص 34.

02 المؤرخ في 19 جوان 2016¹، إذ بموجبه أضاف مادتين 87 مكرر 11 و 87 مكرر 12 فجرم من خلالهما أفعالا، تعد خطيرة تتمثل في التجنيد الإلكتروني، وكذا السفر بغرض ارتكاب أفعال إرهابية أو تدبيرها أو الإعداد لها أو المشاركة فيها أو التدريب على ارتكابها أو لتلقي تدريب عليها. وبموجب نفس القانون أضاف إلى القسم السابع مكرر المادة 394 مكرر 8، فأقر المسؤولية الجزائية لمقدمي خدمات الأنترنت في حالة الإخلال بالالتزامات الواقعة على عاتقهم.

ثانيا: تعديل قانون الإجراءات الجزائية

ونظرا لخطورة الجرائم المستحدثة ومنها الجريمة الإلكترونية، قام المشرع الجزائري بسن قواعد إجرائية جديدة تتعلق بالتحقيق تتماشى مع الطبيعة المميزة للجريمة الإلكترونية وذلك من خلال تعديل قانون الإجراءات الجزائية بموجب قانون رقم 06-22²، المؤرخ في 20/12/2006 تتمثل في الإجراءات الواردة في الفصل الرابع تحت عنوان "في إعتراض المراسلات وتسجيل الأصوات والنقاط الصور" من المادة 65 مكرر 5-65 مكرر 10 من ق.إ. ج كما نص أيضا في الفصل الخامس على إجراء التسرب بموجب المادة 65 مكرر 11-65 مكرر 18.

ثالثا: القوانين الخاصة

فبعد التعديل الذي مس قانون العقوبات، أصدر المشرع مجموعة من القوانين لمواجهة الجريمة الإلكترونية بنصوص خاصة وتتمثل في:

-الأمر رقم 03-05 المؤرخ في 19/06/2003 المتعلق بحقوق المؤلف والحقوق المجاورة.³

¹ _ القانون رقم 16-02 المؤرخ في 19/06/2016 يعدل ويتمم الأمر 66-156 المؤرخ في 08/06/1966 والمتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، عدد 37، الصادرة بتاريخ 22/06/2016.

² _ القانون رقم 06-22 المؤرخ في 20/12/2006 يعدل ويتمم الأمر 66-155 المتضمن قانون الإجراءات الجزائية الجريدة الرسمية للجمهورية الجزائرية، عدد 84، الصادرة بتاريخ 24/12/2006.

³ _ الأمر رقم 03-05 المؤرخ في 19/07/2003 يتعلق بحقوق المؤلف والحقوق المجاورة، الجريدة الرسمية للجمهورية الجزائرية عدد 44، الصادرة بتاريخ 23/07/2003.

اعتبر المشرع الجزائري برامج الحاسب الآلي من المصنفات الأدبية والفنية بموجب نص المادة 04/04 وقواعد البيانات بموجب المادة 1/05 مما تطلب تعزيزها بحماية جزائية تمثلت في جرائم التقليد والوارد في المواد من 143 وما بعدها و 151 وما بعدها.

-القانون رقم 01-08 المؤرخ في 2008/01/23 المتعلق بالتأمينات الإجتماعية .

نظم هذا القانون مكافحة الجريمة الإلكترونية عن طريق هيئات الضمان الإجتماعي، في نصوص قانونية تخص البطاقة الإلكترونية، وتتضمن هذه البطاقة على معلومات شخصية تتعلق بالمؤمن له، لذا أقر لها المشرع الجزائري حماية جزائية يمكن أن تعرض صاحبها للجزاء المقررة في حالة الإستعمال غير المشروع.

-القانون رقم 04-09 المؤرخ في 2009/08/05 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها.

وكعادته المشرع الجزائري كلما تفاحلت جرائم خطيرة، يسن قوانين خاصة للوقاية منها أو مكافحتها، ومنها الجرائم الإلكترونية، حيث أصدر القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، ويتضمن القانون ستة فصول بدأت بتحديد المصطلحات، كما نصت على إجراءات متعلقة بمكافحة هذا النوع من الجرائم ويمكن تلخيصها فيما يلي:

-جواز التفتيش ولو عن بعد للمنظومة المعلوماتية أو جزء منها من طرف الجهات القضائية المختصة وضباط الشرطة القضائية.

-مراقبة الإتصالات الإلكترونية.

-إمكانية الإستعانة بالسلطات الأمنية المختصة للحصول على المعطيات محل البحث المخزنة في منظومة موجودة خارج الاقليم الوطني، وذلك طبقا للاتفاقيات الدولية ومبدأ المعاملة بالمثل.

-حجز المعطيات المعلوماتية والتزامات مقدمي الخدمات.

-التعاون الدولي والمساعدة القضائية الدولية.

-إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها.

تجاوب المشرع الجزائري مع التغيرات التي طرأت على وسائل الاتصال والإعلام واستعمالاتها في المعاملات المختلفة، فسار على نهج التشريعات المقارنة في الاعتراف بالكتابة الإلكترونية بموجب المادة 323 مكرر من القانون 10/05¹، وسأوى بين الكتابة الورقية والكتابة الإلكترونية من حيث الإثبات.

كما أصدر القانون رقم 04-15 المؤرخ في 2015/02/01 المحدد للقواعد المتعلقة بالتوقيع والتصديق الإلكتروني²، من خلال توفير حماية فنية وجنائية للتوقيع الإلكتروني.

-القانون رقم 04-18 المؤرخ في 2018/05/10 يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية³، وتضمن هذا القانون القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية جملة من الإجراءات الجديدة المنظمة للقطاع، ويهدف هذا القانون إلى تحديد الشروط التي من شأنها تطوير وتقديم خدمات البريد والاتصالات، كما أضفى هذا القانون حماية جزائية لانتهاك الحياة الخاصة للأفراد معاقب كل شخص ينتهك المراسلات السرية عن طريق البريد أو الاتصالات الإلكترونية بموجب المادة 164 من نفس القانون.

-القانون رقم 05-18 المؤرخ في 10 ماي 2018 يتعلق بالتجارة الإلكترونية⁴.

سن المشرع القانون رقم 05-18 المؤرخ في 2018/05/10 يتعلق بالتجارة الإلكترونية ويعد مشروعا أعد من طرف وزارة البريد وتكنولوجيا الاتصال السلكية واللاسلكية، ويهدف هذا القانون إلى تحديد القواعد العامة المتعلقة بالتجارة الإلكترونية للسلع والخدمات، وقد تضمن هذا القانون أربعة أبواب، تضمن الباب الأول الأحكام العامة، الباب الثاني ممارسات التجارة الإلكترونية، أما الباب الثالث يتضمن المخالفات والعقوبات المقررة، فيما خص الباب الأخير للأحكام الانتقالية، وجاء هذا القانون لسد الفراغ

¹ _ القانون 05-10 المؤرخ في 2005/06/20، يعدل ويتمم الأمر 75-85 المؤرخ في 1975/09/26 يتضمن القانون المدني، الجريدة الرسمية للجمهورية الجزائرية، عدد 44، الصادرة بتاريخ 2005/06/26.

² _ قانون 04-15 المؤرخ في 2015/02/01، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، الجريدة الرسمية للجمهورية الجزائرية، عدد 06، الصادرة بتاريخ 2015/02/10.

³ _ القانون 04-18 المؤرخ في 2018/05/10 يعدل ويتمم القانون رقم 2000-03 المؤرخ في 2000/08/05، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، الجريدة الرسمية للجمهورية الجزائرية، عدد 27، الصادرة بتاريخ 2018/05/13.

⁴ _ القانون رقم 05-18 المؤرخ في 2018/05/10 يتعلق بالتجارة الإلكترونية، الجريدة الرسمية للجمهورية الجزائرية، عقد 28، الصادرة بتاريخ 2018/05/16.

القانوني الذي كانت تعاني منه الجزائر في مجال المعاملات التجارية الإلكترونية، وفي نفس السنة أصدر المشرع الجزائري لحماية المعطيات ذات الطابع الشخصي للأشخاص الطبيعة أثناء المعاملات الإلكترونية المتمثل في:

-القانون رقم 07-18 المؤرخ في 2018/06/10 يتعلق بحماية الأشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي¹، أدرج المشرع الجزائري مفهوم المعطيات الشخصية لأول مرة إثر تعديل دستور سنة 2016 وذلك وفقا لما نصت عليه المادة 4/46 على أنه «...حماية الأشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي حق أساس يضمنه القانون ويعاقب على انتهاكه»²، إلا أنه لم ينظم أعمال المعالجة للمعطيات ذات الطابع الشخصي، إلا خلال عام 2018 حيث أصدر قانون 07/18 والذي يعتبر قانون أخلاقيات معالجة المعطيات ذات الطابع الشخصي بحسب قول بعض الفقهاء³، في فرنسا عندما صدر قانون المعلوماتية في فرنسا سنة 1978.

ويهدف قانون 07-18 إلى ضرورة أن تتم معالجة المعطيات ذات الطابع الشخصي، مهما كان مصدرها أو شكلها، في إحترام الكرامة الإنسانية والحياة الخاصة والحريات العامة وألا تمس بحقوق الأشخاص وشرفهم وسمعتهم، وهذا ما جاء في نص المادة الثانية من هذا القانون⁴، وقد جاء متكونا من 76 مادة موزعة على سبعة أبواب.

رابعا: الإتفاقيات

صادقت الجزائر على الإتفاقية العربية لمكافحة جرائم تقنية المعلومات بالمرسوم الرئاسي رقم 14-252 المؤرخ في 2014/09/08، وتهدف هذه الإتفاقية إلى تعزيز التعاون وتدعيمه بين الدول العربية، في مجال مكافحة جرائم تقنية المعلومات لدرء أخطار هذه الجرائم، حفاظا على أمن الدول العربية

¹ _ القانون رقم 07-18 المؤرخ في 2018/06/10 يتعلق بحماية الأشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي، الجريدة الرسمية للجمهورية الجزائرية، عدد 34 الصادرة بتاريخ 2018/06/10.

² _ المادة 46 من التعديل الدستوري بمقتضى قانون 01/16 لمؤرخ في 6 مارس 2016، الجريدة الرسمية للجمهورية الجزائرية، عدد 14، الصادرة في 2016/03/07.

³ _ عز الدين طباش، الحماية الجزائرية للمعطيات الشخصية في التشريع الجزائري دراسة في ظل قانون 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، المجلة الأكاديمية للبحث القانوني، العدد 02، 2018، ص 28.

4 - أنظر المادة 02 من القانون 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي.

ومصالحها وسلامة مجتمعاتها وأفرادها، فهذه الاتفاقية جاءت لتكميل النقائص الموجودة في الترسانة القانونية لمكافحة الجريمة الإلكترونية وتكون سنداً لدعم سياسته الجنائية.

كذلك اتفاق الشراكة الأورو متوسطي بين الإتحاد الأوروبي والجزائر بتاريخ 2002/04/22 وصادقت عليها الجزائر بموجب القانون رقم 1144/2003 بتاريخ 2003/12/02.

بعد استعراض مجموعة القوانين التي أصدرها المشرع الجزائري لمواجهة الإجرام المعلوماتي، سوف نتطرق إلى تفصيل أهم صور للجرائم المنتشرة سواء المنصوص عليها في القوانين العامة، وكذا الصور التي شملتها نصوص خاصة ويكون ذلك في الفصل الثاني من هذا الباب.

الفصل الثاني: المواجهة التشريعية للجريمة الإلكترونية

لقد أدى الاستخدام المتزايد للحاسب الآلي في كافة مجالات الحياة اليومية، وكذا التطور السريع في مجال المعلوماتية وتكنولوجيا الاتصالات إلى ظهور أنواع جديدة من الجرائم، تختلف عن الجرائم التقليدية في أطرافها، ومكان ارتكابها وموضوعها وأساليبها، تتمثل في الجرائم الإلكترونية، التي تعتبر من الجرائم المستحدثة كونها تطل الكيان المنطقي للحاسب الآلي بما يشمله من برامج ومعطيات، حيث تخلف هذه الجرائم آثارا نفسية واجتماعية واقتصادية وأمنية بالغة الخطورة سواء على مستوى الأفراد أو الدولة، وعندما تعرفنا على ماهية الجرائم الإلكترونية من حيث تعريفها وذكر خصائصها ومبررات حمايتها، والجهود المبذولة سواء الدولية أو الإقليمية والذي كان لها بالغ الأثر على مستوى التشريع الوطني، الذي سن تشريعات تخص مكافحة هذه الجريمة التي نص عليها المشرع الجزائري في قانون العقوبات أو نصوص خاصة لهذا سوف نتناول في هذا الفصل مبحثين خصصنا المبحث الأول (مواجهة الجريمة الإلكترونية بموجب قانون العقوبات)، والمبحث الثاني (مواجهة الجريمة الإلكترونية بموجب قوانين خاصة).

المبحث الأول: مواجهة الجريمة الإلكترونية بموجب قانون العقوبات

إن ظاهرة الإجرام المعلوماتي تستدعي ضرورة حماية جنائية جديدة كونه إجراما يقوم على انتهاك المواقع المعلوماتية وسرقة بياناتها وأموالها الإلكترونية، وهذه الحماية الجنائية تستوجب استحداث نصوص حديثة، فالنصوص الجنائية التقليدية عاجزة عن مواجهتها ما جعل المشرع الجزائري يقوم بتعديل قانون العقوبات للنص على جملة من الجرائم منها جريمة القذف والسب أو الإهانة باستعمال الوسائل الإلكترونية (المطلب الأول)، جرائم المساس بأنظمة المعالجة الآلية للمعطيات (المطلب الثاني) إضافة لإستحداث نص خاص بجريمة الإرهاب الإلكتروني (المطلب الثالث) ثم نتعرض في (المطلب الرابع) لجرائم الإعتداء على حرمة الحياة الخاصة والتي باتت تشكل تهديدا كبيرا للخصوصية وأخيرا جرائم الإستغلال للأطفال في المواد الإباحية عبر شبكة الأنترنت في (مطلب خامس) وذلك فيما يلي:

المطلب الأول: جريمة القذف أو السب أو الإهانة باستعمال الوسائل الإلكترونية

تعد من الجرائم الأكثر إنتشارا وشيوعا في نطاق شبكة الأنترنت جرائم الذم والقذف والتحقير، إذ يساء إستخدامها للنيل من شرف الغير أو كرامته أو اعتباره، ففي إطار مجتمع المعلومات الإلكترونية يجد

العابثون حرية في نشر وبث رسائل تحتوي عبارات الذم والقذح والتحقير اتجاه آخرين مستهدفين بذاتهم، بصفة وجاهية أو غيابية أو بواسطة الوسائط الإلكترونية السمعية والسمعية البصرية¹، تناول المشرع هذه الجرائم ضمن قانون العقوبات المعدل والمتمم بموجب القانون 09-01 المؤرخ في 26/09/2001، ويعتبر أول نص تشريعي في مجال الإجرام المعلوماتي من خلال المواد 144 مكرر و144 مكرر 1 والمادة 146 وهي الجرائم المتعلقة بالقذف والسب والإهانة، الماسة بالإساءة لرئيس الجمهورية والرسول والأنبياء، أو ضد الهيئات المؤسسة أو الهيئات العمومية لهذا سوف نتطرق إلى جريمة الإساءة لرئيس الجمهورية (الفرع الأول) والهيئات الأخرى في (الفرع الثاني).

الفرع الأول: جريمة الإساءة لرئيس الجمهورية

إن الأفعال التي تمس وتخدش شرف واعتبار رئيس الجمهورية تشمل جرائم الإهانة والقذف والسب باستعمال الوسائل الإلكترونية سنحاول من خلال هذا الفرع تناو هذه الجرائم.

الفقرة الأولى: جريمة الإهانة².

تنص المادة 144 مكرر من ق.ع.ج على "يعاقب بالحبس من ثلاثة (3) أشهر إلى اثني عشر (12) شهرا وبغرامة من 50.000 دج إلى 250.000 دج بإحدى العقوبتين فقط كل من أساء لرئيس الجمهورية بعبارات تتضمن إهانة أو سبا أو قذفا سواء كان ذلك عن طريق الكتابة أو الرسم أو التصريح أو بأي آلية لبث الصورة أو الصورة أو بأية وسيلة الكترونية أو معلوماتية أو إعلامية أخرى.

تباشر النيابة العامة إجراءات المتابعة تلقائيا، وفي حالة العود تضاعف عقوبة الحبس والغرامة المنصوص عليها في هذا المادة³.

ونقصد بالإهانة "كل قول أو فعل يحكم العرف بأن فيه ازدراء وحط من الكرامة في أعين الناس وإن

¹ محمد أمين أحمد الشوابكة، المرجع السابق، ص 31.

² حددت المادة 144 ق.ع.ج على صفة المجني عليهم والذي يكون ضحية لجريمة الإهانة بقولها «يعاقب بالحبس من شهرين (2) إلى سنتين (2) وبغرامة من 1.000 دج إلى 500.000 دج أو بإحدى هاتين العقوبتين فقط كل من أهان قاضيا أو موظفا، أو ضابطا عموميا أو قائدا أو ضابطا عموميا أو أحد رجال القوة العمومية أو أحد رجال القوة العمومية بالقول أو الإشارة أو التهديد أو إرسال أو تسليم أي شيء إليه بالكتابة أو الرسم غير العلانيين أثناء تأدية وظائفهم أو مناسبة تأديتها، وذلك بقصد المساس بشرفهم أو اعتبارهم أو الاحترام واعتبارهم أو الاحترام لواجب لسطنتهم» وتعديل قانون العقوبات أضاف المشرع إلى قائمة المحمين من الإهانة رئيس الجمهورية (المادة 144 مكرر)، البرلمان المجالس القضائية، والجيش الشعبي والهيئات العمومية.

³ - عدلت هذه المادة بموجب القانون رقم 14/11 المؤرخ في 2 أوت 2011 المعدل والمتمم للقانون 156/66 المؤرخ في 08/07/1966 المتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، عدد، الصادرة بتاريخ 10/08/2011.

لم يشمل قذفاً أو لبساً أو افتراء.¹

و تقوم جريمة الإساءة لرئيس الجمهورية على الركن المادي والمعنوي وعقوبة مقررة لها، إضافة إلى الركن المفترض المتمثل في صفة الضحية وهو المساس بشرف رئيس الجمهورية واعتباره.

أولاً: الركن المادي

يتمثل النشاط الإجرامي في إهانة رئيس الجمهورية انتقاصاً للاحترام الواجب له ليس بوصفه إنساناً فحسب، وإنما باعتبار صفة أساسية فيه وهي صفته الوظيفية أو مركزه السياسي وهذه الصفة ذاتها يتوجب أن يكون لها الاحترام²، وذلك باستعمال الكتابة أو الرسم أو التصريح أو آليات بث الصورة أو الصورة أو بأي وسيلة إلكترونية أو معلوماتية أو إعلامية أخرى، فالمشرع الجزائري ركز على الوسائل المستعملة التي تتحقق معها العلانية، ولكن ما يهمنا هو تبيان الوسائل الإلكترونية أو المعلوماتية المستعملة، في ذلك والتي ترك فيها المشرع الباب مفتوحاً أمام ظهور وسائل إعلامية جديدة والتي تنطبق على جريمة الإهانة والسب والقذف³، سوف نتناول بعض هذه الوسائل كآلاتي:

1- البريد الإلكتروني (e-mail)

يعد البريد الإلكتروني من أقدم التطبيقات وأكثرها انتشاراً، وهو يتكون من جزئين رئيسيين هما: رأس (Header) ونص (body) ويحتوي الرأس على معلومات حول المرسل والمتلقي والمعلومات اللازمة لتوصيل الرسالة إلى العنوان المناسب، ويحتوي النص على الرسالة التي تم تكوينها، وعندما يرسل شخص ما رسالة إلى شخص آخر، فإنها تنتقل من كمبيوتر المرسل عبر خط تليفون إلى الكمبيوتر الخادم أو ما يسمى ملقم البريد (server Mail) والذي يوجد به صندوق بريد المرسل ومن ثم تنتقل على نحو مباشر أو غير مباشر إلى أي كمبيوتر خادم آخر يخزن صندوق المرسل إليه، وعندها يستطيع المرسل إليه استرجاع محتويات صندوق بريده الإلكتروني عند اتصاله بالخادم الخاص به⁴، ومن خلال البريد

¹ - عمر سالم، الدفع بالحقيقة في جريمة القذف ضد ذوي الصفة -دراسة مقارنة- دار النهضة العربية، القاهرة، ط1، 1995، ص، ص، 25-25.

² - عادل بوزيدة، الإطار القانوني لمكافحة جريمة الإساءة لرئيس الجمهورية عبر المواقع الإلكترونية في التشريع الجزائري، مجلة الحقوق و العلوم السياسية ، المجلد 03، العدد 02، جوان 2016، ص 342.

³ - يزيد بوحليط، المرجع السابق، ص 113.

⁴ - محمد أمين أحمد الشوابكة، المرجع السابق، ص 33.

الإلكتروني يستطيع الجاني إرسال الكتابات والرسوم والصور الإستهزائية، فيتسلمها عدد كبير من المتعاملين مع الأنترنت، وبما أن الكتابة تشكل الاستخدام الأكبر لأنترنت، فإن القذف والسب الخطي يشكل الصورة الغالبة تمثل هذا النوع من الجرائم.¹

2- مجموعات الأخبار (news groups)

هي عبارة عن أماكن وساحات إفتراضية للقاء والتحدث بين مستخدمي شبكة الأنترنت من ذوي الإهتمامات المشتركة الذين يؤلفون فيما بينهم مجموعات نقاش وتبادل للبيانات والمعلومات والأفكار حول موضوع معين²، وذلك عن طريق نظام نيوز جروب (newsgroups) أو نظام يوزنت (Usenet) ويمكن أن ترتكب جرائم القذف والسب من خلال مجموعات الأخبار، ومثال ذلك قيام هؤلاء المشتركين أثناء تبادل الرسائل أو في صدد تعليقهم ومشاركتهم على موضوع معين، بإيراد عبارات تنال من شرف واعتبار أحد المشتركين، حيث تتحقق علانية الفعل لكون المشتركين في مجموعات الأخبار يمكنهم أن يروا ما يرد من رسائل وتعليقات حول الموضوع الذين اختاروه لمناقشتهم.³

3- غرف المحادثة (chat rooms)

غرف المحادثات أو الثثرة عبارة عن ساحات معروفة في الفضاء الإلكتروني تتيح لمستخدميها الاشتراك في محادثات بين بعضهم البعض، بإرسال البريد الإلكتروني الذي يمكن قراءته من قبل الشخص المشترك في غرف المحادثة، في الواقع عندما نتخاطب عبر الأنترنت فإن ما يحدث هو أنك تكتب رسالة بإستخدام لوحة المفاتيح، بحيث يمكن للآخرين رؤية ما تكتب، وبعدها يكتبون رسائل على لوحات المفاتيح الخاصة بهم، فالفائز على عملية التخاطب لا يحدث بالفعل مع شخص الآخر ولا يسمع ما يقوله⁴، ويمكن أن نقوم جريمة قذف أو سب عبر غرف المحادثة بخدش شرف واعتبار أي شخص سواء من خلال نشر مقالات أو صور أو رسوم كاريكاتورية أو نشر تعاليق.⁵

¹ _محمد أمين أحمد الشوابكة، المرجع السابق، ص 34.

² _نهلا عبد القادر المومني، المرجع السابق، ص 41.

3 _عادل عزام سقف الحيط، جرائم الذم والتحقيق المرتكبة عبر الوسائط الإلكترونية -دراسة مقارنة- دار الثقافة، الأرين، ط1، 2011، ص202.

⁴ _طارق عبد الحق، برمجيات الأنترنت الملاحقة والاستكشاف، قصر الكتاب، الجزائر، ط1، 2005، ص 27.

⁵ _مصطفى محمد مرسى، التحقيق الجنائي في الجرائم الإلكترونية، مطابع الشرطة، القاهرة، ط1، 2009، ص 102.

4- شبكة الويب العالمية (world wide world)

وتعرف بالرمز (www) التي تتيح للمستخدم تصفح مواقع المعلومات، وهذه الخدمة تجمع النصوص والصور والأصوات والأفلام المتحركة، مما تتيح للمستخدم الحصول على المعلومات التي يريدها في أسرع وقت¹، ويتم ارتكاب أفعال الذم والقذح والتحقير عبر شبكة الويب العالمية، من خلال إسناد مادة كتابية، صوتية، فيديو صوتية (سمع بصرية) تسيء إلى أحد الأشخاص، ومن شأنها أن تنال من شرفه وكرامته أو تعرضه إلى بغض الناس وإحتقارهم، كما يمكن من خلال صفحات الويب (web pages) يتم نشر وإذاعة وتوزيع الكتابات أو الرسوم أو الصورة الاستهزائية².

ثانيا: الركن المعنوي

فجريمة الإساءة لرئيس الجمهورية هي جريمة عمدية يتخذ الركن المعنوي فيها صورة القصد الجنائي العام والذي يتحقق متى كان الجاني عالما بحقيقة الوقائع التي ينسبها لرئيس الجمهورية، واتجاه إرادته إلى إذاعة هذه الوقائع عبر الوسائل الالكترونية والمعلوماتية³.

ثالثا: العقوبة المقررة

تعاقب المادة 144 مكرر ق.ع.ج مرتكب هذه الجريمة في صورتها البسيطة بالحبس من ثلاثة (3) أشهر إلى اثني عشر شهرا وبغرامة من 50.000 دج إلى 250.000 أو بإحدى هاتين العقوبتين على أن تضاعف عقوبة الحبس المقررة متى اقترنت الجريمة بحالة العود.

الفقرة الثانية: جريمة القذف

يعرف القذف لغة هو الرمي والتوجيه، ويقال قذف الشيء يقذفه قذفا كذلك القذف الرمي بالسهم والحصى كل شيء مما يضر ويؤذي، فالقذف هو الرمي بالسهم والحصى والكلام⁴.

أما القذف اصطلاحا هو نشر موضوع من شأنه المساس بسمعة شخص أو هيئة أو منتج لدى

¹ _ نهلا عبد القادر المومني، المرجع السابق، ص 40.

² _ محمد أمين أحمد الشوابكة، المرجع السابق، ص 38.

³ _ عادل بوزيدة، المرجع السابق، ص 343.

⁴ _ سالم روضان الموسوي، جرائم القذف والسب عبر القنوات الفضائية-دراسة مقارنة بتطبيقات قانونية-، منشورات الحلبي، بيروت، ط1، 2012، ص 16.

الجمهور¹، ويعرف كذلك بأنه "إسناد واقعة محددة تستوجب عقاب من تتسبب إليه أو احتقاره إسنادا علنيا عمديا²، أو إنه "كل إسناد علني عمدي، أو ادعاء بواقعة محددة تستوجب عقابا أو احتقارا من أسندت إليه".³

نظم المشرع الجزائري جريمة القذف بموجب المادة 296 من قانون العقوبات الجزائري والتي عرفت القذف بأنه "يعد قذفا كل ادعاء بواقعه من شأنها المساس بشرف واعتبار الأشخاص، أو الهيئات المدعى عليها بها أو إسنادها إليهم، أو إلى تلك الهيئة ويعاقب على نشر هذا الإدعاء أو ذلك الإسناد مباشرة أو بطريق إعادة النشر، حتى ولو تم ذلك على وجه التشكيك، أو إذا قصد به شخص أو هيئة دون ذكر الاسم ولكن كان من الممكن تحديدهما من عبارات الحديث أو الصياح أو التهديد أو الكتابة أو المنشورات أو اللافتات أو الإعلانات موضوع الجريمة."، في حين نجد المشرع الفرنسي نص على جريمة القذف ضمن أحكام قانون الإعلام الصادر بتاريخ 29 جويلية 1881 المتعلق بحرية الصحافة المعدل والمتمم.

أولا: الركن المادي

لوقوع جريمة القذف يشترط تحقق ثلاثة عناصر هي:

1- الإسناد

ويفيد الإسناد نسبة الواقعة أو الأمر إلى الشخص المقذوف على سبيل التأكيد، كما يتحقق الإسناد سواء على سبيل القطع أو التشكيك⁴، وبعبارة أخرى فإن الإسناد يتحقق بمجرد الإخبار بواقعة تحتمل الصدق أو الكذب، وباستعمال هذين التعبيرين يدل أن المشرع الجزائري قصد أن يشمل بالعقاب كل حالات التعبير التي من شأنها أن تنال من شرف واعتبار الأشخاص أو الهيئة المدعى عليها به، ولو كان بطريقة تفيد التشكيك أو الإستفهام أو الغموض⁵، ويستوي في القذف أو يسند القاذف الأمر الشائن إلى

¹ _خالد لعلاوي، جرائم الصحافة المكتوبة في القانون الجزائري-دراسة قانونية بنظرة إعلامية، دار بلقيس، الجزائر، د ط، 2012، ص 79.

² _انسام سمير طاهر الحجامي، جريمتي القذف والسب عن طريق الأنترنت، مجلة رسالة الحقوق، العدد2، 2015، ص 339.

³ _محمد صبحي نجم، شرح قانون العقوبات- القسم الخاص-، ديوان المطبوعات الجامعية، الجزائر، د ط، 2000، ص 38.

⁴ _سالم روضان الموسوي، المرجع السابق، ص 23.

⁵ _محمد صبحي نجم، المرجع السابق، ص 99.

المقذوف على أنه عالم به، أو يسنده إليه بطريق الرواية عن الغير أو يردده على أنه مجرد إشاعة.¹

2-موضوع الإسناد

يشترط لقيام الركن المادي لجريمة القذف أن تكون هناك واقعة محددة، من شأنها أن تجعل من أسندت إليه محلا للازدراء والعقاب، وهذا ما يميز بين القذف عن السب، فالقذف يشترط لقيامه أن تكون الواقعة محددة، ولا يشترط ذلك لقيام جريمة السب بل يكفي أن يكون خادشا للشرف والاعتبار، ويجب أن تكون الواقعة معاقبا عليها طبقا للقانون، ويشمل ذلك كل الجرائم سواء أكانت جنائية أو تأديبية وذلك لورود النص مطلقا، بشرط أنها توجب الإزدراء والإحتقار عند أهل المجني عليه، أو تحط من شرفه واعتباره²، كما يجب أن يكون الإسناد المعاقب عليه موجها إلى شخص معين، سواء كان شخصا طبيعيا أو شخصا معنويا وليس من الضروري أن يكون معينا بالإسم، وإنما يكفي لقيام القذف أن تكون عبارته موجهة على صورة يمكن معها فهم المقصود منها، ومعرفة الشخص الذي يعنيه القانون وهي مسألة تقديرية تناط بقاضي التحقيق.³

3-العلانية

لا تقوم جريمة القذف إلا بتوافر العلانية في وسيلة الإسناد التي استعملها الجاني، ويقصد بها إتصال علم الجمهور بالتعبير الصادر عن فكرة المتهم، أو رأيه أو شعوره عبر إحدى الوسائل التعبيرية والتي لا تخرج عن ثلاث هي: القول أو الصياح، الفعل أو الإيماء، الكتابة وما يقوم في حكمها⁴، أو بأي وسيلة أخرى من وسائل التعبير عن الرأي أو المعنى، ونعني هنا كافة الوسائل الإلكترونية كإرسال الرسائل النصية والصوتية وملفات الفيديو بواسطة الهاتف، كما يمكن نشر الصور والتعليق الساخرة على شبكة

¹ _قضى بأنه يستوي أن تكون عبارات القذف أو السب التي أذاعها الجاني منقولة عن الغير أو من إنشائه هو، ذلك أن نقل الكتابة التي تتضمن جريمة ونشرها يعتبر في حكم القانون كالنشر الجديد سواء بسواء. أنظر: خالد بن محمد بن عوض آل شنيف القرني، القذف بواسطة الرسائل الإلكترونية وعقوبته في النظام السعودي، مذكرة لنيل شهادة الماجستير، كلية العدالة الجنائية، جامعة نايف للعلوم الأمنية، الرياض، 1024، ص32.

² _محمد عبيد الكعبي، المرجع السابق، ص 122.

³ _أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص-الجزء الأول-، دار هومة، الجزائر، ط17، 2014، ص 22.

⁴ _حسن بن سعيد الغافري، السياسية الجنائية في مواجهة جرائم الانترنت-، دار النهضة العربية، القاهرة، دط، 2009، ص

الأنترنت بواسطة المواقع الإلكترونية أو مواقع التواصل الاجتماعي¹، فهي الركن المميز لجنحة القذف وتمثل أساس العقاب عليها، لأن خطورة هذه الجريمة لا تكمن في العبارات المسيئة فحسب وإنما في إعلامها للجمهور.

ثانيا: الركن المعنوي

جريمة القذف جريمة عمدية تتطلب توافر القصد الجنائي العام بعنصرية العلم والإرادة، حيث يكون الجاني على علم بأركان جريمة القذف ونتيجتها الإجرامية، واتجاه إرادته على القيام بهذا الفعل، ولا تتطلب قصدا جنائيا خاصا، إذ يكفي أن يأتي الجاني أحد الأفعال الواردة في المادة 269 من ق.ع.ج.

ثالثا: العقوبة المقررة

يعاقب على مرتكب جريمة القذف بالحبس من ثلاثة أشهر إلى إثني عشر شهرا وبغرامة من 50.000 دج إلى 250.000 دج وفي حالة العود تضاعف عقوبة الحبس والغرامة.

الفقرة الثالثة: جريمة السب

يعرف السب لغة على أنه " الشتم سواء بإطلاق اللفظ الصريح الدال عليه، أو باستعمال المعاريض التي تؤدي إليه"²، ويعرف اصطلاحا على أنه " خدش شرف شخص واعتباره عمدا دون أن يتضمن ذلك واقعة معينة إليه"³.

نص المشرع الجزائري على جريمة السب، بموجب المادة 297 من ق.ع.ج بقوله "يعد سببا كل تعبير مشين أو عبارة تتضمن تحقيرا أو قدحا لا ينطوي على إسناد أية واقعة".

أولا: الركن المادي

يتمثل النشاط الإجرامي في جريمة السب في تعبير معين يحط من قدر المجني عليه، وينال من سمعته بأي وجه من الوجوه، كما يتحقق النشاط الذي يخدش شرف أو اعتبار المجني عليه بإسناد عيب معين دون أن يحدد واقعة معينة، وذلك كأن ينسب المجني عليه صفة إجرامية معينة موصفه أو نعتة

¹ يزيد بوحليط، المرجع السابق، ص 118.

² شمسان ناجي صالح الخيلي، الجرائم المستخدمة بطرق غير مشروعة لشبكة الأنترنت - دراسة مقارنة -، دار النهضة العربية، القاهرة، د ط، 2009، ص 153.

³ -انسام سمير طاهر الحجامي، المرجع السابق، ص 344

بأنه لص أو مزور أو قاتل أو مرتش¹، ولا عبرة بالوسيلة أو الأسلوب الذي تصاغ به عبارات السب، فهو يتحقق بكل صيغة توكيدية أو تشكيكية صريحة أو ضمنية، كما يشترط أن يكون السب موجها إلى شخص معين، حتى يمكن القول بأنه قد نال من شرفه ومكانته الإجتماعية سواء كان شخصا طبيعيا أو معنويا²، ولا يشترط تحديد شخص المجني عليه بالإسم، بل يكفي أن يكون من السهل التعرف عليه.

1- العلانية

تشترط جريمة السب العلانية وهي نفسها المقررة للقذف وتتحقق بالكتابة أو الصور أو بالوسائل السمعية البصرية أو بأي وسيلة إلكترونية أو إعلامية أخرى، وهذا ما تطرقنا إليه في جريمة القذف، غير أن العلنية ليست ركنا أساسيا في جريمة السب، إذ لا تنتفي الجريمة بانتفاء العلانية وإنما تتحول من جنحة إلى مخالفة حسب المادة 02/463³، ولكن المشرع لم يشر إلى العلانية في نص المادة 297 من ق. ع ج خلافا للمشرع الفرنسي والمصري الذي اشترطا هذا العنصر في الجنحة.

ثانيا: الركن المعنوي: جريمة السب جريمة عمدية، ومن ثم يتخذ ركنها المعنوي صورة القصد الجنائي، والقصد في جريمة السب قصد عام، يتطلب توافر عنصري العلم والإرادة، وبناء على ذلك يتعين ثبوت علم الجاني بمعنى الألفاظ التي صدرت عنه، وأن يكون مدركا لمعنى الألفاظ التي صدرت منه بأن من شأنها خدش المجني عليه أو إعتباره، كما تتجه إرادته إلى إثيان السلوك المتمثل في القول أو الكتابة أو الرسالة الموجهة عن طريق شبكة الأنترنت، أو الهاتف أو أي وسيلة أخرى⁴.

ثالثا: العقوبة المقررة

الحبس من ثلاثة أشهر إلى اثني عشر شهرا وبغرامة من 50.000 دج إلى 250.000 دج وفي حالة العود تضاعف العقوبة والغرامة.

¹ يوسف حسن يوسف، المرجع السابق، ص 206.

² محمد صخري، شرح جريمة السب في القانون الجزائري، الموسوعة الجزائرية للدراسات السياسية والإستراتيجية منشور على الموقع: <https://www.politics.dz.com> أطلع عليه 2019/11/25 على الساعة 17.00.

³ تنص المادة 463 فقرة 02 من ق.ع. ج على أنه «يعاقب بغرامة من 30 إلى 100 دج ويجوز أن يعاقب أيضا بالحبس لمدة ثلاثة أيام على الأكثر كل من ألقى بغير احتياط أقذرا على أحد الأشخاص كل من ابتدر أحد الأشخاص بألفاظ سباب غير علنية دون أن يكون قد استفزه».

⁴ يوسف حسن يوسف، المرجع السابق، ص 208.

الفرع الثاني: جرائم الإهانة والقذف والسب في حق مؤسسات الدولة

وهي الجرائم المنصوص عليها في المادة 146 من ق.ع.ج والتي تنص على " تطبق على الإهانة أو السب أو القذف الموجه بواسطة الوسائل التي حددتها المادة 144 مكرر ضد البرلمان أو أحد غرفتيه أو ضد الجهات القضائية أو ضد الجيش الشعبي الوطني أو أية هيئة نظامية أو عمومية أخرى، العقوبات المنصوص عليها في المادة المذكورة أعلاه، في حالة العود تضاعف الغرامة".

أولاً: الركن المادي

لقد تناولنا جرائم الإهانة والسبب والقذف وقمنا بتحليل ركنها المادي والمعنوي والعقوبات المقررة لها في الفرع الأول لهذا وتناديا للتكرار سوف نتطرق إلى صفة المجني عليهم.¹

ثانياً: صفة المجني عليه

حددت المادة 146 من ق.ع.ج صفة المجني عليهم التي ترتكب ضدهم الجرائم الماسة بالشرف والإعتبار.

-البرلمان أو أحد غرفتيه

نصت المادة 112 من التعديل الدستوري المؤرخ في 2016/03/06 على «يمارس السلطة التشريعية برلمان يتكون من غرفتين، وهما المجلس الشعبي الوطني ومجلس الأمة، وله السيادة في إعداد القانون والتصويت عليه.

-الجهات القضائية

نصت المادة 02 من القانون رقم 05-11 المؤرخ في 2005/07/17 المتعلق بالتنظيم القضائي على " التنظيم القضائي يشمل النظام القضائي العادي والنظام القضائي الإداري ومحكمة التنازع ويشمل النظام القضائي العادي المحكمة العليا والمجالس القضائية والمحاكم، كما يشمل النظام القضائي الإداري مجلس الدولة والمحاكم الإدارية".²

¹ -يزيد بوحليط، المرجع السابق، ص 119.

² -المادتان 03 و 04 وما بعدهما من القانون رقم 05-11 المؤرخ في 2005/07/17 المتعلق بالتنظيم القضائي، الجريدة الرسمية للجمهورية الجزائرية، عدد 51 الصادرة بتاريخ 2005/07/20.

-الجيش الوطني الشعبي: هي مؤسسة الجيش الشعبي الوطني، وظيفتها الدفاع عن أرض الوطن ضد أي أخطار تهدد أمنه، واستقراره وهو ما نصت عليه المادة 25 من دستور 1996.¹

-الهيئات النظامية أو العمومية

وتتمثل في مديرية الأمن الوطني، والمديرية العامة للجمارك، والمديرية العامة للحماية المدنية وكل المؤسسات العمومية ذات الطابع الإداري كالجامعات والمعاهد...إلخ.

المطلب الثاني: جرائم المساس بأنظمة المعالجة الآلية للمعطيات

ركزت إستراتيجية المشرع الجزائري في مواجهة الجريمة الإلكترونية، على إصدار القسم السابع مكرر من قانون العقوبات رقم 15/04² تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات"، جملة من قواعد قانونية موضوعية، حدد من خلالها كل الأفعال الماسة بنظم المعالجة الآلية للمعطيات، وما يقابلها من جزاء أو عقوبة،³ وذلك بموجب المواد من 394 مكرر إلى 394 مكرر 7، حاول من خلال هذه النصوص حماية مصالح متعلقة بمعطيات الحاسب الآلي، وجرم العدوان عليها وهي سرية المعطيات وسلامتها أو تكاملها، وإتاحتها أو وفرتها، وتعرف هذه الجرائم كذلك بجرائم الإختراق.

ولحماية سرية المعلومات قام المشرع الجزائري، بتجريم الدخول غير المصرح به إلى أنظمة المعالجة الآلية للمعطيات، أما فيما يتعلق بحماية سلامة المعطيات أو تكاملها جرم التلاعب بالمعطيات، وكذلك تخريب أنظمة المعالجة الآلية للمعطيات كظرف مشدد، والنص على هذه الجرائم يحمي المعطيات في إتاحتها ووفرتها.⁴

¹ نصت المادة 25 من دستور 1996 على "... تتمثل المهمة الدائمة للجيش الشعبي في المحافظة على الاستقلال الوطني والدفاع عن السيادة الوطنية، كما يضطلع بالدفاع عن وحدة البلاد وسلامتها الترابية، وحماية مجالها البري والجوي، ومختلف مناطق أملاكها البحرية.

² -القانون رقم 15/04 المؤرخ في 2004/11/01 يعدل ويتم الأمر رقم 156/66 المتعلق بقانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، عدد 71 الصادرة بتاريخ 2004/11/15.

³ -راضية عيمور، الجريمة الإلكترونية وآليات مكافحتها في التشريع الجزائري، المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد السادس، عدد الأول، 2022، ص 99.

⁴ -عالم المشرع الجزائري هذه الجرائم متبعا في ذلك نهج المشرع الفرنسي، وكذلك فعلت إتفاقية بودابست وقد أشارت المذكرة التفسيرية لهذه الأخيرة إلى أن هذه الصور تمثل التهديدات الرئيسية وفقا للمناقشات التي دارت حوله أمن الحاسبات والبيانات التي تؤثر على نظم المعالجة الآلية وإرسال البيانات.

ولذا سيتم التعرف على أنواع الصور المختلفة لهذه الجرائم، وبيان أركانها والعقوبات المقررة لها.

الفرع الأول: جريمة الدخول أو البقاء غير المصرح به

قبل دراسة هذه الجرائم يقتضي الأمر فهم ودراسة نظام المعالجة الآلية للمعطيات باعتباره شرطا مفترضا لقيام هذه الجرائم.

الفقرة الأولى: مفهوم نظام المعالجة الآلية للمعطيات

يعد نظام المعالجة الآلية للمعطيات الشرط الأولي للبحث، في توافر أو عدم توافر أي جريمة من جرائم الإعتداء على نظام المعالجة، فإذا تخلف هذا الشرط لا يمكننا الحديث عن قيام هذه الجريمة، إذ أن هذا الشرط يعتبر عنصرا لازما لكل منها، لذلك يكون من الضروري تحديد مفهوم مصطلح نظام المعالجة الآلية للمعطيات فهو تعبير تقني يصعب على المشتغل بالقانون إدراك حقيقته بسهولة، فضلا عن أنه تعبير متطور يخضع للتطورات السريعة والمتلاحقة في فن الحاسبات الآلية¹، لذلك يجب تحديد مفهومه.

أولا: تعريف نظام المعالجة الآلية للمعطيات

قدمت إتفاقية بودابست تعريفا للنظام المعلوماتي، في مادتها الأولى على أنه "يقصد بمنظومة الكمبيوتر أي جهاز أو مجموعة من الأجهزة المتصلة ببعضها البعض أو التي ذات صلة بذلك، ويقوم أحدهما أو أكثر من واحد منها، تبعا للبرنامج يعمل معالجة آلية للبيانات"²، كما عرفه قانون اليونسترال النموذجي بشأن التجارة الإلكترونية لسنة 1996³، بموجب المادة 9/و ومن خلال تحديد المصطلحات أنه "النظام الذي يستخدم لإنشاء رسائل البيانات أو إرسالها أو استلامها أو تخزينها لتجهيزها على أي وجه آخر".

¹ _علي عبد القادر القهوجي، الحماية الجنائية لبرامج الكمبيوتر، المكتبة القانونية، القاهرة، ط1، 1999، ص 119-120.
² _Art1 Dé finition 2- a- « système informatique désigne Tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données. » convention européenne de la cybercriminalité, op, cit, p3.

³ _قرار لجنة الأمم المتحدة للقانون التجاري الدولي رقم 162/51، معتمد من قبل جمعيتها العامة بناء على تقرير اللجنة السادسة [A51/62/628] بتاريخ 1996/02/16، ويشار إليه بقانون اليونسترال النموذجي بشأن التجارة الإلكترونية.

وعرفته الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بأنه "مجموعة برامج وأدوات معدة لمعالجة وإدارة البيانات والمعلومات".¹

وقد أعطى الفقه الفرنسي تعريفا للنظام المعلوماتي بأنه "كل مركب يتكون من وحدة أو مجموعة وحدات معالجة والتي تتكون كل منها من الذاكرة والبرامج والمعطيات وأجهزة الادخال والايخراج وأجهزة الربط، والتي يربط بينها مجموعة من العلاقات التي عن طريقها تحقق نتيجة معينة وهي معالجة المعطيات على أن يكون هذا المركب خاضعا لنظام الحماية الفنية"²، وبعبكس المشرع الفرنسي الذي لم يعط تعريفا لنظام المعالجة الآلية للمعطيات.

وبالرجوع إلى المشرع الجزائري، نجده تبني نفس التعريف الذي جاءت به اتفاقية بودابست السالفة الذكر، مستخدما في ذلك مصطلحين مترادفين هما " نظام المعالجة الآلية للمعطيات ومصطلح "منظومة معلوماتية"، حيث عرفت المادة 2/ب من القانون رقم 04/09 المؤرخ في 05/08/2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، المنظومة المعلوماتية على أنها "أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين".³

لقد وفق المشرع الجزائري في تعريفه لنظام المعالجة الآلية حيث اشترط ضرورة الترابط بين مكونات وأجهزة النظام وبين الأنظمة فيما بينها كما نجد أنه ركز على وظيفة النظام ووسع من ذلك ليشمل كل من المعالجة الآلية والمعالجة المعلوماتية للمعطيات.

¹ - الإتفاقية العربية لمكافحة جرائم تقنية المعلومات وافق عليها مجلسا وزراء الداخلي والعرب في اجتماعهما المنعقد بمقر الأمانة العامة لجامعة الدول العربية بتاريخ 2021/12/21.

² Le sénat désirait Définir un stad comme « Tout ensemble composé d'une ou plusieurs unités de traitement automatisées, de mémoires, des logiciels de données, d'organe d'entrées, sorties et de liaison qui conçurent a un résultat déterminé, cet ensemble qui conçurent à un résultat déterminé, cet étant protégé par un dispositifs de sécurité. Rap j Thyrand Doc-Sénat 1987, 88n°3, p53.

³ _عرف المشرع السعودي النظام المعلوماتي من خلال المادة 1 من النظام مكافحة جرائم المعلوماتية بقوله: "النظام المعلوماتي عبارة عن "مجموعة برامج وأدوات معدة لمعالجة البيانات وإدارتها وتشمل الحاسبات الآلية". أما قانون رقم 02 لسنة 2006 المتعلق بمكافحة جرائم نظم المعلومات عرف النظام المعلوماتي على أنه «مجموعة برامج وأدوات معدة لمعالجة وإدارة البيانات والمعلومات أو الرسائل الإلكترونية وغير ذلك» فيما عرفه قانون المعاملات الأردني رقم 85 لسنة 2001 بموجب المادة 6/2 بأنه «نظام الكتروني لإنشاء أو استخراج أو إرسال أو استلام أو تخزين أو عرض أو معالجة المعلومات أو الرسائل إلكترونيا».

وعليه وبناء على التعاريف السابقة نخلص إلى أن تعريف نظام المعالجة الآلية للمعطيات يعتمد على عنصرين.¹

-العنصر الأول: مركب يتكون من عناصر مادية ومعنوية مختلفة تربط بينهما نتيجة علاقات توحيدها نحو تحقيق هدف محدد.

-العنصر الثاني: ضرورة خضوع النظام لحماية فنية حتى يتمتع بالحماية القانونية الجنائية.

ثانيا: ضرورة خضوع النظام للحماية الفنية

يقصد بمصطلح الحماية الفنية للنظام، هو ذلك الإجراء الوقائي الذي يتخذه صاحب النظام أو صانع البرنامج أثناء وضعه له للحد من الإعتداءات الخارجية التي تقع عليه²، ولقد أثار مجلس الشيوخ الفرنسي في تعريفه لمفهوم النظام المعلوماتي شرطا متمثلا بالحماية الفنية للنظام، مما أدى هذا الوضع إلى خلق تساؤل في الوسط القانوني، هل الأنظمة المحمية بأجهزة أمان هي التي تحظى بحماية جنائية، أم أن كل الأنظمة تحظى بتلك الحماية؟ وللإجابة على هذا التساؤل اختلف الفقه، خاصة الفقه الفرنسي بين موسع للحماية لتشمل كل الأنظمة، وبين من يحصرها في تلك المحمية بأجهزة أمان فقط، علما أن أنظمة المعالجة تقسم إلى ثلاثة أنواع: أنظمة مفتوحة للجمهور، وأنظمة قاصرة على أصحاب الحق فيها ولكن بدون حماية فنية، وأنظمة قاصرة على أصحاب الحق فيها وتتمتع بحماية فنية.³

-الإلتجاه المؤيد

يرى أصحاب هذا الإلتجاه ضرورة وجود نظام أمني، على إعتبار أن القانون يجرم الإعتداء على نظم الأمن المتضمنة في النظام المعلوماتي، ويستند هؤلاء إلى عدد من الحجج، منها أن الإعتداء على النظام الأمني شرط مفترض لقيام الجرائم التي تتعلق بالمعلوماتية، كما تبين في الأعمال التحضيرية لمناقشة القانون⁴، كما يضيف أنصار هذا الإلتجاه أن هذا الشرط تقتضيه كذلك متطلبات العدالة والمنطق، حيث

¹ _أمال قارة، المرجع السابق، ص 102.

² _مسعود خثير، المرجع السابق، ص 111.

³ _غنية باطلي، المرجع السابق، ص 140.

⁴ _فبالرجوع إلى الأعمال التحضيرية للقانون (19) حول الغش المعلوماتي، يلاحظ أن بعض أعضاء البرلمان يتطلبون ذلك ويصرّون عليه لأن الحماية الجزائية في نظرهم يجب أن تقتصر على الأنظمة المحمية قنياً أنظر علي عبد القادر القهوجي، المرجع السابق، ص 123.

أن القانون الجزائي لا ينبغي أن يقوم بحماية الأشخاص الذين لا يأخذون الاحتياطات اللازمة المتطلب من الإنسان العادي، فوجود نظام الحماية الفنية يمكن إعتبره إلتزاماً مفروضاً، بنص القانون على كل من يقوم بإدارة نظام المعالجة الآلية.¹

-الاتجاه المعارض للحماية الفنية

وهو الرأي الغالب في الفقه الفرنسي، والمؤيد يرى أن هذا الشرط ليس ضرورياً، وذلك أن هذا الشرط وجوده لا يكون له سوى دور واحد، هو إثبات سوء نية من قام بانتهاك النظام والدخول إليه بطريقة غير مشروعة ويدخل في عبء إثبات القصد الجنائي، كما أضاف أصحاب هذا الإتجاه أن الأعمال التحضيرية لقانون الغش المعلوماتي في فرنسا لسنة 1988، تعرض لهذا الشرط ولكن المشرع الفرنسي لم ينص عليه في نص القانون، وهذا يفسر بأن الإرادة اتجهت إلى رفض تطلب هذا الشرط من طرف البرلمان مما لا يدع مجالاً للشك، وأن الأعمال التحضيرية لا قوة إلزامية لها، ودورها يقتصر على تفسير النصوص الغامضة أو المتعارضة.²

ونستنتج من ذلك، أنه لا يشترط لوجود الجريمة أن يكون الدخول إلى النظام مقيداً بوجود حماية فنية، ذلك أن الواقع يكشف أن غالبية الأنظمة المعالجة الآلية للمعطيات تتمتع بنظام حماية فنية، بل نجد هناك شركات متخصصة في تقديم خدمات التأمين، كما أكد القضاء الفرنسي في عدة أحكام له عدم الأخذ بهذا الشرط، وذلك من خلال الحكم الصادر من محكمة إستئناف باريس في 5 أبريل 1994، حيث جاء في حيثياته أنه " من غير الضروري لقيام جريمة الدخول غير المصرح به أن يكون فعل الدخول قد تم بمخالفة التدابير الأمنية، وأنه يكفي أن يكون هذا الدخول غير المصرح به أن يكون فعل الدخول قد تم بمخالفة التدابير الأمنية، وأنه يكفي أن يكون هذا الدخول قد تم ضد إرادة المسؤول عن النظام.³

¹ _رشيدة بوكري، المرجع السابق، ص 167.

² _محمد خليفة، جريمة التواجد غير المشروع في الأنظمة المعلوماتية، المرجع السابق، ص 143.

³ _Dans une décision du 5avril 1994, la cour d'appel de paris a précisé que « pour être punissable, cet accès ou ce maintien doit être fait sans droit et en pleine connaissance décause, étant précisé à cet égard qu'il n'est pas nécessaire pour l'infraction existe que l'accès soit limité par un dispositif de protection..... ».

C.A de paris, 5 avril 1994, disponible eu ligne a l'adresse suivant, <http://Documents and settings use /desktop/les atteintes aux systèmes informatises de données e juristes-org.nert.un>.

مايمكن قوله في الأخير أن سكوت القانون على هذا الشرط، سواء بالنسبة للمشرع الفرنسي أو المشرع الجزائري فقد تبنى الإتجاه الرافض لإضفاء الحماية الفنية على النظام المعلوماتي، لتمتد الحماية وتشمل كل أنظمة المعالجة الآلية للمعطيات¹، لذلك فلا يمكن إعتباره عنصرا في هذه الجرائم، إذ لا تفرض هذه الجرائم، سوى وجود نظام معلوماتي كشرط أولى وعندها يمكن البحث في قيام أركانها أو عدمها.

الفقرة الثانية: صور جريمة الدخول أو البقاء غير المصرح به

تعتبر هذه الجريمة من أهم الجرائم الإلكترونية عموما، وذلك أن أغلب الجرائم لا يمكن إرتكابها إلا بعد الدخول إلى النظام المعلوماتي، لهذا كانت جريمة الدخول هي الباب والحد الفاصل بين الجاني وبين إرتكابه لمختلف الجرائم الإلكترونية الأخرى²، وسوف نتعرض فيما يلي لأركان هذه الجريمة.

أولا: جريمة الدخول أو البقاء غير المشروع في صورتها البسيطة

نص المشرع الجزائري على هذه الصورة بموجب المادة 394 مكرر من ق. ع. ج والتي جاء نصها كما يلي: " يعاقب بالحبس من ثلاث (3) أشهر إلى سنة، وبغرامة من 50000 دج إلى 200.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.

وتضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة."

وتقابلها المادة 1/323 من قانون العقوبات الفرنسي³، كما نصت عليها المادة 02 من الإتفاقية

¹ -تتعدد أنواع الأنظمة المعلوماتية، فلا تنحصر سوى في نظام الحاسوب بل كل نظام أو جهاز يقوم بالمعالجة الآلية للمعطيات كشبكة الأنترنت، البريد الإلكتروني، البطاقة الإلكترونية كبطاقة الائتمان البنكية، موزع النقود بالإضافة إلى مصالح الخدمات التقنية للدخول إلى شبكة الأنترنت، أو تثبيت صفحات أو مواقع انترنت في شبكة الأنترنت... إلخ للمزيد أنظر دررور نسيم، جرائم المعلوماتية على ضوء القانون الجزائري والمقارن، مذكرة لنيل شهادة الماجستير في الحقوق، كلية الحقوق والعلوم السياسية، جامعة قسنطينة، 2012-2013، ص، ص22-23.

² -محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، المرجع السابق، ص 131.

³ Art 323-1 du c.p.f dispose que « le fait d'accéder ou de se maintenir, frauduleusement dans Tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et 30000euras d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système la peine est de trois d'emprisonnement et de 45000euras d'amende. Voir Myriam qu'emmenner, Yves charpenel op. cit, p73.

الدولية للإجرام المعلوماتي، وجاءت تحت عنوان "الدخول غير القانوني" "Accès illégal"¹، كما جرمّت هذه الجريمة أيضا المادة 06 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات.²

إنطلاقا من النصوص القانونية السابقة الذكر، فإن هذه الصورة من الجرائم تتكون من ركن مادي وركن معنوي، وعقوبة مقررة لها.

1-الركن المادي: باستقراء نص المادة 394 مكرر من ق.ع.ج، فإن الركن المادي لهذه الجريمة يتمثل في نشاط إجرامي، وهو الدخول المنطقي أو الاتصال بطريق الغش مع نظام معلوماتي بغرض إختراقه كله أو جزء منه أو قد يتمثل في البقاء في النظام المعلوماتي دون وجه حق وسوف نتناول السلوك الإجرامي لهذه الجريمة في كلتا صورتين.

أ-فعل الدخول: ويعد فعل الدخول³، السلوك الأساسي لقيام هذه الجريمة، وبقية الجرائم الأخرى التي تتجر عنها هذا الفعل، فمن خلال المادة 94 مكرر ق.ع.ج فلا يقصد بالدخول إلى نظام معلوماتي التواجد المادي للمخترق، لأن هذا لا يمكن تصوره بشأن الدخول إلى نظام المعالجة الآلية بالطريقة ذاتها بإعتبار هذا النظام ظاهرة غير مادية⁴، وإنما يقصد بالدخول هو التواجد المعنوي أو المنطقي في نظام المعالجة الآلية، وهذا ما جعل المشرع الفرنسي يستعمل مصطلح Accéder بدلا من عبارة entrée، ونفس الأمر بالنسبة لإتفاقية بودابست، ونجد هذا المصطلح هو الأكثر ملائمة في هذا المجال، ولقد

(1) Art 2 du c.c.c dispose que « chaque partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément a son droit interne l'accès intention et sans droit à tout ou partie d'un système informatique. Une partie peut exiger que l'infraction soit commise en violation des mesures de sécurité, dans l'intention d'obtenir des données informatique ou dans une autre intention délictueuse, ou soit en relation avec un système informatique connecte a un autre système information, convention Budapest.

² تنص المادة 6 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات على أنه: «جريمة الدخول غير المشروع:

1-الدخول أو البقاء وكل اتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار به.

2-تشدد العقوبة إذا ترتب على هذا الدخول أو البقاء أو الاتصال أو الاستمرار بهذا الاتصال.

أ-محو أو تعديل أو تشويه أو نسخ أو نقل أو تدمير للبيانات المحفوظة والأجهزة والأنظمة الإلكترونية وشبكات الاتصال وإلحاق الضرر بالمستخدمة والمستفيدين.

ب-الحصول على معلومات حكومية.

³ ونلاحظ أن المشرع التونسي استعمل عبارة النفاذ عوضا عن مصطلح الدخول ليؤكد خاصية اللا مادية لهذه الجريمة.

⁴ نهلا عبد القادر المومني، المرجع السابق، ص 158.

اختلفت آراء الفقهاء في تعريف الدخول، أو المقصود من عبارة الدخول فهناك من عرفه بأنه "الولوج إلى المعلومات والمعطيات المخزنة داخل نظام الحاسب الآلي، بدون رضا المسؤول عن هذا النظام"¹، أو هو "عملية دخول غير مصرح به إلى أجهزة الغير وشبكاتهم الإلكترونية بواسطة برامج متطورة يستخدمها كل من يملك خبرة في استعمالها."²، أو أنه "إساءة استخدام الحاسب الآلي ونظامه عن طريق شخص غير مرخص له بإستخدامه والدخول إليه للوصول إلى المعطيات المخزنة بداخله للاطلاع عليها، أو لمجرد التسلية أو إشباع الشعور بالنجاح في إختراق الحاسب الآلي."³

ونلاحظ من التعاريف السابقة المتعلقة بالدخول، أنها متشابهة في تحديد معنى الدخول، كما أن هذه التعاريف حاولت ربط مصطلح الدخول بعدم التصريح، في حين هناك من يحصر الدخول إلى النظام إلى وجود ثغرات فنية، نتيجة لوجود خلل في خدمة الأمن، وهو المنفذ الذي يشغله المخترقون للولوج إلى الأنظمة المعلوماتية وتحقيق أهدافهم⁴، غير أن التكنولوجيا أثبتت أن هناك وسائل تقنية يمكن من خلالها تحقق الوصول إلى النظام حتى ولو توفر على حماية فنية منها معرفة رقم TP address الخاص بالجهاز كذلك استعمال حصان طروادة، التفتيش في مخلفات التقنية.

وبالرجوع إلى نص المادة 394 مكرر ق.ع.ج، يتبين أن المشرع الجزائري لم يحدد الطريقة التي يتم بها الدخول، وعليه فإن الجريمة تتحقق بأي وسيلة⁵، فقد يكون عن طريق برنامج فيروسي أو عن طريق

¹ Bainbridge David, Hacking the unauthorised access of computer system, the legal implication –ml Rev 1989, Vol 52, p237.

² _خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، المرجع السابق، ص 84.

³ _نايلة عادل محمد فريد قورة، المرجع السابق، ص 326.

⁴ _رشيد بوكري، المرجع السابق، ص 180.

⁵ _ من أكثر التقنيات استعمالا لتحقيق الدخول إلى النظام:

-استخدام البرامج المصممة أصلا لإختراق أنظمة الحماية.

-الفخ (la trappe) وهو عبارة عن منفذ يجهز به النظام مسبقا من قبل مصمم النظام ليسمح له لاحقا بإنزال برامج تعيق سير عمله.

-التخفي (déguisement) ويعني انتحال صفة من له الحق في الدخول إلى النظام ثم الحصول على امتيازاته في الاطلاع على المعلومات.

- القناة المخفية (canal cache) وهو من أخطر الاعتداءات ويتطلب ذكاء فائقا من المعتدي لاخترق سياسة الأمن والحماية المعتمدة في الأنظمة المعلوماتية لتهريب المعلومات.

-التسلل (faufillement) ومعناه التسلل وراء مستعمل مرخص له بالدخول إلى نظام معلوماتي وتخطي حاجز الدخول:

إستعمال الرقم السري لشخص آخر أو الدخول من خلال شخص مسموح له بالدخول¹، وذلك أن المشرع أدرك أن التكنولوجيا في تطور مستمر، ولا يمكن حصر فعل الإختراق في وسيلة معينة، كما أن هذه الجريمة، تقع من أي إنسان أيا كانت صفته، أي أنها ليست من جرائم ذوي الصفة، وإنما يرتكبها أي شخص سواء كان يعمل في مجال الأنظمة أم لا، إنما يشترط ألا يكون من أولئك الذين لهم حق الدخول إلى هذا النظام.

إن الدخول إلى النظام المعلوماتي لا يشكل سلوكا غير مشروع، إلا إذا كان هذا السلوك بدون وجه حق أو بدون تصريح ممن يملك الحق أو كان المسؤول عن النظام، بالتالي عدم مشروعية الدخول إلى النظام مرتبط بالمسؤول عنه ومعرفة من له الحق بإعطاء التصريح، لذلك إن تحديد الشخص أو الهيئة التي تصرح بالدخول أمر بالغ الأهمية، إذ تتوقف الجريمة على إرادة ذلك الشخص أو تلك الهيئة، لأنهما يملكان السيطرة على النظام وبملكان التصرف في تنظيمه والتصريح بالدخول إليه أو عدم التصريح بذلك².

ويسمى الفقه الفرنسي هذا الشخص بصاحب السلطة على النظام³، le maître du system أما عن حالات التصريح بالدخول تتحقق في الحالة، التي لا يملك الشخص أي تصريح أو رخصة من المسؤول عن النظام وليس له علاقة بالنظام بتاتا وذلك لعدم كونه من العاملين لدى الجهة التي يتبعها النظام، أما الحالة الثانية تتمثل في تجاوز التصريح بالدخول إلى النظام، ففي هذه الحالة أن يكون هناك تصريح جزئي والمصرح له يتجاوز هذه الحدود⁴.

نظر رامي حليم، جرائم الاعتداء على أنظمة المعالجة الآلية للمعلومات، مجلة دراسات وأبحاث، كلية الحقوق والعلوم السياسية، جامعة زياني عاشور، الجلفة، الجزائر، العدد 1، 2009م، ص 343 وأيضا: Myriam Quémèner, Joël ferry, op.cit. , p75.

¹ _ علي عبد القادر القهوجي، المرجع السابق، ص 121.

² _ محمد خليفة، الحماية الجنائية لبرامج الحاسب الآلي، المرجع السابق، ص 145.

³ _ عرفته المادة 2 من الإتفاقية الخاصة بحماية الأفراد في مواجهة النظم المعالجة الآلية للمعلومات ذات الطابع الشخصي والتي تبناها المجلس الأوروبي في 28 يناير 1989 بأنه " كل شخص طبيعي أو معنوي أو كل سلطة عامة، أو كل مؤسسة أو جهاز يكون لهم سلطة التصرف في نظام الحاسب الآلي التابع لهم وتقرير مضمونه أو محتواه، وكيفية تنظيمه والهدف منه" أنظر نائلة عادل محمد فريد قورة، المرجع السابق، ص 346.

⁴ _ رشيدة بوكري، المرجع السابق، ص 194.

وبناء على ما سبق ذكره، فإن دخول أي شخص إلى نظام المعالجة الآلية للمعطيات من دون تصريح أي صدف لا يكفي على أنه جريمة لكن بشرط أن يقطع تواجده من النظام فوراً.¹

ب- فعل البقاء غير المصرح به

يعتبر فعل البقاء غير المصرح به الصورة الثانية للسلوك الإجرامي، تناوله المشرع في نص المادة 394 مكرر ق.ع.ج، واعتبره سلوكاً مجرمًا إلى جانب فعل الدخول بقوله: "...أو بقي..." وبقابله النص الفرنسي بموجب المادة 1/323 من ق.ع.ف الذي جاء نصه "ou de maintenir"....².

لم يتطرق المشرع الجزائري شأنه شأن المشرع الفرنسي، وأغلب التشريعات المقارنة إلى تحديد المقصود "بفعل البقاء"، غير أن الفقه تصدى إلى هذه المهمة، وقد تعددت التعريفات التي قيلت بشأنها ومن أهمها يعرف بأنه "مشاركة ذات سيطرة من المخترق على تفاعل الحاسوب مع حركة الدخول والخروج"³، أو أنه " فعل الاتصال بعد أن توافر للشخص العلم بكونه نظاماً ممنوعاً عليه الدخول واتجاه إرادته إلى الإبقاء على هذا الاتصال الذي حدث بطريق الخطأ".⁴

والهدف من تجريم البقاء غير المصرح به داخل نظام المعالجة الآلية للمعطيات، أن الجاني دخل بإرادته للنظام، إلا أنه إمتنع عن الخروج منه بعد علمه بعدم مشروعية سلوكه،⁵ ومما سبق يتضح أن سلوك الجاني في هذه الجريمة هو سلوك سلبي إذ رغم علمه بعدم أحقيته، إلا أنه يعتمد البقاء في النظام كله أو في جزء منه ويرفض الخروج منه، وفقاً لهذا الرأي يعد من صور فعل البقاء المعاقب عليه أن يظل الجاني باقياً داخل النظام بعد المدة المحددة له بالبقاء داخله، أو كمن يقوم بطبع نسخة من المعلومات في الوقت الذي كان مسموحاً له فيه الرؤية والإطلاع فقط، ويتحقق ذلك أيضاً بالنسبة للخدمات المفتوحة للجمهور.⁶

¹ مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، القاهرة، دط، 2001، ص 52.

² لم تنص اتفاقية بودابست على فعل البقاء غير المصرح به في نظام المعالجة الآلية وتركت تجريم ذلك إلى التشريعات الوطنية فميا تراه مناسباً من الأفعال.

³ عمر محمد أبوبكر بن يونس، المرجع السابق، ص 332.

⁴ أيمن عبد الله فكري، المرجع السابق، ص 238.

⁵ رشيدة بوكر، المرجع السابق، ص 196.

⁶ عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، دار الفكر الجامعي، الاسكندرية، دط، 2004، ص 31.

كما يتحقق البقاء المعاقب عليه داخل النظام، مستقلاً عن الدخول إلى النظام مشروعاً ومن أمثلة ذلك إذا تحقق الدخول إلى النظام بالصدفة، أو عن طريق الخطأ أو السهو، إذ يجب على الشخص في هذه الحالة أن ينسحب فوراً، فإذا بقي رغم ذلك فإنه يعاقب على جريمة البقاء غير المصرح به إذا توافر الركن المعنوي.¹

كما قد يجتمع فعل الدخول غير المصرح به إلى النظام الآلي لمعالجة المعطيات، مع فعل البقاء غير المصرح به داخله معاً، يتحقق ذلك في حالة ما إذا لم يكن للجاني الحق في الدخول إلى النظام، بالرغم من ذلك يدخل إليه فعلاً، ضد إرادة صاحبه أو من له حق السيطرة، ثم يبقى داخل هذا النظام بعد ذلك.²

ومن الإشكاليات التي تثيرها هذه الحالة الأخيرة، هي المدة الزمنية أي متى تنتهي جريمة الدخول إلى النظام ومتى تبدأ جريمة البقاء؟ اختلف الفقه للإجابة على هذه الإشكالية، فذهب رأي من الفقه للقول أن جريمة الدخول تتحقق منذ اللحظة التي يتم فيها الدخول فعلاً إلى البرنامج، ويبقى مدة قصيرة من الزمن داخله، وبعد تلك اللحظة تبدأ جريمة البقاء وتنتهي بإنهاء حالة البقاء.

كما يذهب رأي آخر إلى تحديد اللحظة منذ الوقت الذي يعلم فيه أن بقاءه داخل النظام غير مشروع، أما الرأي الراجح يرى أن جريمة البقاء داخل النظام المعلوماتي بكامله أو جزء منه، تبدأ من اللحظة التي يقوم فيها الجاني بالتجول داخل النظام، أو يستمر في التجول داخله بعد إنتهاء الوقت المصرح به بالبقاء فيه.³

إن الحكمة من تجريم الدخول والبقاء غير المصرح به، هو حماية نظام المعالجة الآلية للمعطيات بصورة مباشرة، كما أنها تحقق حماية المعطيات بصورة غير مباشرة من الوصول إليها، من طرف أشخاص غير مصرح لهم الدخول إلى هذا النظام، لا تتحقق في هذه الحالة، فالدخول في الحالتين تتم بموافقة المسؤول عن هذا النظام، مما يعني له السماح بالإطلاع على تلك المعلومات التي يحتويها النظام لهذا البقاء، هنا لا تعتبر غير مشروع ولكن يمكن اعتباره سرقة وقت الحاسب الآلي.⁴

¹ - آمال قارة، المرجع السابق، ص 110.

² - علي عبد القادر القهوجي، المرجع السابق، ص 133.

³ - ناصر حمودي، الحماية الجنائية لنظم المعالجة الآلية للمعطيات في التشريع الجزائري، المجلة الأكاديمية للبحث القانوني، المجلد 7، العدد 2، 2016، ص 75.

⁴ - حسين بن سعيد الغافري، المرجع السابق، ص 3355.

2-الركن المعنوي

تنص المادة 394 مكرر من ق.ع.ج صراحة على وجوب كون جريمة الدخول أو البقاء غير المصرح به جريمة عمدية، ويستشف ذلك من قولها " كل من يدخل أو يبقى عن طريق الغش..."، ونفس المعنى أشارت إليه المادة 01/323 من ق.ع.ف بقولها "fraude leusement"

ويتخذ الركن المعنوي صورة القصد الجنائي، أي توافر القصد العام بعنصريه العلم والإرادة، فيكفي لتوافر هاته الجريمة، أن يعلم الجاني أنه قد دخل إلى نظام ليس له حق الدخول فيه، أو تعتمد البقاء فيه رغم إنتهاء مدة حقه في البقاء فيه، ولو كان الدخول مشروعاً.

إضافة إلى وجوب توافر العلم، لابد من وجود إرادة وإتجاهها إلى ارتكاب فعل الدخول أو فعل البقاء في النظام المعلوماتي، دون أن تتجه إلى إحداث النتيجة الجرمية، لأنها تعتبر من الجرائم الشكلية سواء في القانون الجزائري والفرنسي.

فإذا توافر القصد الجنائي بعنصرية العلم والإرادة، فإنه لا يتأثر بالباعث على الدخول أو البقاء، فيظل القصد الجرمي قائماً، ولو كان الباعث من الدخول الفضول أو التنزه، أو مجرد محاولة قهر النظام أو التفوق على الوسائل التقنية.¹

لقد ثار خلاف فقهي حول مدى ضرورة توافر القصد الجنائي الخاص في جريمة الدخول أو البقاء غير المصرح بهما، فهناك جانب من الفقه الفرنسي ذهب الى إشتراط توافر القصد الجنائي الخاص لهذه الجريمة، وذلك من خلال لفظ عبارة "الغش"، والذي يختلف عن لفظ عمدا وإرادي، ويتفق الفقه هنا أن الغش هنا ليس المقصود به نية الإضرار، وإلا ترتب على ذلك تناقض كبير في الركن المادي الذي لا يتطلب النتيجة والركن المعنوي.²

ويرى جانب من الفقه أن الدخول أو البقاء غير المصرح بهما يتحققان عندما يكونان بدون رضا صاحب النظام، ويستندون في ذلك إلى ما قضت به محكمة باريس في قرارها الصادر بتاريخ 5 أفريل 1994 المتعلق بالدخول أو البقاء غير المصرح بما في نظم المعالجة الآلية، والتي قضت بأن الدخول أو

¹ _علي عبد القادر القهوجي، المرجع السابق، ص 137.

² _غنية باطلي، المرجع السابق، ص 167.

البقاء يكون بدون وجه حق مع معرفة السبب.¹

3- عقوبة الدخول أو البقاء غير المشروع في صورتها البسيطة

يعاقب المشرع الجزائري على هذه الجريمة بالحبس من ثلاثة أشهر إلى سنة وبغرامة مالية من 50.000 دج إلى 100.000، وترك المشرع للقاضي السلطة التقديرية بأن جعل له حدا أدنى وحد أقصى في تقدير العقوبة بحسب الوقائع المعروضة أمامه.

ثانيا: جريمة الدخول والبقاء في صورتها المشددة

أسلفنا القول أن المشرع الجزائري يكتفي لقيام جريمة الدخول أو البقاء غير المصرح بهما دون اشتراط نتيجة معينة، بإعتبارها من الجرائم الشكلية، لكن إذا ترتب عن هذا الدخول أو البقاء نتائج ضارة بالنظام المعلوماتي أو المعلومات، فإن المشرع لجأ إلى تشديد العقوبة وذلك وفقا لما أشارت إليه المادة 394 مكرر فقرة الثانية والثالثة من ق.ع.ج بقولها "تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة"، وكذا الفقرة الثالثة تنص على أنه "وإذا ترتب على الأفعال المذكورة أعلاه تخريب بنظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر (6) غلى سنتين (2) والغرامة من 50.000 دج إلى 150.000 دج".

ونستنتج من هذه الفقرات أن ليست كل النتائج محل اعتبار من المشرع بل هناك نتائج ثلاثة فقط يترتب عليها الأثر القانوني، وهي حذف أو تغيير معطيات نظام المعالجة الآلية للمعطيات، أو تخريب هذا النظام.²

1- الركن المادي

يتحقق النشاط الإجرامي بإحدى الأفعال المحددة في المادة السالفة الذكر، المتمثلة في فعل الحذف ويعني إزالة المعلومات الموجودة داخل نظام المعالجة الآلية للمعطيات، وهو أقصى أنواع الضرر مما دعا المشرع إلى تشديد العقاب.³

¹_qui ont accédé et se maintenus dans des systèmes sans droit et en pleine connaissance de cause..238 مشاركة إليه لدى رشيدة بوكري، المرجع السابق، ص 238.

²_محمد خليفة، جريمة التواجد غير المشروع الأنظمة المعلوماتية، المرجع السابق، ص 169.

³_رشيدة بوكري، المرجع السابق، ص 231.

أما مصطلح التغيير، فيشير إلى إحداث تعديلات فحسب في المعلومات دون أن يصل الأمر إلى حد إزالتها، بحيث تظل المعلومة موجودة ولكن بدون معنى أو فائدة، أو أن تكون لها معنى يخالف المعنى الأصلي الذي كانت عليه قبل هذا الفعل، ويقصد بتخريب النظام عدم صلاحية النظام للقيام بوظائفه، والقول بوجود هذا الظرف المشدد، لا بد من توافر علاقة سببية بينه فعل الدخول أو البقاء غير المصرح بهما وبين النتيجة التي تحققت¹، وهي محو النظام، أو عدم قدرته على أداء وظيفته، أو تعديل البيانات، ومما تجدر الإشارة إليه أن المشرع الجزائري خص بالذكر هذه النتائج الثلاثة لأنها تعد من أخطر الأفعال جسامة وإضراراً بالنظام المعلوماتي.

2-الركن المعنوي

إن الأثر المترتب على جريمة الدخول أو البقاء غير المصرح به والذي يعتبر ظرفاً مشدداً هو نتيجة غير عمدية، وهي نتيجة لإرادية حيث لم تتجه نية الفاعل إلى الإضرار بالمعطيات أو بالنظام²، فنجد المشرع الجزائري في نص المادة 394 مكرر 1 من ق.ع.ج قد استعمل عبارة "الغش" فقط مع فعل الإدخال، معتبراً أن الإدخال لا يمكن أن يكون إلا أن يقع عمداً، عكس الحذف والتغيير اللذين لا يمكن أن يقعاً إلا عن طريق الخطأ، وبالتالي فهذه الجريمة من جرائم الإهمال، مجرد إرتكاب الفعل المادي يعد كافياً لقيام الجريمة، إلا إذا استطاع الجاني إثبات وجود قوة قاهرة أدت إلى وقوعها، فإذا قصد الجاني تحقيق النتيجة المشددة، فتدخل ضمن جريمة التلاعب بالمعطيات ويطبق عليها نص المادة 394 مكرر 1 من ق.ع.ج وليس نص المادة 394 مكرر، أما بالنسبة للظرف المشدد المتعلق بتخريب النظام الوارد في نص الفقرة الثالثة من نص المادة 394 مكرر ق.ع.ج، فإذا كانت مقصودة فنكون أمام جريمة إفساد أو إعاقاة النظام المنصوص عليها في قانون العقوبات الفرنسي (المادة 2/323 ق.ع.ف)³، وليس لها ما يقابلها في قانون العقوبات الجزائري، ولكي يعاقب على الظرف المشدد لا بد أن تحدث النتيجة بعد دخول أو بقاء غير مصرح بهما، إذ لا يعاقب على هذه النتيجة إذا كان الدخول أو البقاء مصرح بهما.

¹ -أيمن عبد الله فكري، المرجع السابق، ص 208.

² -غنية باطللي، المرجع السابق، ص 170.

³ -ناصر حمودي، المرجع السابق، ص 78.

3-العقوبة المقررة

تنص المادة 394 مكرر في فقرتها الثانية من قانون العقوبات الجزائري، تضاعف العقوبة إذا ترتب عن هذه الأفعال حذف أو تغيير لمعطيات المنظومة.

أما في الفقرة الثالثة من ذات المادة السابقة الذكر تكون العقوبة الحبس من ستة أشهر الى سنتين وغرامة مالية من 50000 دج إلى 150000 دج، وإذا ترتب عن الدخول أو البقاء غير المشروع تخزين لنظام اشتغال المنظومة.

الفرع الثاني: جريمة التلاعب غير المصرح به بمعلومات نظام المعالجة الآلية

بعد أن جرم المشرع الجزائري فعلي البقاء والدخول بطريق الغش لنظم المعالجة الآلية للمعطيات، قام بتجريم فعل التلاعب غير المصرح به بالمعلومات التي تتضمنها نظم المعالجة الآلية، وهي جريمة مستقلة تضمنتها المادة 394 مكرر 1 من ق.ع.ج والتي نصت على «يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 500000 دج إلى 2.000.000 كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها» وتقابلها المادة 3/323 من قانون العقوبات الفرنسي¹، ونجد أيضا إتفاقية بودابست بشأن الجرائم الإلكترونية نصت هي الأخرى على هذه الجريمة، وذلك بموجب المادة 4 منها تحت عنوان "الإعتداء على سلامة المعلومات".

إذن يستفاد من خلال النصوص السابقة الذكر، أن جريمة التلاعب غير المصرح به بالمعلومات تقوم على أركان محددة، فلا بد من توافر الركن المادي المتمثل في فعل الإدخال، أو التعديل أو الإزالة، وركن معنوي يتمثل في القصد الجنائي، وعقوبة مقررة لها.²

¹_Art 323/3-1 du C.P.f Dispose que »le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75000 euros d'amende.

²_Art du c.c.c dispose que :

1-chaque partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément a son droit interne, le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques.

2-une partie peut se réserver le droit d'exiger que le comportement décrit au para graphe 1entraîne des dommages sérieux convention Budapest, op, cit.

أولاً: الركن المادي

يتحقق النشاط الإجرامي لهذه الجريمة، أن يتم بإحدى الصور التي حددتها المادة السالفة الذكر وهي صورة الإدخال أو التعديل أو المحو، ولا يشترط إجتماعهما معا لتوافر النشاط الإجرامي، يعني يكفي لتحقيق هذا النشاط قيام الجاني بإحدى هاته الأفعال.

1- فعل الإدخال

يقصد بفعل الإدخال بأنه "تغذية النظام بالمعلومات المراد معالجتها، أو بتعليمات لازمة لعملية المعالجة"¹، أو أنه "إضافة خصائص ممغنطة جديدة في الدعامة الموجودة سواء كانت فارغة غير مشغولة، أو كانت تحتوي على خصائص ممغنطة قبل هذا الإدخال."²

ويقصد بذلك إدخال بيانات في نظام المعالجة لم تكن موجودة من قبل، وقد يتم إدخال هذه البيانات بقصد التشويش على صحة البيانات القائمة، ولعل إصطناع المعلومات هو الأكثر سهولة في التنفيذ ولاسيما في المنشآت ذات الأموال، حيث يعد المسؤول في القسم المعلوماتي في أفضل وضع يؤهله لإرتكاب هذا النمط غير المشروع من التلاعب³، ومن صور إدخال المعلومات المصطنعة "اختلاس النقود عن طريق الغش المعلوماتي، ويتحقق كذلك فعل الإدخال في القرص الذي يتمكن فيه الحامل الشرعي لبطاقة السحب الممغنطة والتي تسحب النقود من البنوك تحديدا أجهزة السحب الآلي، وذلك حين يستخدم رقمه الخاص السري للدخول كي يسحب مبلغا أكثر من ذلك المبلغ المسموح به لصاحب البطاقة، أو في حالة إدخال فيروس «حصان طروادة أو قنبلة منطقية تؤدي إلى إضافة معطيات جديدة»⁴.

وقد تعرض القضاء الفرنسي لهذه الجريمة في العديد من أحكامه، منها ما ذهب إلى محكمة استئناف باريس لسنة 1990، عندما أدانت أحد الأشخاص بتهمة إتلاف المعلومات لقيامه بإدخال معطيات غير صحيحة إلى نظام الحاسب الآلي، كما أيدت محكمة النقض الفرنسية سنة 1994 إدانة أحد الأشخاص بتهمة إتلاف المعطيات، لقيامه بتدوين معطيات غير صحيحة بالنسب الخاصة بضريبة

¹ نائلة عادل محمود فريد قورة، المرجع السابق، ص 437.

² علي عبد القادر القهوجي، المرجع السابق، ص 144.

³ مسعود خثير، المرجع السابق، ص 124.

⁴ عبد المجيد جباري، دراسات قانونية في المادة الجزائية على ضوء أهم التعديلات الجديدة، دار هومة، الجزائر، ط2،

2013، ص 117.

المبيعات وذلك في الإستثمارات الخاصة بذلك، ثم قام بإدخال بعض المعطيات إلى نظام الحاسب الآلي.¹

2- فعل المحو (الإزالة)²

ويقصد به إلغاء جزء من المعطيات المسجلة على الدعامة والموجودة داخل النظام، أو تحطيم تلك الدعامة (أي إلغاء كل المعطيات، أو نقل وتخزين جزء من المعطيات إلى منطقة أخرى من الذاكرة.³

ومن أهم الأمثلة الواقعية على هذا الفعل، ما قام به العاملون في شركة السمسرة والتأمين على الحياة في فورت ورتو (fortwarth) بولاية تكساس سنة 1985، بعد فصله من العمل بإختراق النظام المعلوماتي للشركة المذكورة بهدف الإنتقام، حيث تمكن من محو أكثر 168000 من سجلات الشركة عن طريق زرع فيروس معلوماتي.⁴

3- فعل التعديل

ويقصد بهذا الفعل تغيير المعطيات الموجودة داخل النظام واستبدالها بمعطيات أخرى، ويتحقق هذا الفعل عن طريق برامج غريبة تتلاعب في المعطيات، سواء بمحوها كلياً أو جزئياً أو تعديلها، وذلك كإستخدام القنابل المعلوماتية الخاصة بالمعلومات، أو برامج المحاة gomme d'effacement أو برامج الفيروسات بصفة عامة.⁵

ومما سبق نجد أن هاته الأفعال السابقة (الإدخال، المحو، التعديل) وردت في نص التجريم على سبيل الحصر، وبالتالي لا تقع تحت طائلة التجريم أي فعل آخر غيرها، كنسخ المعطيات أو نقلها.

4- النتيجة الإجرامية

بخلاف جريمة الدخول أو البقاء غير المصرح به التي لا يشترط لوقوعها تطلب وجود نتيجة جرمية

¹ _محمد خليفة، المرجع السابق، ص 182.

² _ويختلف التعبير الذي يستعمله كل تشريع لتجريمه لهذا الفعل، فإتفاقية بودابست نصت في المادة الرابعة على عدة مصطلحات تصب كلها في سياق الإزالة وهي مصطلحات الإضرار، المحو، الطمس والإتلاف، وقد فضل المشرع الجزائري شأنه شأن الفرنسي مصطلح الإزالة.

³ _أمال قارة، المرجع السابق، ص 47.

⁴ _عبد اللاه أحمد هلال، حجية المخرجات الكمبيوترية في المواد الجنائية، دراسة مقارنة، دار النهضة العربية، القاهرة، د ط، 1999، ص 10.

⁵ _غنية باطلي، المرجع السابق، ص 176.

للسلوك المرتكب، لإعتبارها من جرائم الخطر، لكن جريمة التلاعب بمعطيات نظام المعالجة الآلية تتطلب نتيجة معينة، حيث تشترط وقوع ضرر فعلي على هذه المعطيات، وهو تغيير حالتها¹، وذلك من خلال الإزالة والمحو أو التعديل، وبالتالي فهي من الجرائم المادية ذات النتيجة، وليست مجرد جريمة شكلية.

ثانيا-الركن المعنوي

جريمة التلاعب بمعطيات نظام المعالجة الآلية للمعطيات جريمة عمدية، يجب توافر القصد الجنائي لمرتكبها، أي تتطلب قصدا جنائيا عاما، و المتمثل في العلم والإرادة، أي أن يعلم الجاني أنه يقوم بإحدى الأفعال التي أوردها النص القانوني، أي يعلم بأنه يقوم بإدخال أو إزالة أو المحو التي تؤدي إلى الإضرار بالمعطيات، وتغيير حالتها وتنتج إرادته، إلى القيام بهذه الأفعال وتحقيق النتيجة.

غير أن الفقه آثار جدلا واسعا حول وجوب توافر القصد الجنائي الخاص حتى تقوم الجريمة، فمن خلال نص المادة 394 مكرر 1 من ق.ع.ج، أشارت لمصطلح "الغش" نستنتج أن الجريمة عمدية وهي ذات الوضع بالنسبة للمشرع الفرنسي في مادته 3/323 من ق.ع.ف لكن ما استقر عليه القضاء الفرنسي وكرسه في العديد من أحكامه، منها النقض الجنائي في 1999.12.08²، وبالتالي هذه الجريمة لا تتطلب أي قصد خاص لكن هناك قوانين أخرى، اشترطت قصدا جنائيا كالقانون البرتغالي والفنلندي والتركي بنية تحقيق الربح.

مما سبق يتضح أن المشرع الجزائري بموجب نص المادة 394 مكرر 1 من ق.ع.ج، أراد أن يوفر الحماية الجنائية للمعطيات الموجودة بالنظام المعلوماتي ضد أي نشاط إجرامي.

ثالثا: العقوبات المقررة لجريمة التلاعب بالمعطيات

يقرر قانون العقوبات الجزائري في مادته 394 مكرر 1 على مرتكب جريمة التلاعب بالمعطيات، عقوبة أصلية تتمثل في الحبس في الحبس من ستة أشهر إلى ثلاث وعقوبة، الغرامة التي تتراوح بين 50.000 د.ج إلى د.ج 200.000.

¹ - محمد خليفة، المرجع السابق، ص 184.

² - رشيدة بوكري، المرجع السابق، ص 198.

الفرع الثالث: جريمة التعامل في معلومات غير مشروعة

تعد جرائم الإعتداء على نظام المعالجة الآلية للمعطيات، من أكثر الجرائم وقوعا وتسبب أضرارا بليغة، خاصة إذا كانت المعلومات التي يتم الإعتداء عليها تمثل أموالا، لهذا نجد المشرع الجزائري قد حرص على تبني سياسية جنائية تكفل الحماية لهذه المكونات قبل وبعد تمام العدوان الفعلي عليها¹، وإضافة إلى الجرائم المشار إليها سابقا فقد جرم المشرع التعامل مع هذه المعطيات الناتجة عن هذه الجرائم.

فقد نصت المادة 394 مكرر 2 من ق.ع.ج على أنه " يعاقب بالحبس من شهرين (2) إلى ثلاثة (3) سنوات وبغرامة مالية من 1.000.000 دج إلى 5000.000 دج كل من يقوم عمدا وعن طريق الغش بما يأتي:

- تصميم أو بحث أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلّة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

- حيازة أو إنشاء أو نشر أو إستعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم.

وتقابلها المادة 323-1 من قانون العقوبات الفرنسي والتي جاء فيها " كل من يقوم بدون مبرر قانوني بإستيراد أو حيازة أو توفير أو تجهيزات أو أدوات، برامج معلوماتية أو كل معطيات مصممة أو معدة لإرتكاب واحد أو أكثر من الجرائم المنصوص عليها المواد من 321-1 إلى 323-3 يعاقب بنفس العقوبات المنصوص عليها على التوالي بحسب أشد الجرائم عقوبة"²، وأيضا نص المادة 06 من إتفاقية بودابست المتعلقة بالجرائم الإلكترونية، أما الإتفاقية العربية لمكافحة جرائم تقنية المعلومات فقد نصت عليها في المادة 09.

فجريمة التعامل في معطيات غير مشروعة، مثل كل جريمة تتكون من ركن مادي ومعنوي وعقوبة

¹ _رشيدة بوكري، المرجع السابق، ص 274.

(2) _Art 323-3-1 du (C.P.F).

Le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçue ou spécialement adaptée pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

مقررة لها.

أولاً-الركن المادي

ويتخذ السلوك الإجرامي لهذه الجريمة صورتين أساسيتين هما:

1-التعامل في معطيات صالحة لإرتكاب جريمة

تجرم المادة 394 مكرر 02 مجموعة من الأفعال الخطيرة، التي لو تركت دون تجريم لأدت إلى حدوث جرائم أخرى، ولقيام هذه الجريمة يكتفي أن ترتكب بإحدى الأفعال المنصوص عليها في المادة السالفة الذكر وسوف نبين معنى هذه الأفعال.

أ- التصميم

وهي أول عملية في سلسلة التعامل في المعطيات، وتتمثل في إخراج المعطيات إلى الوجود وجعلها صالحة لارتكاب الجريمة، ولا يمكن تصور القيام بهذا السلوك، إلا من ذوي الاختصاص في المجال المعلوماتي كالمبرجين ومصممي البرامج¹.

ب-البحث

ويقصد بهذه العبارة البحث في كيفية تصميم هذه المعطيات وإعدادها، وليس مجرد البحث عنها أي البحث عن المعلومات من أجل تصميمها لأغراض تجريمية²، لهذا جاءت عبارة البحث بعد عبارة التصميم مباشرة، مثل البحث عن الشيفرات والبيانات التي يمكن من الإستيلاء على التوقيع الإلكتروني للشخص أو فك الشفرات تعاملاته المالية الالكترونية³.

ج-التجميع

وهو القيام بجمع أكبر عدد ممكن من المعلومات الخطيرة، يمكن أن ترتكب بها إحدى جرائم الإعتداء على نظم المعالجة الآلية للمعطيات، فما من شك أن الذي يحوز معلومة واحدة لا يشكل خطراً بقدر ما يشكله من يقوم بتجميع العديد من المعطيات، إن التجميع يعكس خطورة الفاعل ومدى قدرته على

¹ _محمد خليفة، المرجع السابق، ص 200.

² _رشيدة بوكري، المرجع السابق، ص 200/ وفي المعنى نفسه أحمد عبد اللاه هلال، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست، دار النهضة العربية، القاهرة، ط1، 2003، ص 101.

³ _ناصر حمودي، المرجع السابق، ص 82.

إرتكاب وسهولة إرتكاب إحدى الجرائم المنصوص عليها في القسم السابع مكرر من قانون العقوبات الجزائي.¹

د-التوفير

ويقصد به عرض المعلومات وإتاحتها، وجعلها في متناول الغير وتحت تصرفه وحيازته، مثل كلمات أو شفرات المرور التي تسمح بالدخول لجزء من النظام أو كله، فنجد القضاء الفرنسي قد توسع في تفسير مدلول التوفير ليشمل الكشف أو الإنشاء العلني للثغرات الأمنية في النظام.²

هـ-النشر

ويقصد بالنشر إذاعة المعلومات محل الجريمة، وتمكين الغير من الإطلاع عليها مهما كانت طبيعة هذه المعلومات³ وذلك عن طريق مختلف الوسائل التي يتصور النشر بها، ويعد النشر من أخطر الأفعال كونه يعني نقل هذه المعلومات إلى أكبر قدر ممكن من الأشخاص، وهذا ما أشارت إليه إتفاقية بودابست إلا أن مصطلح النشر ينبغي أن يمتد ليشمل كل نشاط من شأنه نقل معلومات إلى الآخرين⁴، وما يمكن ملاحظته أن النص الفرنسي جاء خاليا من عبارة النشر.

-الإتجار

الإتجار بالمعطيات تعني تقديمها للغير بمقابل، والمشرع عندما نص على مصطلحي التوفير والإتجار أراد من ذلك أن يجرم كل أفعال التعامل في المعطيات بطريقة غير مشروعة، سواء أكانت بمقابل أو بغير مقابل، بعكس المشرع الفرنسي لم ينص على مصطلح الإتجار، فيما نصت إتفاقية بودابست على مصطلح الإنتاج والبيع في نص المادة 06 ويعتبر مصطلح الإتجار أوسع من مصطلح البيع والإنتاج، فالمشرع الجزائري أصاب حين نص على مصطلح الإتجار، ليشمل كل أنواع التعاملات التي تبين خطورة هذه الجريمة.

¹ _غنية باطلي، المرجع السابق، ص 188.

² _cass crin 27 octobre 2009, disponible en ligne a l'adresse suivante : [http://www.globe.net.org/FMG/pdf/de cassation full disclosure criminelle chambre criminelle, 27 octobre 2009, 09-82-346 publie e au Bulletin sur ligne.pdf](http://www.globe.net.org/FMG/pdf/de%20cassation%20full%20disclosure%20criminelle%20chambre%20criminelle,%2027%20octobre%202009,%2009-82-346%20publie%20e%20au%20Bulletin%20sur%20ligne.pdf). 282. مشار إليه لدى رشيدة بوكري، المرجع السابق، ص 101.

³ _محمد خليفة، الحماية الجنائية لبرامج الحاسب الآلي، المرجع السابق، ص 203.

⁴ _ عبد اللاه أحمد هلال، الجوانب الموضوعية والاجرائية على ضوء إتفاقية بودابست، المرجع السابق، ص 101.

فقضية الهاكرز من ولاية باتنة التي حدثت سنة 2010، فالجريمة التي إرتكبها تضمنت كافة أشكال التعامل في معلومات غير مشروعة المنصوص عليها في المادة 394 مكرر 2، حيث كان يقوم بجمع المعلومات الخاصة بشركة أمريكية ثم قام بتهديدها، عن طريق نشر هذه المعلومات مقابل حصوله على مبالغ مالية.¹

2- جريمة التعامل في معطيات متحصلة من جريمة

وهي الجريمة الواردة في الفقرة الثانية من المادة 394 مكرر 2 من ق.ع.ج² وتمثل الصورة الثانية من صور جريمة التعامل في معطيات غير مشروعة، لم يتطرق المشرع الفرنسي ولا إتفاقية بودابست لهذه الصورة من الجرائم، وتتحقق هذه الجريمة بإرتكاب أفعال وسلوكات، حددت على سبيل الحصر والتي تتمثل فيما يلي:

أ-الحيازة

الحيازة هي السيطرة الفعلية والإرادية للحائز على المنقول، تخوله مكنه الإنتفاع به، أو تعديل كيانه أو تحطيمه أو نقله، فهي السيطرة من الشخص على الشيء الذي تستند لسبب قانوني، وفي هذه الحال المعطيات هي منقولات معنوية، التي تخول الحائز الإنتفاع به أو تعديل كيانه، أو تحطيمه أو نقله فهي سيطرة إرادية وتامة على الشيء والتي تكون غير مشروعة.³

ويقصد بالحيازة في جريمة التعامل في معطيات غير مشروعة تكون دائما غير مشروعة، ويشترط أن تكون متحصلة من إحدى جرائم المعطيات، سواء كانت جريمة دخول أو بقاء غير مصرح بهما، أو كانت جريمة تلاعب بمعطيات، ويتحقق فعل الحيازة بمجرد قيام الجاني بحفظ البيانات وجعلها بجوزته دون إذن أو ترخيص، وفي هذه الحالة لامجال لإذن أو ترخيص، طالما أن المشرع إشتراط أن تكون المعطيات

¹ _يزيد بوحليط، المرجع السابق، ص 135/ وانظر كذلك الحكم رقم 10/05272 الصادر عن محكمة باتنة بتاريخ 2010/06/01.

² _تنص المادة 394 مكرر 2 ف2 على أنه "يعاقب بالحبس من شهرين (2) إلى ثلاث (3) سنوات وبغرامة من 1.000.000 دج إلى 5000.000 دج كل من يقوم عمدا وعن طريق الغش بما يأتي:

-حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم."

³ _نسيمة جدي، جرائم المساس بأنظمة المعالجة الآلية للمعطيات، مذكرة لنيل شهادة الماجستير في الحقوق، كلية الحقوق، جامعة وهران، الجزائر، 2013-2014، ص 74.

متحصلة من الجرائم¹، الواردة في القسم السابع مكرر من قانون العقوبات الجزائري ومجرد الحياة يشكل قيام السلوك الإجرامي.

ب- الإفشاء

هو إفشاء معلومات يكون قد تم الحصول عليها بإرتكاب جريمة من جرائم الإعتداء على نظم المعالجة الآلية للمعطيات السابق تبيانها، وهو فعل يفترض إنتقال المعلومات من حياة الجاني إلى غيره من الأشخاص.

ج- النشر

النشر يعني إختراق النظم المعلوماتية، والحصول على المعلومات منها ومن ثم القيام بإفشائها، أيا كانت وسيلة الإفشاء، ونلاحظ أن المادة لم تشترط عددا معيناً من المرات حتى يمكن القول بتوافر فعل النشر، إذن المادة جاءت مطلقة، فالنشر لمرة واحدة تقوم الجريمة، كما لم يتم تعيين وسيلة معينة لفعل النشر، لذلك يمكن تصور أي وسيلة للقيام بهذا السلوك، قد يكون النشر عن طريق شبكة الأنترنت، أو الأقراص المضغوطة، أو حتى عن طريق نشرها كتابة.²

د- الإستعمال

يعد الإستعمال أخطر سلوك يمكنه أن يقع على المعطيات المتحصلة من جريمة، كأن تستعمل شركة ما معطيات أو معلومات عن شركة منافسة لها، ثم الحصول عليها بطريقة عن طريق دخول غير مصرح به³، ويشمل هذا التجريم أيا كان نوعية هذا الإستعمال والغرض منه رغبة من المشرع غلق الباب أمام، أي إستعمال معلومات متحصل عليها بطرق مجرمة.

وما يمكن ملاحظته، أن المشرع الجزائري و بموجب نص المادة 394 مكرر²، توسع في حمايته للمعطيات محل جريمة التعامل في معطيات صالحة لارتكاب جريمة، لتشمل المعطيات المخزنة أو

¹ يمكن تشبيه هذه الجريمة بجريمة حيازة أشياء متحصل عليها من جنحة أو جنابة، أو جنحة إخفاء أشياء مسروقة المعروفة في النصوص التقليدية لجرائم الأموال.

² محمد خليفة، الحماية الجنائية لبرامج الحاسب الآلي، المرجع السابق، ص 209.

³ غنية باطلي، المرجع السابق، ص 193.

المعالجة أو المرسل¹، وهذا ما أكدته المادة السالفة الذكر بقولها "..... في معطيات مخزنة أو معالجة أو مرسل²...." وهذا المسلك يبرره أن كثيرا من المعطيات التي يمكن أن ترتكب بها الجرائم قد لا تكون داخل نظام المعالجة الآلية للمعطيات، وإنما تكون على وسائط أخرى أو تكون مرسل² بين نظم المعلومات، وبالتالي فعدم تقييد النص بأنظمة المعالجة الآلية والمعطيات المعالجة كان الهدف منه أن يشمل مختلف المعطيات الصالحة لإرتكاب الجريمة²، إذا كان المشرع الجزائري قد اقتصر على المعلومات كمحل للجريمة، فإن المشرع الفرنسي توسع في ذلك، حيث أقر أن الأفعال المجرمة يمكن أن تقع على العناصر المادية من تجهيزات، أو أدوات أو على برنامج معلوماتي، أو المعطيات مصممة أو معدة لإرتكاب واحدة أو أكثر من الجرائم السابقة، وهذا ما جاء في نص المادة 323/3¹، إلا أنه قيد هذا التوسع بأن تكون الوسائل معدة ومصممة، لإرتكاب واحدة أو أكثر من جرائم المساس بأنظمة المعالجة الآلية للمعطيات، على عكس المشرع الجزائري الذي إشتراط أن تكون المعطيات صالحة لأن ترتكب بها الجريمة.

وبعد دراستنا لصور السلوك الإجرامي لجريمة التعامل في معطيات غير مشروعة ومتحصلة من جريمة، المشرع لا يتطلب وجود نتيجة إجرامية، ولا يتطلب تحقق ضرر فعلي، وإنما يجرم تلك الأفعال بوصفها أفعالا خطيرة يمكن أن تؤدي إلى ضرر فعلي.

ثانيا: الركن المعنوي

جريمة التعامل في معطيات غير مشروعة جريمة عمدية، وهو ما يمكن أن يستفاد صراحة من نص المادة 394 مكرر² من ق.ع من خلال عبارة "عمدا" وعن طريق الغش.... عكس الجرائم السابقة أين إكتفى بمصطلح "عن طريق الغش"، مما جعل البعض يرى أن استعماله من قبل المشرع غرضه توفر قصد خاص يضاف إلى القصد العام³.

فالجريمة تتطلب قصدا عاما يقوم على عنصرين هما العلم والإرادة، لا بد أن يعلم الجاني بكل

¹ _تراسل المعلومات عبارة عن توزيع المعلومات بين نقطتين أو أكثر، وعندما تكون هذه النقاط عبارة عن حواسيب أو طرفيات حواسيب فإن النقل يتم عبر شبكة حواسيب إن المعلومات المنقولة قد تمثل نصوصا أو أصواتا أو صورا أو صورا متحركة، ويتم نقل هذه المعلومات على شكل صفر أو واحد (0-1) وذلك بعد تحويلها من شكلها الأصلي عن طريق إحدى الشيفرات العالمية المعروفة مثل سيرفه أكسي Ascil، أنظر رشيدة بوكري، المرجع السابق، ص 291.

² _آمال قارة، المرجع السابق، ص 123.

³ _ناصر حمودي، المرجع السابق، ص 84.

عناصر الجريمة، إذ يلزم العلم بأن المعطيات التي يتعامل فيها أن تستعمل في إرتكاب الجرائم (هذه بالنسبة إلى الصورة الأولى للجريمة)، أو يعلم أن من شأن تعامله في المعطيات المتحصلة من الجريمة أن يزيد من الضرر المترتب على تلك الجريمة، كما يجب العلم بالصفة غير المشروعة للمعطيات، أي يعلم بأنه يمكن أن ترتكب بها الجريمة أو أنها متحصلة من جريمة، إلى جانب العلم لابد من توافر الإرادة أي أن تتصرف إلى النشاط الجرمي دون تحقيق نتيجة معينة، على إعتبار أنها من الجرائم الشكلية التي لا تتطلب نتيجة.

لكن السؤال الذي يمكن طرحه هل تتطلب جريمة التعامل بمعطيات غير مشروعة قصد جنائي خاص أم أنها تكتفي بقيام القصد الجنائي العام؟

كما رأينا أن جريمة التعامل في معطيات غير مشروعة تتخذ صورتين، ففي الصورة الأولى يرى جانب من الفقه توافر قصد خاص، إلى جانب القصد الجنائي العام حتى تقوم جريمة التعامل في معلومات صالحة لإرتكاب جريمة، يتمثل هذا القصد الخاص في إتجاه إرادة الجاني إلى الإعداد وتمهيد هذه المعلومات في إرتكاب جريمة من جرائم نظم المعالجة الآلية للمعطيات، غير أن المشرع لم يشترط صراحة القصد الخاص في نص المادة 394 مكرر2، أما فيما يخص الصورة الثانية تكتفي بتوافر القصد الجنائي العام لقيام الجريمة.

ثالثا: العقوبة المقررة

يعاقب مرتكب الجريمة بالحبس من شهرين (2) إلى ثلاث (3) سنوات وبغرامة مالية تقدر من 1000.000 دج إلى 5000.000 دج.

الفرع الرابع: الجرائم الأخرى ضد الأنظمة

لقد نص المشرع الجزائري على صور الجرائم الإلكترونية ضد الأنظمة المعلوماتية، ضمن القانون رقم 04-15 المعدل والمتمم لقانون العقوبات ضمن القسم السابع مكرر تحت تسمية "المساس بأنظمة المعالجة الآلية للمعطيات" في المواد 394 مكرر وما يليها، لكنه أغفل بعض أشكال الإعتداء على النظام المعلوماتي، والتي تناولتها التشريعات المقارنة بالدراسة فما هي هذه الجرائم؟ وهذا ما سنحاول دراسته في هذا الفرع.

الفقرة الأولى: جريمة إعاقة أو تحريف تشغيل نظم المعالجة الآلية للمعطيات

لم يتعرض المشرع الجزائري لهذه الجريمة، بل اكتفى بالنص على جريمة الإعتداء على المعطيات وذلك للتشابه الكبير بينهما، حيث اكتفى بإفساد النظام وتخريبه كظرف مشدد لجريمة الدخول أو البقاء غير المصرح بهما واستبعدها كجريمة قائمة بحد ذاتها¹، بعكس المشرع الفرنسي الذي أفرد لها نصا خاصا للتجريم، حيث نصت المادة 2/323 من ق.ع.ف عليها على أنه "يعاقب كل من عطل أو أفسد نشاطا أو وظائف المعالجة الآلية للمعطيات بالحبس خمس (5) سنوات وبغرامة 75000 أورو".²

ومن خلال استقراء نص المادة نجدها، نصت على السلوك الإجرامي لهذه الجريمة والذي يتخذ صورتين إما التعطيل أو الإفساد وبذلك فالهدف من النص هو التعرض لكل محاولة لإعاقة أو تحريف التي قد تلحق بالنظام.

ولتحقق هذه الجريمة لابد من توافر الركن المادي والركن المعنوي.

أولا: الركن المادي

ويقصد بإعاقة سير عمل النظام المعلوماتي ذلك الفعل الذي يسبب تباطؤ في عمل النظام أو ارتباكا مما يؤدي إلى تغيير في حالة عمل النظام على نحو يصيبه بالشلل المؤقت.

ويتحقق الركن المادي لهذه الجريمة بإتيان أحد الإفعال، إما توقيف أو تعطيل نظام المعالجة الآلية عن أداء نشاطه، وإما إفساد نشاط ووظائف هذا النظام.

1- التعطيل (العرقلة) ويقصد بإعاقة سير عمل النظام المعلوماتي في ذلك الفعل الذي يسبب تباطؤا في عمل النظام أو ارتباك عمل نظام المعالجة، ومن ثم ينتج عن ذلك تغيير في حالة عمل النظام، وهكذا الإرتباك الناجم عن الإعاقة تتأثر به أجهزة الكمبيوتر والبرامج على السواء.³

¹ _ولقد وضع الفقه معيار للتفرقة بين الإعتداء على المعطيات والإعتداء على النظام على أساس ما إذا كان الإعتداء وسيلة أو غاية، فإذا كان الإعتداء وقع على المعطيات مجرد وسيلة فإن الفعل يشكل جريمة الإعتداء العمدي على النظام، أما إذا كان الإعتداء الذي وقع على المعطيات غاية فإن الفعل يشكل جريمة الإعتداء العمدي على المعطيات. للمزيد أنظر: آمال قارة، المرجع السابق، ص 115.

² _Art 323/2 du c.p.f « le fait d'entraver ou de fausser le fonctionnement d'un système de Traitement automatisé des données est puni de cinq ans d'emprisonnement et de 75000 euros d'amende

³ _محمد أمين الشوابكة، المرجع السابق، ص 223.

والتوقيف أو التعطيل يقع بأي وسيلة، فالمشرع لم يشترط وسيلة معينة، قد يقع أو يتم بإدخال فيروس على البرنامج أو تعديل كلمة السر أو كيفية أداء النظام بوظيفته بوسيلة ما، على سبيل المثال أن يتباطأ هذا النظام عن أداء وظيفته داخل النظام المعلوماتي.¹

2- التعيب ويقصد به الإفساد، وهو لا يعطل نظام المعالجة للمعطيات، بل يؤدي إلى جعل هذا النظام غير صالح على الاستعمال السليم، وذلك أن يعطي نتائج غير تلك التي كان من الواجب الحصول عليها.²

وقد لاحظ جانب من الفقه أن التعيب المعاقب عليه في نص المادة 2/323 من ق.ع.ف يقترب من التعيب الذي يعد ظرفاً مشدداً حسب المادة 1/323 من ق.ع.ف الفرق بينهما أن الإفساد في حال الظرف المشدد لا يشترط فيه أن يكون عمدياً³، بينما يتطلب هذا الشرط بالنسبة لهذه الجريمة التي نحن بصدد دراستها.

وتتنوع وسائل التعيب أو الإفساد كاستخدام القنبلة المعلوماتية، أو استخدام البرنامج الذي يحمل فيروساً يطلق عليه "حصان طروادة"، وغير ذلك من الفيروسات التي تجعل مخرجات النظام غير تلك التي كان يجب أن يخرجها، بل إن الإفساد يمكن أن يتحقق عن طريق إتلاف العناصر المادية في النظام.⁴

ثانياً: الركن المعنوي: جريمة إعاقة أو تخزين تشغيل نظم المعالجة الآلية للمعطيات جريمة عمدية، ويتخذ الركن المعنوي فيها صورة القصد الجنائي العام بعنصرية العلم والإرادة، أي أن يعلم الجاني أن نشاطه يؤدي إلى تعطيل وإفساد النظام، وأن ذلك يتم بدون رضا صاحب الحق في السيطرة على النظام وتنتجه إرادته إلى فعل الإفساد أو التعيب.

ومن أمثلة التخريب أو التعطيل الواقع على نظام المعالجة الآلية للمعطيات قضية موريس، وتعد أولى الهجمات وقعت سنة 1988 على يد طالب يبلغ من العمر 23 سنة ويدعى روبير موريس من إطلاق فيروس عرف باسمه أدى إلى إصابة 6 آلاف جهاز يرتبط معها حوالي 6000 نظام عبر الأنترنت من ضمنها العديد من المؤسسات والدوائر الحكومية وقدرت الخسائر لا عادة تصلح الأنظمة وتشغيلها بحوالي مائة مليون دولار .

¹ _ عبد المجيد جباري، المرجع السابق، ص 114.

² _ المرجع نفسه، ص 114

³ _ آمال قارة، المرجع السابق، ص 119.

⁴ _ على عبد القادر القهوجي، المرجع السابق، ص 143.

ثالثاً: العقوبة المقررة

يعاقب المشرع الفرنسي على هذه الجريمة بعقوبة سالبة للحرية تتمثل بالحبس لخمس سنوات وغرامة مالية قدرها 75000 أورو.

الفقرة الثانية: جريمة سرقة وقت النظام المعلوماتي

يرى بعض فقهاء القانون الجنائي أن الإستخدام غير المشروع لنظام الحاسب الآلي، ما هو إلا سرقة لوقت هذا الحاسب الآلي، والتي تعرف تسميات متعددة منها جريمة إساءة استخدام وقت الحاسب الآلي أو سرقة وقت الحاسب الآلي، وأخيراً جريمة سرقة منفعة الحاسب الآلي¹، أي إستخدام وقت الحاسب الآلي من أجل أغراض شخصية.

ويعرف بأنه كل نشاط إجرامي ينطوي على اختلاس لوقت الحاسوب²، وبمعنى آخر هو كل استخدام للحاسب الآلي لاستفادة من الخدمات التي يقدمها، دون أن يكون للشخص الذي يمارس هذا الاستخدام الحق في ذلك³.

في الواقع نجد هذا السلوك منتشراً بين أوساط العاملين في المؤسسات المختلفة، وذلك لعدم وجود الشعور بعدم أخلاقية أو مشروعية هذا الفعل بين هؤلاء الأشخاص⁴، كما يمكن أن يقوم به شخص من الغير ليس له أي صلاحية أو ترخيص لاستعمال نظام المعالجة الآلية، وذلك باستغلاله للنظام غفلة أثناء تشغيله، كما قد يتحقق هذا السلوك عندما يعتمد شخص إلى زرع فيروس في النظام الخاص بالغير ويحصل بذلك على فوائد النظام دون أن يقوم بتسديد نفقات الحصول على المعلومات أو هذه الخدمات⁵.

¹ محمد سامي الشوا، المرجع السابق، ص 87.

⁽²⁾ _Devez (J), les qualifications pénales applicables aux Fraudes informatique, acte du VITI de l'AFDP, Grenoble 28-30 novembre 1985, Economisa, 1986, pp 185-213.

³ _نهلا عبد القادر المومني، المرجع السابق، ص 114.

⁴ _قامت المؤسسة العامة لشركات التأمين ضد الحريق والمخاطر الأخرى في فرنسا استطلاع للرأي، فكان السؤال الذي تم طرحه على العاملين في المؤسسة كالاتي: هل من الممكن أن تستخدموا الأنظمة المعلوماتية داخل المؤسسات لأغراض شخصية؟ وكانت نتيجة الاستطلاع أن أجاب 23% فقط النفي، لأن ذلك يشكل عملاً غير مشروع، في حين أن 77% أجاب بالإيجاب على اعتبار أن ذلك يعد عملاً مألوفاً من بينهم 19% قاموا فعلاً بإستخدام الحاسوب لأغراض شخصية، أنظر نائلة عادل محمد فريد قورة، المرجع السابق، ص 396.

⁵ _رشيدة بوكري، المرجع السابق، ص 221.

كما اختلف الفقه في تكييف هذا الفعل أو السلوك فمنهم من اعتبره سرقة للتيار الكهربائي، وغيره كيفه على أنه احتيال، والبعض الآخر وصفه بأنه إساءة ائتمان، أما البعض الآخر اعتبره إستعمالاً لأشياء الغير بدون وجه حق.¹

وبالرغم من أن الاستعمال غير المصرح للنظام المعلوماتي، لا يسبب خسائر كبيرة مقارنة بالجرائم المعلوماتية الأخرى، إلا أنه يمس مصالح جديرة بالحماية كالمصالح الإقتصادية للمؤسسة التي قد يصيبها الكثير من الضرر، نتيجة عدم حماية النظام المعلوماتي من الاستعمال.

ويمكن أن نذكر في هذا الخصوص واقعة، تتمثل في إثنيين من مستخدمي شركة غاز بريطانية قاما عن طريق إعلانات صغيرة ببيع رسومات صممت بواسطة النظام المعلوماتي الخاص بهذه الشركة، وهذا يساوي من الناحية العملية "العمل في الظلام" على حاسب آلي مملوك لرب العمل ولكن بدون علمه.²

لهذا نجد التشريعات المقارنة تباينت في طريقة معالجتها لهذه الجريمة، فمنها من نصت على تجريم هذا النوع من السلوك الإجرامي، كتشريعات بعض الولايات المتحدة الأمريكية وأستراليا، أما المشرع الجزائري لم يضع نصا خاصا وصريحا لجريمة استعمال غير مصرح به لوقت نظام المعالجة الآلية سواء في القانون رقم 04-15 الخاص بالمساحات بأنظمة المعالجة الآلية للمعطيات، أو القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وكذلك نفس الإتجاه الذي انتهجه المشرع الفرنسي.

إلا أن هناك من يرى أن النصوص الخاصة بجريمة البقاء غير المصرح به، يمكن أن تنطبق على فعل سرقة وقت نظام المعالجة الآلية، على أساس أن هذا الاستعمال مرفوض من صاحب النظام، إن هذا الفعل يتداخل كثيرا مع فعل البقاء غير المصرح به، من حيث كونه من الجرائم المستمرة، إلا أن هناك فرق بينهما، فالبقاء يتم بمجرد التواجد داخل النظام بغض النظر عن الانتفاع، بينما فعل سرقة وقت نظام المعالجة الآلية يقوم على استعمال أو استخدام النظام بغير وجه حق.³

ومن خلال دراستنا لصور الجرائم الماسة بنظام المعالجة الآلية للمعطيات، الواردة في القسم السابع

¹ _محمود أحمد عابنة، المرجع السابق، ص 89.

² _محمد سامي الشوا، المرجع السابق، ص، ص 87-88.

³ _رشدة بوكري، المرجع السابق، ص 222.

مكرر من قانون العقوبات الجزائري، التي تهدف لمواجهة الإعتداءات المعلوماتية التي تكون نظم المعالجة الآلية عرضة لها، نرى أن المشرع الجزائري وفق إلى حد كبير في مواجهة هذا النوع من الجرائم، بحيث سائر مختلف التشريعات المقارنة في ذلك، خاصة المشرع الفرنسي الذي كان سابقا في تجريم الإعتداءات على نظم المعالجة الآلية للمعطيات، وفي الأخير يمكننا أن نقول أن قانون العقوبات الجزائري بتعديله لقانون 15/104 يكون قادرا على إضفاء حماية جنائية للنظم المعلوماتية.

المطلب الثالث: جريمة الإرهاب الإلكتروني

بدأت علاقة الإرهاب والأنترنت تظهر إلى حيز الوجود، وتشغل بال الدول والمنظمات المعنية بمكافحة الإرهاب بعد أحداث 11 سبتمبر 2000، حيث أصبحت التنظيمات الإرهابية لا تقتصر نشاطاتها في المجال المادي الواقعي، بل انتقلت إلى الفضاء الإلكتروني¹، الذي أصبح المقر المختار للحركات والمنظمات المتطرفة والإرهابية لبث الأفكار المتطرفة، والحصول على التمويل والتبرعات وعملية التجنيد، وتبادل المعلومات والأفكار والتخطيط والتنسيق للعمل الإرهابي²، لذا سعت الدول إلى إتخاذ التدابير لمواجهة الإرهاب الإلكتروني، وحتى تتضح الرؤية نتطرق إلى مفهوم الإرهاب الإلكتروني (الفرع الأول) وصوره وأشكاله (الفرع الثاني) وأهم جرائمه في (الفرع الثالث)

الفرع الأول: مفهوم الإرهاب الإلكتروني

لقد تعددت تعاريف الإرهاب واختلفت في شأنه الآراء ولم يصل المجتمع الدولي حتى الآن إلى تعريف جامع ومانع متفق عليه للإرهاب، ويرجع ذلك إلى تنوع أشكاله ومظاهره، وتعدد أساليبه وأنماطه، وإختلاف وجهات النظر الدولية والاتجاهات السياسية حوله، فما يراه البعض إرهابا يراه الآخر عملا مشروعاً³، فعرفت الإتفاقية الدولية لمكافحة الإرهاب في جنيف (ب) عام 1937 الإرهاب بأنه "الأفعال الإجرامية الموجهة ضد أحد الدول والتي يكون هدفها أو من شأنها إثارة الفرع أو الرعب لدى شخصيات

¹ -أيسر محمد عطية، دور الآليات الحديثة للحد من الجرائم المستحدثة الإرهاب الإلكتروني وطرق مواجهته، ورقة علمية مقدمة في الملتقى العلمي حول الجرائم المستحدثة في ظل التغيرات والتحولات الإقليمية والدولية، كلية العلوم الإستراتيجية، عمان، المنعقد في الفترة بين 7-9/11/2014، ص 2.

² -حسين المحمدي بوادي، إرهاب الأنترنت الخطر القادم، دار الفكر الجامعي، الاسكندرية، ط1، 2006، ص 87.

³ -علي عدنان الفيل، الإجرام المعلوماتي-دراسة مقارنة-منشورات الحلبي الحقوقية، لبنان، ط1، 2011، ص 54.

معينة أو جماعات من الناس أو لدى العامة.¹

كما عرفته الإتفاقية العربية لمكافحة الارهاب الصادرة في القاهرة عام 1998م بأنه "كل فعل من أفعال العنف أو التهديد أيا كانت بواعثه، يقع تنفيذا لمشروع إجرامي فردي أو جماعي، ويهدف إلى إلقاء الرعب بين الناس أو ترويعهم بإيذائهم، أو تعريض حياتهم أو حرياتهم أو أمنهم للخطر، أو إلحاق الضرر بالبيئة أو بأحد المرافق أو الأملاك العامة أو الخاصة، أو إحتلالها أو الإستيلاء عليها أو تعريض الموارد الوطنية للخطر"²، هذا بالنسبة لمفهوم الإرهاب أما الإرهاب الإلكتروني³، الذي جاء نتيجة الثورة التكنولوجية التي شهدتها العالم الحديث عرف بأنه: "هجمات غير مشروعة، أو تهديدات بهجمات ضد الحاسبات أو الشبكات أو المعلومات المخزنة إلكترونيا، توجه من أجل الإنتقام أو الإبتزاز أو الإكراه أو التأثير في الحكومات أو الشعوب أو المجتمع الدولي بأسره، لتحقيق أهداف سياسية أو دينية أو إجتماعية معينة."⁴ ، وبالتالي فلكي نعت شخصا ما بأنه إرهابي على الأنترنت، وليس مخترقا فلا بد وأن تؤدي الهجمات التي يشنها إلى عنف ضد الأشخاص أو الممتلكات، أو على الأقل تحدث أذى كافيا من أجل نشر الخوف والرعب⁵، وقد عرفه مجمع الفقه الإسلامي الدولي التابع لمنظمة المؤتمر الإسلامي بأنه "العدوان أو التخويف أو التهديد المادي والمعنوي، الصادر عن الدول أو الأفراد أو الجماعات على الإنسان في دينه، نفسه، عرضه، عقله، أو ماله بغير حق بإستخدام موارد المعلوماتية والوسائل الإلكترونية بشتى صنوف العدوان والفساد."⁶، ويعتبر هذا التعريف من أفضل وأدق التعريفات الخاصة بالإرهاب الإلكتروني.

¹ محمد عبد المطلب، تعريف الارهاب الدولي بين الاعتبارات السياسية والاعتبارات الموضوعية، دار الجامعة الجديدة، الاسكندرية، ط، 2007، ص 48.

² المادة 02/01 من الاتفاقية العربية لمكافحة الإرهاب الصادرة في القاهرة عام 1998م، والتي صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم 98-413 المؤرخ في 1998/12/27م، الجريدة الرسمية للجمهورية الجزائرية، عدد 93 الصادرة بتاريخ 1999/03/09.

³ استخدم هذا المصطلح خلال فترة الثمانيات على يد باري كولين Barry collin الذي عرفه بأنه التقاء ما بين الفضاء السريري والإرهاب

John Arquilla, David ronfeldt, Networks and Net wars, the future of Terror, crime and Militancy, U.S.A .J rand publication, 2001, p281.

⁴ -هبة نبيلة هروال، جرائم الأنترنت، المرجع السابق، ص 333.

⁵ -علي عدنان الفيل، المرجع السابق، ص 60.

⁶ -أمير فرج يوسف، الجرائم الدولية للأنترنت، المركز القومي للإصدارات القانونية، القاهرة، ط1، 2011، ص 139.

ومن خلال التعاريف السابقة يتضح أن الإرهاب بشقيه التقليدي أو الإلكتروني، له نفس الغرض والهدف والمتمثل في بث الخوف والرعب في أوساط المجتمع، لكن وجه الاختلاف في الوسيلة المستعملة فقط المتمثلة في تقنيات تكنولوجيا الإعلام والاتصال، لذا يطلق عليها الأسلحة الناعمة.¹

وبالرجوع إلى القانون الجزائري، عرفت الجريمة الإرهابية بموجب المادة 87 مكرر²، من القانون رقم 01-14 المؤرخ في 04 فيفري 2014³، على أنه "يعتبر فعلا إرهابيا أو تخريبيا في مفهوم هذا الأمر كل فعل يستهدف أمن الدولة والوحدة الوطنية والسلامة الترابية وإستقرار المؤسسات وسيرها العادي عن طريق عمل غرضه ما يلي:

- بث الرعب في أوساط السكان وخلق جو إنعدام الأمن من خلال الإعتداء المعنوي أو الجسدي على الأشخاص أو تعريض حياتهم أو حريتهم وأمنهم للخطر أو المس بملكاتهم.

- عرقلة حركة المرور أو حرية التنقل في الطرق والتجمهر أو الاعتصام في الساحات العمومية.

- الاعتداء على رموز الأمة والجمهورية أو تدنيس القبور.

- الإعتداء على وسائل المواصلات والنقل والملكيات العمومية والخاصة والاستحواذ عليها أو احتلالها دون مسوغ قانوني.

- الإعتداء على المحيط أو إدخال مادة أو تسريبها في الجو أو في باطن الأرض أو إلقاءها عليها أو في المياه الإقليمية من شأنها جعل صحة الانسان أو الحيوان أو البيئة الطبيعية في خطر.

- عرقلة عمل السلطات العمومية أو حرية ممارسة العبادة والحريات العامة وسير المؤسسات المساعدة للمرفق العام.

- عرقلة سير المؤسسات العمومية أو الإعتداء على حياة أعوانها أو ممتلكاتهم أو عرقلة تطبيق

¹ - إيمان بن سالم، جريمة التجنيد الإلكتروني وفقا لقانون العقوبات الجزائري، المركز الديمقراطي للدراسات الاستراتيجية والسياسية والاقتصادية، برلين، 2018 نص 14.

² - أضيفت المادة 87 مكرر بموجب الأمر 95-11 المؤرخ في 25/02/1995، الجريدة الرسمية الجمهورية الجزائرية، عدد 11، الصادرة بتاريخ 27/02/1995.

³ - القانون رقم 01-14 المؤرخ في 04 /20/ 2014، يعدل ويتمم الامر 156/66 المت

القوانين والتنظيمات.

- تحويل الطائرات أو السفن أو أي وسيلة أخرى من وسائل النقل.

- إتلاف منشآت الملاحة الجوية أو البحرية أو البرية.

- تخريب اتلاف وسائل الاتصال.

- احتجاز الرهائن.

- الاعتداءات باستعمال المتفجرات أو المواد البيولوجية أو الكيميائية أو النووية أو المشعة.

- تمويل إرهابي أو منظمة إرهابية.¹

ومن خلال نص المادة السابق الذكر، حاول المشرع الجزائري احتواء كل الأفعال التي يمكن أن تصنف ضمن الجرائم الإرهابية، فنجدده وسع في تحديد مدلول الفعل الإرهابي، فاستعمل عبارات فضفاضة وغير دقيقة، حيث اكتفى بتعداد الأعمال الإرهابية على سبيل الحصر، مع اشتراطه توافر الباعث المستهدف لمصلحة معينة والمحمية قانوناً²، وعليه نرى أن المشرع لم يعط تعريف دقيقاً للإرهاب، أما فيما يتعلق بالإرهاب الإلكتروني لم يعرفه، لكن تصدى له بنصوص غير مباشرة وذلك من خلال القانون 04-15 المعدل والمتمم لقانون العقوبات، فبعض الأفعال الواردة في المواد من 394 مكرر إلى 394 مكرر 7 تشكل جزء من صور الإرهاب الإلكتروني، كاستعمال المشرع لعبارات تدخل ضمن السلوك الإجرامي لهذه الجريمة كالدخول، الحذف، التخريب، التغيير وغيرها من المصطلحات، كما تضمن القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها بموجب المادة 02 تحت عنوان المصطلحات فعرّف الجرائم المتصلة بتكنولوجيا الإعلام والاتصال على أنها "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية."، يفهم ضمناً حيث يمكن إدخال جريمة الإرهاب الإلكتروني ضمن أي جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظم للاتصالات الإلكترونية.

وباستقراء نصوص قانون العقوبات فإن المادة 87 مكرر 4³، من القانون 14-01 المؤرخ في

¹ - المادة 87 مكرر من قانون العقوبات الجزائري.

² - إيمان بن سالم، المرجع السابق، ص10.

³ - كنص المادة 87 مكرر 4 من ق.ع.ح على أنه «يعاقب بالسجن المؤقت من خمسة (5) إلى عشر (10) سنوات وبغرامة مالية من 100.000 دج إلى 500.000 دج كل من يشيد بالأفعال المذكورة في المادة 87 مكرر أعلاه أو يشجعها أو يمولها بأية وسيلة كانت».

2014/02/04 المعدل والمتمم فقد نصت على عقوبة جريمة الإشادة بالأفعال الإرهابية المذكورة في المادة 87 مكرر من نفس القانون، وكذا تشجيع هذه الأفعال أو تمويلها بأية وسيلة، فالترجيع والتشجيع كسلوك إجرامي، هو نشر أفكار التنظيم أو الجماعة ونشر أهدافه الهدامة، ويكون ذلك بكتابات منشورة أو أقوال في حفل عام¹، كما يقصد بتمويل المنظمات الإرهابية هو التمويل المادي كتوفير الأموال في صورتها النقدية أو العينية²، ولم يحدد النص شكلا معيناً للإشادة أو التشجيع أو التمويل فاستعمل المشرع عبارة بأية وسيلة، رغبة منه في توسيع الوسائل المستعملة كالتلفزيون، الفيديو والجرائد والمجلات وحتى الوسائل التكنولوجية الحديثة، كشبكة الأنترنت والهواتف المحمولة، فأحسن وأصاب في ذلك، وتزامنا مع اعتماد الجماعات الإرهابية على الوسائل التكنولوجية في تنفيذ جرائمهم، تصدى المشرع ونص صراحة على جريمة الإرهاب الإلكتروني وأسماها بجريمة الإرهاب باستخدام تكنولوجيات الإعلام والاتصال وهذا بموجب القانون رقم 16-02 المؤرخ في 19 جوان 2016.³ المعدل والمتمم لقانون العقوبات وذلك من خلال المواد 87 مكرر 11 و 87 مكرر 12 الواردة في القسم الرابع مكرر تحت عنوان "الجرائم الموصوفة بأفعال إرهابية وتخريبية"، وهذا سنقوم بدراسة لاحقا.

الفرع الثاني: صور وأشكال الارهاب الإلكتروني.

يتخذ الإرهاب الإلكتروني عدة أشكال تتماشى والتقدم التقني والتكنولوجي، وتغير تطور الأساليب التي حاولت المنظمات الإرهابية الوصول بها إلى أهدافهم، ومنها تحقيق أضرار جسمية من خلال تنفيذهم لتلك الجرائم ومن أهم هذه الأشكال ما يلي:

أولا-قيادة الجماعات الإرهابية ونشر الأفكار المتطرفة

لقد أصبح الفضاء الإلكتروني ملاذا لدعاة التطرف والعنصرية، مثل النازية الجديدة "تفوق الجنس الأبيض" و"معاداة السامية"، وقد تبلورت أساليبهم الإلكترونية الرقمية التي تخدم أفكارهم، بالإضافة إلى فعاليتها في تجنيد العناصر الشبابية لصالح معتقداتهم المتطرفة والإرهابية، حيث يمكن من خلال شبكة

¹ _ عبد الرحيم عبد الصادق شكر، جرائم الإرهاب في القانون الجنائي المصري والمقارن-دراسة موضوعية وإجرائية، دار النهضة العربية، القاهرة، ط1، 2012، ص 126.

² _يزيد بوحليط، المرجع السابق، ص 148.

³ _ القانون رقم 16-02 المؤرخ في 19 / 60 / 2016، يعل ويتم الامر 66-156 المؤرخ في 8 جوان 1966، المتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، عدد 37 الصادرة بتاريخ 2016/06/22.

الأنترنت بث الأفكار المتطرفة، سواء كانت سياسية أو دينية أو عنصرية والتي تسيطر على وجدان الأفراد وإفساد عقائدهم، واستغلال معاناتهم في تحقيق مآرب خاصة تتعارض مع مصلحة المجتمع.¹

ثانياً: إنشاء المواقع الإرهابية الإلكترونية

يقوم الإرهابيون بإنشاء وتصميم مواقع لهم على شبكة الأنترنت، لنشر أفكارهم والدعوة الى مبادئهم المنحرفة ولإبراز قوة التنظيم²، كما تعتمد على التقنية الإلكترونية لتعليم صناعة المتفجرات وتقديم النصائح والإرشادات لأعضائها، حول كيفية إختراق وتدمير المواقع المحجوبة ونشر الفيروسات³، ولم يقف الأمر عند هذا بل تجاوز ذلك إلى إنشاء قسم خاص بالمعلومات وشركات إعلامية نشطة منها "شركة السحاب الإعلامية"، ومواقع إلكترونية جهادية كموقع أبو محمد المقدسي الذي يعد من أشهر مشايخ الأنترنت، وقيامه بنشر الفتاوى والرسائل المتطرفة على أكثر من موقع.⁴

ثالثاً - القصف الإلكتروني

هو أسلوب للهجوم على شبكات المعلومات، عن طريق توجيه مئات الآلاف من الرسائل الإلكترونية إلى مواقع الشبكات، مما يزيد الضغط على قدرتها على استقبال الرسائل من المتعاملين معها، مما يؤدي إلى وقف عمل الشبكة، وقد كشفت التحقيقات أن هؤلاء المهاجمين قد استخدموا عناوين وهمية للرد على رسائلهم التي يوجهونها لمهاجمة هذه المواقع، من أجل إخفاء مصدر رسائلهم ثم الوصول إلى مصدر هذه الرسائل أو البرامج الذي استخدموه لتنفيذ هجماتهم.⁵

رابعاً: التجسس الإلكتروني⁶

¹ _حسين المحمدي، المرجع السابق، ص 84.
² _علي عدنان الفيل، المرجع السابق، ص 84.
³ _عبد الرحمان بن عبد الله السند، وسائل الإرهاب الإلكتروني حكمها وطرق مكافحتها، مقال منشور على موقع السكينة الإلكترونية، ص9، منشور على الموقع: [www.Assakina.com/filis/Book 8 PDF](http://www.Assakina.com/filis/Book%208%20PDF) أطلع عليه بتاريخ 2018/09/19 على الساعة 15.30
⁴ _إيمان بن سالم، المرجع السابق، ص 19.
⁵ _حسنين المحمدي بواوي، المرجع السابق، ص، ص 97-98.
⁶ _يعرف التجسس الإلكتروني بأنه "الحصول وتجميع المعلومات السرية المخزنة والمحفوظة داخل الحواسيب المربوطة بالأنترنت، والخاصة بسياسية الدولة ودفاعها ونظامها الإقتصادي والصناعي، وكذا أبحاثها العلمية خاصة تلك المتعلقة بأبحاث الطاقة النووية وتسليمها إلى حكومة أجنبية أخرى، أو تجميع معلومات شخصية عن مستخدمي الأنترنت بغية استغلالها لأغراض معينة أنظر: نبيلة هروال، جرائم الأنترنت، المرجع السابق، ص 372.

هو قيام الإرهابيين بالتجسس على الأشخاص، والدول أو المنظمات أو الهيئات أو المؤسسات الدولية أو الوطنية ويكون التجسس بإختراق المواقع والصفحات الإلكترونية على الأنترنت، بغرض التجسس أو التنصت على ما تحتويه من بيانات ومعلومات، وقد تم رصد بعض حالات التجسس الدولي من طرف وكالة الأمن القومي الأمريكي "NSA" والكشف عن شبكة دولية ضخمة للتجسس بإدارة كندا وبريطانيا وأستراليا ونيوزيلندا، لرصد المكالمات الهاتفية والرسائل بمختلف أنواعها وتدعى هذه الشبكة باسم "echelow".¹

الفرع الثالث: صور جرائم الإرهاب الإلكتروني

إستجابة للالتزامات الدولية المتعلقة بمكافحة الإرهاب، خاصة منها قرار مجلس الأمن رقم 2178 الصادر بتاريخ 24 سبتمبر سنة 2014²، سارعت الجزائر إلى تعزيز منظومتها التشريعية للتصدي ومحاربة الإرهاب، خاصة المرتكب بواسطة وسائل التكنولوجيا الحديثة، فبادرت إلى تعديل قانون العقوبات فأصدرت القانون رقم 16-02 المؤرخ في 19/06/2016، لتجريم ومعاينة تنقل الجزائريين أو رعايا أجانب مقيمين في الجزائر إلى دولة أخرى للتحريض على تنفيذ أعمال إرهابية، وتمويل وتنظيم عمليات التنقل نحو دولة أخرى باستعمال وسائل تكنولوجيا الإعلام والاتصال، فأضاف المادتان 87 مكرر 11 و 87 مكرر 12، المتعلقة بالتجنيد لسد الفراغ القانوني في مجال مكافحة الإرهاب الإلكتروني وسنحاول تحليل ما جاءت به المادتان كما يلي:

الفقرة الأولى: جريمة السفر إلى دولة أخرى لارتكاب أفعال إجرامية

تنص المادة 87 مكرر 11 من ق.ع.ج على أنه " يعاقب بالسجن المؤقت من خمس (5) سنوات إلى عشر (10) سنوات وبغرامة مالية من 100.000 دج إلى 500.000 دج كل جزائري أو أجنبي مقيم بالجزائر بطريقة شرعية أو غير شرعية يسافر أو يحاول السفر إلى دولة أخرى بغرض ارتكاب أفعال إرهابية أو تدبيرها أو الإعداد لها أو المشاركة فيها أو التدريب على ارتكابها أو لتلقي تدريب عليها.

يعاقب بنفس العقوبة كل من:

¹ إيمان بن سالم، المرجع السابق، ص 19.

² قرار رقم S/RES /2178/2014 لمجلس الأمن الذي يلزم جميع الدول الأعضاء في الأمم المتحدة بتجريم سفر المواطنين أو سعيهم إلى السفر الى الخارج ليصبحوا "مقاتلين إرهابيين أجانب".

- يوفر أو يجمع عمدا أموالا بأي وسيلة وبصورة مباشرة أو غير مباشرة بقصد إستخدامها أو مع علمه بأنها ستستخدم في تمويل سفر أشخاص إلى دولة أخرى بغرض ارتكاب الأفعال المذكورة في الفقرة الأولى من هذه المادة.

- قام عمدا بتمويل أو تنظيم سفر أشخاص إلى دولة أخرى بغرض ارتكاب أفعال إرهابية أو تدبيرها أو الإعداد لها أو المشاركة فيها أو التدريب على ارتكابها أو لتلقي تدريب عليها أو تسهيل ذلك السفر.

- يستخدم تكنولوجيا الإعلام والاتصال لارتكاب الأفعال المذكورة في هذه المادة".

ومن خلال هذا النص نحاول إستخراج أركان هذه الجريمة والمتمثلة في الركن المادي والركن المعنوي والعقوبة المقررة لها.

أولا - الركن المادي

ركزت المادة 87 مكرر 11 من ق.ع.ج على فعل السفر وقد تضمن التجريم السفر بالنسبة للشخص نفسه لغرض ارتكاب أعمال إرهابية، وتمويل سفر الغير لغرض ارتكاب أعمال إرهابية، وكذا تنظيم سفر أشخاص آخرين عمدا لغرض ارتكاب أفعال إرهابية، أو تدبيرها أو الإعداد لها أو المشاركة فيها أو التدريب على ارتكابها أو لتلقي تدريب عليها، ويقصد بالسفر هو التنقل من مكان إلى آخر رغبة في تحقيق هدف معين، كالسياحة أو التجارة أو الدراسة وغيرها... لكن في هذه المادة أكدت على السفر بغرض ارتكاب أفعال إرهابية، رغم أن المشرع لم يحدد الأفعال التي تتعلق بالإرهاب الإلكتروني بإعتبار النص ضمن عبارة "لإرتكاب أفعال إرهابية"، ما يؤكد على احتواء كل الأفعال الموصوفة بأفعال إرهابية وتخريبية الوارد في المادة 87 مكرر ق.ع.ج، إذا المشرع الجزائري أضاف سلوكا إجراميا جديدا يمكن إدخاله ضمن مفهوم الجريمة الإرهابية التقليدية، ونص على حالة خاصة تتحول فيها هذه السلوكات، وتكيف على أنها سلوكات إرهاب إلكتروني، وهي حالة استخدام وسائل تكنولوجيا الإعلام والاتصال¹، وهذا ما جاء في الفقرة الأخيرة من نفس المادة السالفة الذكر فالنص جاء غامضا في هذه النقطة فلا يمكن أن نتصور وجود السفر بإستعمال هذه الوسائل²، إلا إذا كان قصد المشرع الولوج عبر الشبكة الأنترنت التي

¹ - أمينة علالي، الجرائم العابرة للحدود المرتكبة بتقنية الأنترنت، أطروحة لنيل شهادة دكتوراه علوم، كلية الحقوق والعلوم السياسية، جامعة باجي مختار، عنابة، الجزائر، 2018، ص 119.

² - وضع مكتب الأمم المتحدة لمكافحة الإرهاب برنامجا لمكافحة سفر الإرهابيين، حيث يساعد الدول الأعضاء على بناء

تتيح تبادل المعلومات والأفكار بين الأشخاص لتنفيذ مخططاتهم الإجرامية، أو كان يقصد التنقل من مكان إلى آخر بوسائل السفر المعروفة ويعتبر الاحتمال الأخير هو الذي يقصده المشرع.

ومن جهة أخرى أن المشرع الجزائري، لم يعط تفسيراً لهذه الأفعال جاءت مبهمة وغامضة، بإعتبار أن التدبير أو الإعداد لها والمشاركة فيها، أو التدريب على ارتكابها أو لتلقي التدريب عليها فإن هذه السلوكات تدخل ضمن التحضير للعمل الإرهابي وليس الفعل الإرهابي نفسه، لكن بالرجوع إلى البرتوكول الإضافي لإتفاقية مجلس أوروبا لمنع الإرهاب أعطت مفهوماً لعبارة "تلقى تدريب" طبقاً لما جاء في المادة 3 من البند الأول فعرفته بأنه "لأغراض هذا البرتوكول يعني "تلقى تدريب للإرهاب" تلقي تعليمات بما في ذلك الحصول على المعرفة أو المهارات العملية، من شخص آخر في صنع أو إستخدام المتفجرات أو الأسلحة النارية، أو غيرها من الأسلحة أو المواد الضارة أو الخطرة، أو في الوسائل أو الطرق بغرض تنفيذ جريمة الإرهابية أو المساهمة في ارتكابها.¹

كما قام المشرع الجزائري بتجريم فعل السفر، سواء من جزائري أو أجنبي مقيم بالجزائر بطريقة شرعية أو غير شرعية لارتكاب أفعال إرهابية، أو تدبيرها أو الإعداد لها، أو المشاركة فيها أو التدريب على ارتكابها أو لتلقي تدريب عليها، تنفيذاً للقرار الصادر عن الأمم المتحدة 2178(20014)، وفي ذلك عالجت محكمة الجنايات لدى مجلس قضاء تيزي وزو، قضية الإنخراط في جماعة إرهابية ومحاولة السفر إلى دولة أخرى بغرض ارتكاب أفعال إرهابية والمشاركة فيها، واستخدام تكنولوجيا الإعلام والاتصال لدعم تنظيم إرهابي ونشر أفكاره²

كما أضاف سلوكاً آخر ممثلاً، في تمويل أو تنظيم أشخاص للسفر عن طريق جمع وتوفير أموالاً

قدراتها على الكشف عن الجرائم الإرهابية وذلك باستخدام نظام المعلومات المسبقة عن الركاب وسجل أسماء الركاب وبيانات الركاب، كما يساعد هذا البرنامج الدول في المجالين التشريعي والتشغيلي بشكل شامل والعمل مع قطاع النقل والمجالات التقنية، ويشمل ذلك التبرع بنظام برمجية go travel للأمم المتحدة وتعميم العمل به . أنظر الموقع الإلكتروني www.un.org/counterterrorism/ar/countering-t.... أطلع عليه يوم 20/05/15 على الساعة 12h 30.

¹ - عبد النور بعجي، نسيمه مالك، الإرهاب الإلكتروني: بين عولمة الجريمة وضرورة المكافحة، مجلة الدراسات والبحوث القانونية، المجلد 7، عدد 2، 2022، ص، ص، 87-79.

² - فروجة م، تلميذ ثانوي يقود خلية لـ "داعش" تيزي وزو، مقال منشور على موقع جريدة الشروق، للمزيد من الإطلاع أنظر الرابط التالي:

<https://www.echororik.online.com> أطلع عليه يوم 2021/04/15 على الساعة 13.00.

عمدا وهذا ما تناولته الفقرة الثانية من المادة السابقة الذكر، وقد عرف تمويل الإرهاب بموجب المادة الثالثة من قانون 06/15¹، المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتها بأنه " كل فعل يقوم به شخص بأية وسيلة كانت مباشرة أو غير مباشرة، وبشكل غير مشروع وإرادة الفاعل، من خلال تقديم أو جمع أموال بنية استخدامها كليا أو جزئيا، من أجل ارتكاب الجرائم الموصوفة بأفعال إرهابية أو تخريبية المنصوص عليها والمعاقب عليها بالمواد 87 مكرر إلى 87 مكرر 10 من قانون العقوبات." ²

لكن اشترط التمويل في هذه الجريمة أن يكون باستخدام تكنولوجيا الإعلام والاتصال عن طريق المواقع الإلكترونية، أو شبكات التواصل الإجتماعي التي يتم فيها اصطيد الأشخاص لجمع التبرعات المالية أو عن طريق قرصنة الحسابات البنكية وبطاقات الائتمان لتحويل الأموال من حساب إلى آخر³، أو باستعمال البريد الإلكتروني غير المرغوب فيه أو ما يعرف باسم "سبام" SPAM.⁴

وكعادته المشرع لا يعتد بالوسيلة المستعملة في ارتكاب الجرائم التقليدية، إلا أنه اشترط من خلال نص المادة 87 مكرر 11 ق.ع.ج، أنه في حالة ارتكاب هذه السلوكات الإجرامية عن طريق الأنظمة المعلوماتية، تعتبر جرائم إرهاب إلكتروني، إذا فهذه الوسيلة تعتبر شرطا جوهريا لقيام الجريمة الإرهابية الإلكترونية فعدم وجود هذه الوسيلة تعتبر جريمة إرهابية تقليدية.

كما لا تتطلب حدوث نتيجة معينة، فتكفي بإثبات الأفعال المجرمة لأنها من الجرائم الشكلية، فالضرر فيها محتملا بمجرد التهديد بالعدوان الذي ينال من المصلحة محل الحماية الجنائية.⁵

ثانيا: الركن المعنوي

إن الجرائم الإرهابية تعتبر جرائم عمدية في الغالب، فالجريمة الواردة في المادة 87 مكرر 11 ق.ع.ج جريمة عمدية فاستعمل المشرع مصطلح "يوفر أو يجمع عمدا"، وكذا قيام عمدا تمويل أو تنظيم

¹ _ القانون رقم 06/15 المؤرخ في 2015/02/15 يعدل ويتم القانون رقم 01/05 المؤرخ في 2005/02/06 المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتها.

² _ وهو نفس التعريف الوارد في الاتفاقية العربية لمكافحة غسيل الأموال وتمويل الإرهاب لعام 2010، المصادق عليها.
³ _ توفيق مجاهد، جريمة الإرهاب الإلكتروني في ضوء أحكام الاتفاقية العربية لمكافحة تقنية المعلومات، مجلة العلوم القانونية والسياسية، المجلد 09، العدد 03، ديسمبر 2018، ص 88.

⁴ _ وهو استخدام أنظمة الإرسال الإلكتروني لإرسال رسائل غير مرغوب المستخدم بتلقيها، وتختلف الرسائل غير المرغوب فيها ولكن معظمها ترسل لترويج إعلانات.

⁵ _ عبد الرحمن خلفي، محاضرات في القانون الجنائي العام، دار الهدى، الجزائر، ط1، 2012، ص 105.

ولقيامها يجب توافر القصد الجنائي العام، المتمثل في العلم والإرادة، أي علم الجاني بإرتكابه سلوكا مجرما قانونا، مع إتجاه إرادته إلى تحقيق الأفعال المجرمة، كما يتطلب وجود قصد جنائي خاص، يتمثل في نية المجرم إلى القيام بفعل السفر والتمويل باستخدام تكنولوجيا الإعلام والاتصال بغرض إرتكاب أفعال إرهابية.

ثالثا: العقوبة المقررة

يعاقب المشرع الجزائري مرتكب الأفعال المنصوص عليها في المادة 87 مكرر 11 ق.ع.ج بعقوبة سالبة للحرية وهي السجن المؤقت التي تتراوح مدته من خمس (5) سنوات إلى عشر (10) سنوات وعقوبة الغرامة المالية تقدر ب 100.000 دج إلى 500.000 دج.

ما يمكن ملاحظته أن العقوبة التي أقرها المشرع الجزائري، لا تتناسب مع خطورة الأفعال الخطيرة المجرمة، كان على المشرع أن يساير التشريعات المقارنة التي شددت من العقوبة بالنسبة للجرائم الخاصة بالإرهاب الإلكتروني كالتشريع الأردني والمصري.¹

الفقرة الثانية: جريمة التجنيد

نصت المادة 87 مكرر 12 من ق.ع.ج على " يعاقب بالسجن المؤقت من خمس (5) سنوات إلى عشر (10) سنوات وبغرامة من 100.000 دج إلى 500.000 دج، كل من يستخدم تكنولوجيا الإعلام والاتصال لتجنيد الأشخاص لصالح إرهابي أو جماعة أو منظمة يكون غرضها أو تقع أنشطتها تحت طائلة أحكام هذا القسم، أو ينظم شؤونها أو يدعم أعمالها أو أنشطتها أو ينشر أفكارها بصورة مباشرة أو

¹ _عاقب المشرع الأردني على جريمة الإرهاب الإلكتروني بموجب المادة 10 من قانون جرائم أنظمة المعلومات نص على أنه " كل من استخدم نظام المعلومات وشبكة المعلومات أو أنشأ موقعا إلكترونيا لتسهيل القيام بأعمال إرهابية...يعاقب بالأشغال الشاقة، أنظر القانون جرائم أنظمة المعلومات الأردني رقم 30 لسنة 2010 المنشور على الصفحة 5334 من عدد ج رقم 5056 متاح على الموقع: <https://www.unpdc.org> اطلع عليه 2018/09/07 على الساعة: 13:50. أما المشرع المصري وبموجب المادة 15 من قانون رقم 94 المتعلق بمكافحة الإرهاب لسنة 2015 ينص على أنه "يعاقب بالسجن المؤبد أو السجن المؤقت الذي لا تقل مدته عن عشرين سنة، كل من قام بأي طريقة مباشرة أو غير مباشرة ويقصد إرتكاب جريمة الإرهاب في الداخل أو الخارج بإعداد أو التدريب أفراد على صنع أو استعمال الأسلحة التقليدية أو غير التقليدية أو وسائل الاتصال السلكية واللاسلكية أو الإلكترونية أو أي وسيلة تقنية أخرى..." أنظر: قانون رقم 94 لسنة 2015 المتضمن قانون مكافحة الإرهاب المصري، الجريدة الرسمية عدد 33 مكرر، المؤرخ في 2015/08/10، متاح على الرابط: <https://www-allkarama.org> أطلع عليه 2018/09/07 على الساعة 13:30.

غير مباشرة"¹.

ومن خلال نص المادة نستخرج أركان الجريمة المتمثلة في الركن المادي، والركن المعنوي والعقوبة المقررة.

أولا -الركن المادي

يتحقق الركن المادي لهذه الجريمة بإتيان الفاعل بسلوك مجرم وهو فعل تجنيد الأشخاص، والذي يقصد به تصيد واستقطاب الشباب وجمعهم للانخراط في الجماعات الإرهابية محلية كانت أو دولية، عن طريق إعدادهم ماديا ومعنويا للعمل في خدمة هذه الجماعات، وتنفيذ مخططاتها الإرهابية²، أو "جمع الأشخاص وإستقطابهم أو بالأحرى استخدامهم ترغيبا أو ترهيبا، للانضمام إلى العناصر والجماعات الإجرامية المحلية والدولية في مختلف المجالات، وإعدادهم ماديا ومعنويا للعمل في خدمة هذه العناصر والجماعات والانخراط في أنشطتها غير المشروعة، وتكليفهم بالقيام في مختلف الأعمال التي تخدم مصالحها وتحقيق أهدافها.³

ولجذب الشباب وتجنيدهم تنشئ الجماعات الإرهابية مواقع إلكترونية⁴، هدفها إستدراج عدد أكبر من المجندين في صفوفهم بإستخدام شبكات التواصل الاجتماعية⁵، كالفاسبوك (face book) وتويتر (Twitter) يوتيوب (you tube) واتس آب (what's App) انستغرام (instagram) وتدعيمها بخلايا التجنيد.

¹ _المادة 87 مكرر 12 من قانون العقوبات الجزائري يعدل ويتم الأمر 156/66.

² _إيمان بن سالم، المرجع السابق، ص 51.

³ _شريعة كلاع، ظاهرة تجنيد الشباب في الجماعات الإرهابية من خلال إستخدام شبكات التواصل الإجتماعي، مجلة مدارت سياسية، المجلد 2، العدد 6، 2018، ص 84.

⁴ _ ومن أهم المواقع الإلكترونية العربية التي أنشأتها وصممتها بعض التنظيمات الإرهابية:

-موقع النداء وهو الموقع الرسمي لتنظيم القاعدة بعد أحداث 11 سبتمبر 2001، ومن خلاله تصدر البيانات الإعلامية للقاعدة.

-موقع ذروة السنام: وهي صحيفة إلكترونية دورية للقسم الإعلامي لتنظيم القاعدة.

-البتار: وهي مجلة عسكرية إلكترونية متخصصة، تصدر عن تنظيم القاعدة، وتختص بالمعلومات العسكرية والميدانية والتجنيد/ أنظر: عديلة محمد الطاهر، استخدام مواقع التواصل الإجتماعي في عمليات التجنيد الإرهابي، قراءة في الآليات، المضمون، وسبيل الوقاية، مجلة الأستاذ الباحث القانونية والسياسية، 2017، ص 87.

⁵ _تستغل داعش، مواقع التواصل الحديثة في عملية التجنيد وأن 80 % من عمليات التجنيد تتم عبر شبكات التواصل الاجتماعي، بينما 20% فقط يتم داخل المساجد أو السجون.

هدفها إغراء المستهدفين، وفي هذا الصدد قامت مصالح الإستعلامات التابعة للشرطة الجزائرية من توقيف ما يزيد عن 220 جزائريا لهم علاقة مباشرة مع تنظيم "داعش" في سوريا والعراق وليبيا، حيث فككت ما يزيد عن 55 خلية تسعى إلى إستقطاب الشباب وتجنيدهم عبر مواقع الأنترنت ومواقع التواصل الاجتماعي خاصة "فيسبوك" و"تويتر"¹، كما يتم التجنيد عن طريق وسائل أخرى كإختراق البريد الإلكتروني للأشخاص، وإرسال رسائل تجبرهم إلى الإنضمام إلى الجماعات الإرهابية، أو عن طريق اختطاف الرهائن لتجنيدهم فيما بعد.

وقد يقع التجنيد سواء على أشخاص معينين كالشباب ذوي الكفاءات العلمية العليا، كالخبراء في تقنيات وسائل التكنولوجيا والإعلام، أو شخصيات مشهورة، كما يمكن للجماعات الإرهابية اصطيد الفتيات في إطار ما يعرف ب"زواج النكاح"²، كما اشترط المشرع الجزائري لقيام هذه الجريمة الواردة في المادة 87 مكرر 12 ق.ع.ج، أن يتم التجنيد بإستعمال أو عن طريق وسائل تكنولوجيا الإعلام والاتصال³، كما حدد الجهات التي تجند لصالحها وهي إما إرهابي أو جمعية إرهابية أو تنظيم إرهابي أو جماعة إرهابية أو منظمة إرهابية، وما يمكن ملاحظته أن المشرع الجزائري لم يكن واضحا في العبارات التي تحدد هذه الجهات فمثلا الجمعية هي مرادف لتنظيم، جماعة، منظمة، هيئة وهي لها نفس المعنى والمضمون في قاموس المعاني.

وجريمة التجنيد جريمة شكلية لا تحتاج إلى نتيجة معينة لقيام ركنها المادي، فهي جريمة قائمة بذاتها ولو لم يتحقق فعل التجنيد فعليا كونها جريمة خطر وليس جريمة ضرر، وذلك بالنظر للوسيلة

¹ مقال منشور في جريدة الوطن بعنوان الجيش الجزائري 720 ألف صفحة على مواقع التواصل لتجنيد الإرهابيين منشور على الموقع: alwatannews-net-com-anprojet.org بتاريخ 2018/04/17 أطلع عليه يوم 2018/06/25 على الساعة 14:50.

² إيمان بن سالم، المرجع السابق، ص 52.

³ يقصد بمصطلح تكنولوجيا الإعلام والاتصال كافة التقنيات التي يتم استخدامها لتحويل البيانات على مختلف أشكالها إلى معلومات متنوعة، أو هي مجموعة الأدوات والتقنيات أو النظم أو الوسائل المختلفة التي يتم توظيفها في سبيل معالجة المحتوى والمضمون وإيصاله، وتتم عن طريق جمع البيانات والمعلومات سواء كانت مسموعة أو مصورة أو مكتوبة أو مرسومة عن طريق الحاسبة الإلكترونية ومن ثم تخزينها والعمل على استرجاعها في الوقت المناسب، ومن ثم نقلها ونشرها من مكان إلى آخر، أنظر في ذلك عادة الحلايقة، بحث حول تكنولوجيا الإعلام والاتصال منشور بتاريخ 2018/08/11 على الموقع التالي: <https://mawdoo3.com> اطلع عليه يوم 2018/10/27 على الساعة 15.00.

المعتمد عليها في تنفيذ الجريمة والمتمثلة في إستخدام تكنولوجيا الإعلام والاتصال.¹

ثانيا : الركن المعنوي

جريمة التجنيد باستخدام تكنولوجيا الإعلام والاتصال جريمة عمدية، تتطلب توافر القصد الجنائي العام المتمثل في علم الجاني بإرتكابه سلوكا مجرما قانونا، وهو فعل التجنيد وعلمه كذلك بالوسيلة المعتمدة عليها في عملية التجنيد، وهي إستخدام تكنولوجيا الإعلام والاتصال، كما تتجه إرادته إلى استعمال هذه الوسيلة من أجل تجنيد الشباب في الجماعات الإرهابية.

إلى جانب القصد العام توجب هذه الجريمة وجود قصد جنائي خاص يتمثل في نية الجاني إلى زعزعة استقرار أمن الدولة لتحقيق غايات إرهابية²، وللباعث في الجريمة الإرهابية دور كبير فالغرض هو جوهر الجريمة، إذا انتفى غرض الإرهاب لا تقوم الجريمة الإرهابية، وهذا ما ذهب إليه المشرع الجزائري في نص المادة 87 مكرر من قانون العقوبات الجزائري، فالباعث في الجريمة الإرهابية غرضه بث الرعب والخوف واستهداف أمن الدولة وإستقرارها.

ثالثا :-العقوبة المقررة

عاقب المشرع الجزائري على جريمة التجنيد بإستعمال وسيلة تكنولوجيا الإعلام والاتصال، الواردة في نص المادة 87 مكرر 12 ق.ع.ج، بعقوبة سالبة للحرية وهي السجن المؤقت التي تتراوح مدته من خمس سنوات إلى عشر سنوات وعقوبة مالية تقدر بـ 100.000 دج إلى 500.000 دج.

المطلب الرابع: الاعتداء على حرمة الحياة الخاصة

الحق في الحياة الخاصة مبدأ من أهم المبادئ الأساسية التي تركزها جميع الدساتير في كافة دول العالم وتنص عليها في قوانينها، كما تنص عليها الإتفاقيات الدولية والمعاهدات والمواثيق العالمية³، والحق في الحياة الخاصة يحتوي على عدة حقوق مكفولة لأفراد المجتمع للقيام بها، وأي إنقاص من هذه الحقوق

¹ إيمان بن سالم، المرجع السابق، ص 54.

² سالم روضان الموسمي، فعل الإرهاب والجريمة الإرهابية، منشورات الحلبي الحقوقية، بيروت، ط1، 2010، ص235.

³ الإعلان العالمي لحقوق الإنسان المنشور بموجب قرار الجمعية العامة للأمم المتحدة 217 (الف د3). بتاريخ 10 ديسمبر 1948./العهد الدولي الخاص بالحقوق المدنية والسياسية، قرار الجمعية العامة رقم 2200/01 الصادر عن الدورة 21 للجمعية العامة للأمم المتحدة بتاريخ 16 ديسمبر 1966.

يعتبر مساسا بها، و برز خطر حقيقي يهدد الحياة الخاصة للفرد، فأصبح من السهل التسلل إلى خصوصياته والإعتداء عليها، وبالتالي يعد التقدم العلمي والتكنولوجي من أهم الأسباب التي تهدد الحياة الخاصة، بحيث أصبحت حياته بيد الغير دون أن يشعر صاحب الحياة الخاصة بذلك، لذلك تعد نظم المعلومات وسيلة للخوض في الحياة الخاصة للأفراد واتخاذها وسيلة للربح وكذا الإعتداء عليها¹، فكان لزاما على الدول إصدار تشريعات تواجه مثل هذه الإنتهاكات الخطيرة، فجدد المشرع الجزائري تصدى لهذا النوع من الجرائم، الذي يعد تعدي على حرمة الحياة الخاصة، وذلك بالنص على قواعد قانونية تجرم الإعتداء عليها.

لهذا سوف نتطرق الى مفهوم حرمة الحياة الخاصة في (الفرع الاول) ثم نتناول صور الإعتداء عليها في (الفرع الثاني).

الفرع الأول: مفهوم حرمة الحياة الخاصة

لم تتفق القوانين المقارنة على وضع تعريف لمفهوم الحياة الخاصة، ويرجع ذلك إلى صعوبة تحديد العناصر التي تشتمل عليها الخصوصية الفردية، بإعتبار أن هذه العناصر تكمن في الأمور المتعلقة بالإنسان، والتي يريد إحاطتها بستار من الكتمان²، لذلك لا يوجد تعريف جامع مانع متعلق بحق الحياة الخاصة والسبب يعود إلى تغير هذا المفهوم وتطوره باستمرار، تبعا لتغير المفاهيم الإجتماعية والإقتصادية والسياسية والثقافية والدينية، ويعرف بعض الفقه الحياة الخاصة بأنها "السرية وما تحمله من معان يمكن التعبير عنها بعدة ألفاظ منها العزلة والانطواء والخلوة وعدم تدخل الآخرين وغير ذلك من المرادفات".³

وعرفها أيضا آلان نواستن Alen wsiten والذي عبر عنها "بخصوصية المعلومات" بأنها "حق الأفراد في تحديد متى وكيف وإلى أي مدى تصل المعلومات عنه للآخرين"⁴، كما عرفها أيضا الفقيه مارتن بقوله أنها "الحق في الحياة الأسرية والشخصية والداخلية والروحية للشخص عندما يعيش وراء بابه

¹ _لينا محمد الأسدي، المرجع السابق، ص 38.

² _عبد العزيز نويري، الحماية الجزائية للحياة الخاصة، دراسة مقارنة، أطروحة لنيل شهادة دكتوراه علوم، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، الجزائر، 2010-2011، ص 29.

³ _عبد الرحمن خلفي، الحق في الحياة الخاصة في التشريع العقابي الجزائري، دراسة تأصيلية تحليلية مقارنة، مجلة البحوث والدراسات، العدد 12، 2011، ص 155.

⁴ _مفيدة مباركية، الحماية الجنائية للحق في الخصوصية الرقمية في القانون الجزائري، مجلة الشريعة والإقتصاد، المجلد السابع، العدد 13، جوان، 2018م، ص 461.

المغلق"¹، فيما عرفها الفقيه "ميلر" بأنها "قدرة الأفراد على التحكم بدورة المعلومات التي تتعلق بهم ويعتبر الفرد في حالة من الخصوصية إذا كان في حالة من العزلة والألفة والتستر."²

ولهذا كان مفهوم الخصوصية نسبيا وظل كذلك الى حد الآن، لأن ما يعد خاصا في زمان لا يكون كذلك في زمان آخر، وما يمكن أن يكون خاصا في مكان قد لا يكون كذلك في مكان آخر.

وترجع ضرورة منح الفرد خصوصية داخل الفضاء الرقمي نظرا للاستعمالات اللامحدودة لشبكة الأنترنت في الوقت الحاضر، وما نتج عنها عدة إشكالات تخص أمن الحياة الخاصة، فهي شبكة تتيح عمليات جمع وتخزين المعلومات المتعلقة بالأشخاص بأساليب وتقنيات لم تكن معروفة مسبقا بالإضافة إلى أن الأنترنت كشبكة دولية يسهل جمع المعلومات وتحديد مصدرها بدقة مستعينا بعنوانين "IP"³، التي تميز كل حاسوب عن الآخر، كذلك تنامي قدرات وأساليب الهيئات المكلفة بجمع المعلومات الخاصة بالأفراد في إطار عملها على تغذية بنوك المعلومات التي أنشأتها أغلب الدول في العالم بمعلومات تخص نشاط الأفراد على الشبكات⁴.

أما بالنسبة للمشرع الجزائري فقد أخذ بتصور المشرع الفرنسي، الذي يرى أن الحماية المباشرة للحق في الحياة الخاصة تعد مكملة للحماية غير المباشرة، والموجودة قبلها في نصوص قانونية أخرى⁵، لم يعط المشرع تعريفا لحرمة الحياة الخاصة للأشخاص، لكنه اعتبرها من الحقوق اللصيقة بالشخصية، فأعترف بالحق في الحياة الخاصة في كل الدساتير المتعاقبة بداية بدستور 1963⁶ إلى غاية دستور 1996

¹ أسامة عبد الله قايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دار النهضة العربية، القاهرة، 1994، ص 08.

² بولين انطونيوس أيوب، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، دراسة مقارنة، منشورات الحلبي الحقوقية، ط1، 2009م، ص 56.

³ عنوان بروتوكول الأنترنت (adress IP) Address internet Protocol ويعرف أيضا بالعنوان الرباعي المنقذ وهو عنوان رقمي خاص بكل حاسوب يضمن التعريف به على شبكة الأنترنت وتحديد موقعه، يتكون من أربعة مجموعات من الأرقام تفصل بينها نقاط.

⁴ حسين ربيعي، المراقبة الإلكترونية وحقوق الفرد في الخصوصية داخل الفضاء الرقمي، المجلة الأكاديمية للبحث القانوني، المجلد 13، العدد 01، 2016، ص 413.

⁵ - عبد العزيز نويري، المرجع السابق، ص 49.

⁶ نص دستور 1963 في المادة 14 منه أنه "لا يجوز الاعتداء على حرمة المسكن ويضمن حفظ سر المراسلة لجميع المواطنين"، أما دستور 1976 اعترف صراحة بالحقوق في الخصوصية من خلال المادة 49 التي نصت على «لا يجوز انتهاك حرمة حياة المواطن الخاصة ولا شرفه والقانون يصونها». وهو نفس النص الذي أورده المشرع في دستور 1989 في المادة 37. ولكن بتعديل في الصياغة "لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه يحميها القانون".

المعدل بدستور 2016، والذي يؤكد على هذا المبدأ صراحة بموجب المادة 46 منه والتي جاء نصها "لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه، وبحميها القانون سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة" واعتبر الحق في الحياة الخاصة من الحقوق المطلقة.

ولكن النص القانوني الذي له أهمية بالغة، حيث وفر من خلاله المشرع الجزائري حماية جزائية فعلية للمساس بحرمة الحياة الخاصة، وكان ذلك بالقانون رقم 23/06 المؤرخ في 2006/12/23¹ المعدل والمتمم لقانون العقوبات بموجب المواد من 303 مكرر إلى 303 مكرر 3، وهذا ما سوف نتناوله بالدراسة في الفرع الموالي وذلك كالآتي:

الفرع الثاني: صور الاعتداء على حرمة الحياة الخاصة

خص المشرع الجزائري حماية جزائية لحرمة الحياة الخاصة²، للأفراد بموجب نص المواد 303 مكرر إلى 303 مكرر 3.ق.ع.ج، والتي جاءت مطابقة للمواد من 1/226 إلى 226/ق.ع.ف كما أكدت المادة 14 من الإتفاقية العربية لمكافحة تقنية المعلومات على هذه الحماية، والتي جاء نصها كما يلي "الاعتداء على حرمة الحياة الخاصة بواسطة تقنيات المعلومات، " و هذا ما سوف نتناوله بالدراسة والتحليل لمختلف صور هذه الجرائم وذلك كالآتي:

الفقرة الأولى: جريمة التقاط الأحاديث والصور دون رخصة

تنص المادة 303 مكرر من ق.ع.ج على أنه "يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 50.000 دج إلى 300.000 دج كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص، بأية تقنية كانت وذلك:

1- بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية، بغير إذن صاحبها أو رضاه.

2- النقاط أو تسجيل أو نقل صورة الشخص في مكان خاص بغير إذن صاحبها أو رضاه."

³ - القانون رقم 06-23 المؤرخ في 20/12/2006 يعدل ويتمم الأمر 66-156 المتعلق بقانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، عدد 84، الصادرة بتاريخ 2006/12/24.

² - أول تشريع جزائي في الجزائر أورد عبارة الحياة الخاصة هي المادة 27 من القانون رقم 19/04 المؤرخ في 2004/12/20 المتعلق بتنصيب العمال ومراقبة التشغيل حيث نصت هذه المادة على "يعرض إفشاء المعلومات الشخصية التي تمس الحياة الخاصة لطالب التشغيل مرتكبه لغرامة مالية من 50.000 دج إلى 100.000 دج أنظر :عبد العزيز نويري، المرجع السابق، ص31.

وتقابلها المادة 1/226 من ق.ع.ف التي تنص على "يعاقب بعام حبس وغرامة 45000 أورو كل من اعتدى عمداً، وبأي وسيلة كانت على ألفة الحياة الخاصة للغير".

1- بالتصنت أو التسجيل أو النقل بدون موافقة صاحب الشأن كلام صادر له صفة الخصوصية أو سري.¹

يتبين أن النص القانوني الجزائري جاء مطابقاً للنص الفرنسي لكن مع وجود خطأ في الترجمة فيما يتعلق بمصطلح المساس بحرمة الحياة الخاصة، لكن القانون الفرنسي استعمل عبارة بألفة الحياة الخاصة. وباستقراء نص المادة 303 مكرر من ق.ع.ج يمكن تحديد الأركان الواجب توفرها في هذه الجريمة والتي تتمثل فيما يلي:

أولاً: الركن المادي

يتحقق الركن المادي لهذه الجريمة بإحدى صور النشاط الإجرامي الوارد في نص المادة 303 مكرر من ق.ع.ج بالتصنت عن طريق النقاط أو تسجيل أو نقل الأحاديث وأن تكون هذه الأحاديث ذات طابع خاص أو سري، وأن يرتكب باستعمال أية وسيلة تقنية وبدون رضا المجني عليه.

وبما أن المشرع لم يوضح ما المقصود بكل عنصر منها، سنحاول توضيح هذه العناصر، فيقصد بالحديث كل صوت له دلالة معينة صادر من شخص ما متبادل بين شخصين أو أكثر أياً كانت اللغة المستعملة في ذلك.²، كما قام المشرع بتجريم التصنت وتسجيل الأحاديث الصادرة بين شخصين أو أكثر، وكذا النقاط حديث فردي، ويستشف ذلك من العبارة الواردة في نص المادة 303 مكرر من ق.ع.ج المكالمات الصادرة، وهي تشمل الحديث بين الأشخاص أو بين الشخص ونفسه، ويقصد بالنقاط الحصول على الأحاديث الخاصة أو السرية، والإستماع سرا بأي وسيلة كانت أياً كان نوعها إلى كلام له صفة

¹ _Art 226-1 de l'atteinte à la vie privée du c.p.f « est puni d'un an d'emprisonnement et de 45000 euros d'amende le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée .d'autrui :

1-en captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à Titre privée ou confidentiel.

2-en fixant, enregistrant ou Transmettant, sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé.... »

² _عبد الرحمن خلفي، المرجع السابق، ص 172.

الخصوصية أو سري صادر من شخصين أو أكثر دون رضاه¹، أما التسجيل فهو حفظ الحديث على جهاز أو أية وسيلة أخرى معدة لذلك بقصد الاستماع إليها فيما بعد.²

كما يقصد بالتسجيل نقل ذبذبات الموجات الصوتية من مصادرها وخواصها الذاتية بما فيها من عيوب في النطق إلى شريط التسجيل³، بحيث يمكن سماع الصوت للتعرف على مضمونه، ويتم التسجيل بواسطة أجهزه تعتمد على حفظ الإشارات الكهربائية التي تمثل الصوت عند صدوره⁴، أما النقل فيقصد به نقل الحديث الذي تم الاستماع إليه أو تسجيله من المكان الذي يتم فيه الاستماع أو التسجيل إلى مكان آخر، دون اعتبار للوسيلة المستعملة.⁵

لم يحدد المشرع وسيلة معينة بذاتها لإتيان الفعل الإجرامي، بل استعمل مصطلح بأية تقنية كانت، وهذا يؤدي إلى الاتساع في إحتواء كل الوسائل التقنية الحديثة، كأجهزة مراقبة الصوت والصورة مثل كاميرات الفيديو والهاتف النقال، كما تستعمل تقنية البلوتوث Bluetooth أو تقنية shareit... إلخ لنقل هذه الملفات بصورة سريعة⁶، بقصد التطفل على حياة الغير لتحقيق أغراض غير مشروعة مثل فضح ماضي الشخص وابتزازه.⁷

ويشترط لقيام الجريمة كذلك أن يكون الكلام الذي تم التنصت عليه أو تسجيله أو نقله ذا طابع خصوصي وسري، ولقد أخذ المشرع الجزائري بالمعيار الشخصي، الخاص بخصوصية وسرية الحديث أو المكالمة وليس بالمعيار الموضوعي المتعلق بصدور الحديث في مكان خاص، وهو نفس الإتجاه الذي

¹ عبد المالك بن ذياب، حق الخصوصية في التشريع العقابي الجزائري، مذكرة لنيل شهادة الماجستير في العلوم القانونية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2013، ص 98.

² عبد الرحمن خلفي، المرجع السابق، ص 172.

³ محمد رشاد إبراهيم مفتاح، الحماية الجنائية لحق في رجمة الاتصالات الشخصية، أطروحة لنيل شهادة دكتوراه في الحقوق، جامعة الاسكندرية، 2009، ص 94.

⁴ عرف قانون التسجيل والنقصي الأمريكي جهاز التسجيل بأنه "جهاز أو إجراء يتولى تسجيل أو فك شفرة اتصال هاتفي أو مسار أو عنوان أو معلومات إشارية يتم بثها بواسطة أداة أو وسيلة يتم بها بث اتصال سلكي أو إلكتروني. أنظر : محمد رشاد إبراهيم مفتاح، المرجع نفسه، ص 44.

⁵ عبد الرحمن خلفي، المرجع السابق، ص 172.

⁶ يزيد بوحليط، المرجع السابق، ص 156.

⁷ عبد المالك بن ذياب، المرجع السابق، ص 101.

تبناه المشرع الفرنسي في تعديل قانون العقوبات لسنة 1992 بموجب المادة 1/226، إذا فالعبرة ليست بطبيعة المكان وإنما بطبيعة الحديث، وهذا ما أكدته محكمة النقض الفرنسية في بعض أحكامها، فأخذت بمعيار طبيعة الحديث، ففي قضية تتلخص وقائعها في قيام موظف في إحدى الشركات بتسجيل المحادثات التليفونية لصاحب الشركة، ولأن الجهاز وضع داخل المكتب فقد قام بتسجيل محادثات بين مدير الشركة وزوجة صاحب الشركة، وقد رفضت محكمة الإستئناف تطبيق نص المادة 368 ق.ع.ف، تأسيسا على أن المكتب مكان عام ومن ثم نية التعدي على حرمة الحياة الخاصة غير متوافرة، إلا أن محكمة النقض ألغت الحكم الصادر من محكمة الإستئناف على أساس أن الحديث له طبيعة شخصية.¹

ويشترط كذلك لتجريم فعل التنصت أو التسجيل أو النقل للأحاديث الخاصة أن يتم دون رضا المجني عليه، أي دون موافقته الصريحة أو الضمنية.

ثانيا: الركن المعنوي

تعد جريمة إلتقاط أو تسجيل أو نقل المكالمات والأحاديث الخاصة أو السرية من الجرائم العمدية، تتطلب توافر القصد الجنائي بعنصره العلم والإرادة، فيجب أن يعلم الجاني بموضوع الحق المعتقدى عليه واتجاه الإرادة إلى إتيان تلك الأفعال وتحقيق النتيجة.

ثالثا: العقوبة المقررة

عاقب المشرع الجزائري مرتكب هذه الجريمة بعقوبة الحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 50.000 دج إلى 300.00 دج.

كما يجوز توقيع عقوبات تكميلية نصت عليها المادة 303 مكرر 2 المتمثلة في الحظر من ممارسة حق أو أكثر من الحقوق المنصوص عليها في المادة 9 مكرر 1²، من ق.ع.ج لمدة لا تتجاوز خمس سنوات.

¹ _محمد رشاد إبراهيم مفتاح، المرجع السابق، ص 41.

² _تنص المادة 09 مكرر من ق.ع.ج على: العزل أو الإقصاء من جميع الوظائف والمناصب العمومية التي لها علاقة بالجريمة- الحرمان من حق الإنتخاب أو الترشيح ومن حمل اي وسام-عدم الأهلية لأن يكون مساعدا محلفا، أو خبيرا أو شاهدا على أي عقد، أو شاهد أمام القضاء، إلا على سبيل الاستدلال- الحرمان من الحق في حمل الأسلحة، وفي التدريس، وفي إدارة مدرسة أو الخدمة في مؤسسة للتعليم بوصفه أستاذا أو مدرسا أو مراقبا، عدم الأهلية لأن يكون وصيا أو قيما-سقوط حقوق الولاية كلها أو بعضها.

كما قررت المادة 303 مكرر 2 من ق.ع.ج على جواز نشر حكم الإدانة طبقا للكيفيات المبينة في المادة 18 من نفس القانون.

الفقرة الثانية: جريمة إلتقاط أو تسجيل أو نقل الصورة

لقد أعطى المشرع الجزائري أهمية كبيرة لصورة الشخص، واعتبرها من الأمور التي تدخل في دائرة الحياة الخاصة، ففرض حماية جنائية من خطر الحصول على صورته بغير رضاه، عن طريق التقاطها أو تسجيلها أو نقلها بأية تقنية كانت، فنصت المادة 303 مكرر من ق.ع.ج على أنه "يعاقب بالحبس من 6 أشهر إلى ثلاث (3) سنوات وبغرامة من 50000 دج إلى 300.000 دج كل من تعمد المساس بحركة الحياة الخاصة للأشخاص بأية تقنية كانت و ذلك:

2-بالتقاط أو تسجيل أو نقل صورة لشخص في مكان خاص، بغير إذن صاحبها أو رضاه.¹

يتبين من خلال هذا النص أنه يشترط لقيام هذه الجريمة العناصر التالية:

أولاً: الركن المادي

يتحقق الركن المادي لهذه الجريمة قيام الجاني بنشاط إجرامي، يتخذ إحدى الصور المنصوص في المادة السالفة الذكر وهي، الالتقاط التسجيل والنقل لصورة شخص يتواجد في مكان خاص، ودون رضاه وذلك بأية تقنية كانت.

و نقصد بالصورة هي إمتداد ضوئي لجسم الشخص، ولا تعبر عن فكرة ولا دلالة لها غير أنها تشير إلى شخصية صاحبها، ويقصد بها تثبت أو رسم قسمات شكل الإنسان بالضوء على عامة مادته أيا كانت²، إذا يخرج من نطاق الحماية المقررة للصورة، صورة الحيوان أو الشيء، إنما يكتفي بحماية صورة الأشخاص الذين هم على قيد الحياة، بل يمتد حتى إلى الأموات، وهو ما اعترف به القضاء الفرنسي من خلال قضية راشيل الممثلة الفرنسية.³

¹ _تقابلها المادة 1/226 من القانون الفرنسي.

² _ممدوح خليل بحر، حماية الحياة الخاصة في القانون الجنائي دراسة مقارنة، دار النهضة العربية، القاهرة، د ط، ص 445.

³ _النقطة صوراً فوتوغرافية للممثلة الفرنسية الشهيرة راشيل بعد موتها وهي مسجاة على فراش الموت ونشرها في إحدى الصحف، فأقامت أسرتها دعوى قضائية ضد الصحيفة، فأدانت المحكمة الصحيفة وقررت عدم النقاط الصور دون موافقة المتوفاة أو ورثتها مهما كانت شهرتها الفنية لأن ذلك يعد من قبيل المساس بحياتها الخاصة، أنظر :ممدوح خليل بحر، المرجع نفسه، ص164.

فالجريمة تقوم بإحدى الصور الواردة في نص المادة 303 مكرر ق.ع.ج المتمثلة في النقاط صورة الشخص وتعني تثبيت الصورة على مادة حساسة (النيجاتيف)¹، وبمعنى آخر تثبيت الصورة وتركيزها بسرعة خاطفة ثم أخذها عن طريق جهاز معد لذلك²، كآلة التصوير مثلا، فبمجرد إلتقاط الصورة يتحقق الركن المادي للجريمة.

أما التسجيل فيقصد به " حفظ الصورة عن طريق الوسائل المعدة لذلك ككاميرات الفيديو والأقراص المغنطة"، بينما النقل يقصد به " إرسال الصورة مباشرة إلى مكان غير المكان الذي التقطت فيه بحيث يتمكن شخص يوجد في مكان آخر غير المكان الذي يوجد فيه المجني عليه من الاطلاع على صورته، ويستوي أن يكون المكان الذي تنتقل إليه الصورة مكانا عاما أو خاصا.³

لم يحدد المشرع الجزائري وسيلة معينة من أجل التقاط أو نقل الصورة، بل استعمل عبارة بأية تقنية كانت، مما يسمح بالتوسع لتشمل كل ما يستجد من تقدم في صناعة الآلات التصوير، وفي هذا الصدد يرى الفقه أن حصر المشرع النشاط الإجرامي في الإلتقاط أو التسجيل أو النقل، يعني بداهة ضرورة وجود أداة أو آلة، وعليه لا تقوم الجريمة في حالة الرؤية بالعين المجردة كاستراق النظر من ثقب الباب أو من نافذة مفتوحة وكذا الحال بشأن التطفل الذي يتم عن طريق منظار مقرب.⁴

ولتحقق الإعتداء على الحياة الخاصة عن طريق التصوير، اشترط المشرع أن يتم الإلتقاط أو التسجيل أو النقل للصورة في مكان خاص، وقد اختلف الفقه حول تحديد المكان الخاص إلى إتجاهين، يرى الإتجاه الأول الذي يتبنى المعيار الشخصي للمكان الخاص، ويقوم ذلك على رضا الشخص في تحديد طبيعة المكان هل هو عام أو خاص، أما الإتجاه الثاني بإعتباره الإتجاه المؤيد في هذا الصدد، فيرى يجب تعداد صور المكان العام، وخلافه يعد من المكان الخاص ومنه يعد مكانا عاما الشوارع والحدائق والملاعب.⁵

¹ _محمد أمين الخرشة، إبراهيم سلبيات القطاونة، الحماية الجنائية لحرمة الحياة الخاصة في قانون العقوبات الإماراتي، مجلة جامعة الشارقة للعلوم الشرعية والقانونية، المجلد 13، العدد 1، 2016، ص 77.

² _عبد العزيز نويري، المرجع السابق، ص 129.

³ _محمد أمين الخرشة، إبراهيم سليمان القطاونة، المرجع السابق، ص 78.

⁴ _ممدوح خليل بحر، المرجع السابق، ص 445.

⁵ _عبد الرحمن خلفي، المرجع السابق، ص 179.

كما ألزم المشرع أن يكون التقاط وتسجيل ونقل الصورة دون رضا المجني عليه، أي أن رضا المجني عليه يحول دون قيام هذه الجريمة.

ثانيا: الركن المعنوي

تعتبر جريمة التقاط أو تسجيل أو نقل الصورة من الجرائم العمدية، أي يتوافر القصد الجنائي العام المتمثل في العلم والإرادة، فيجب أن يعلم الجاني أنه أتى أفعالا مجرمة بنص المادة 303 مكرر ق.ع.ج، وتوجه إرادته الحرة إلى القيام بتلك الأفعال من دون رضا الشخص صاحب الصورة.

ويرى جانب من الفقه أن هذه الجريمة تتطلب قصدا خاصا بالإضافة إلى القصد الجنائي العام، ويتمثل القصد الخاص في إتجاه إرادة الجاني إلى الإعتداء على حرمة الحياة الخاصة للغير.¹

ثالثا: العقوبة المقررة

إن العقوبة المقررة لجريمة التقاط أو تسجيل أو نقل صورة شخص في مكان خاص، هي العقوبات نفسها المقررة لجريمة التقاط أو تسجيل أو نقل المكالمات أو الأحاديث الخاصة أو السرية، ألا وهي عقوبة الحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 50.000 دج إلى 30.000 دج.

الفقرة الثالثة: جريمة الإحتفاظ أو الوضع أو الإستعمال للتسجيلات أو الصور أو الوثائق

نص المشرع الجزائي على هذه الجريمة بموجب المادة 303 مكرر 1 من ق.ع في فقرتها الأولى على أنه " يعاقب بالعقوبات المنصوص عليها في المادة السابقة كل من احتفظ أو وضع أو سمح بوضع في متناول الجمهور أو الغير أو استخدام بأي وسيلة كانت، التسجيلات أو الصور أو الوثائق المتحصل عليها بواسطة أحد الأفعال المنصوص عليها في المادة 303 مكرر من هذا القانون" فهذا النص مطابقا لنص المادة 226/2، ق.ع.ف لسنة 1992.

إن ما يبرره هذا التجريم هو أن الأشخاص الذين يلتقطون الصور أو يسجلون الأحاديث بدون رضاهم، لا يفعلون ذلك لإرضاء الفضول عندهم، وإنما هدفهم استغلال ما نتج عن هذه الجريمة بالطرق

(1) _Keyser, la protection de la vie privée parle droit du secret de la vie privée, PUAM, paris, 1990, p394.

(2) _Art 226/2 du c.p.f

« Est puni de même peines le fait de conserver, porter à la connaissance du public ou d'un Tiers ou d'utiliser de quelques manière que ce soit un enregistrement ou document obtenu à l'Aide de l'un des actes prévu à l'article 226/1 CP »

المختلفة، ابتداء من النشر بقصد الحصول على ربح مادي أو منفعة، ويرى بعض الفقهاء أن هذه الجريمة تتولد كنتيجة "De conséquence"¹، لذا كان من المنطقي أن يسارع المشرع إلى حماية الحياة الخاصة بتعقيب البواعث الخبيثة لدى الجناة.²

ومن خلال نص المادة السالفة الذكر يمكن تحديد أركان هذه الجريمة.

أولاً: الركن المادي

يتحقق السلوك الإجرامي في هذه الصورة عن طريق الاحتفاظ، الإعلان، الاستعمال، فيقصد بالإحتفاظ إمساك الجاني لتسجيل أو مستند خاص بشخص أو أشخاص آخرين عن قصد مع علمه بمحتوى التسجيل أو المستند³ متى تم الحصول عليها بإحدى الطرق المبينة في المادة 303 مكرر 1، وقد يأخذ الاحتفاظ شكلين قد يكون احتفاظاً بالوثيقة للغرض الشخصي لتلبية تطلبه الشخصي، أو الاحتفاظ لفائدة الغير وهذا الأخير يتلقى الوثيقة سواء بصفته أميناً أو مودع لديه.⁴

أما الإعلان أو النشر، وهو إطلاع أكبر عدد ممكن من الناس على الأخبار، أو الصور أو التعليقات التي تتصل بأسرار الحياة الخاصة أو العائلية للأفراد بمعنى إذاعته وإعلانه.⁵

الاستعمال عبر المشرع عنها بعبارة "استخدم" ويقصد به استخدام التسجيل أو المستند لتحقيق غرض ما، أي النشاط الذي يسعى الجاني من خلاله إلى تحقيق الغاية التي يرغب فيها، ويستوي أن يتم الإستعمال علناً، أو في غير علانية كما لو إطلع الجاني شخصاً واحداً على المستند، أو أسمعته التسجيل وكان ذلك في مكان خاص وطلب إليه عدم إذاعة ما أسر إليه⁶، لم يشر المشرع الجزائري عن التسجيل في غير علنية، مما يفيد عدم استبعاده لهذه الحالة، فالجريمة قائمة سواء تم الإستعمال في علانية أو في غير علانية.

ولكي تقوم الجريمة الواردة في المادة 303 مكرر 1 من ق.ع.ج، يشترط أن تكون أفعال الحفظ أو

¹ _ممدوح خليل بحر، المرجع السابق، ص 460.

² _عبد المالك بن ذياب، المرجع السابق، ص 126.

³ _عبد الرحمن خلفي، المرجع السابق، ص 183.

⁴ _عبد العزيز نويري، المرجع السابق، ص 152.

⁵ _محمد أمين الخرشة، إبراهيم سليمان القطاونة، المرجع السابق، ص 81.

⁶ _ممدوح خليل بحر، المرجع السابق، ص 465.

الإعلان أو الاستعمال على التسجيل أو الصورة أو وثيقة تم الحصول عليها بالطرق المبينة في المادة 303 مكرر.

ثانيا: الركن المعنوي

تعد الجريمة المنصوص عليها في المادة 303 مكرر 1 ق.ع.ج، جريمة عمدية لتوافر القصد الجنائي العام بعنصرية العلم والإرادة، أي علم الجاني بمصدر الحصول على التسجيل أو الصور أو الوثيقة، وأن إعلانه لها يشكل جريمة، كما تتجه إرادته إلى إذاعة التسجيل أو الوثيقة أو تسهيل إذاعته أو استعماله، ولا تتطلب الجريمة قصدا جنائيا خاص، بل تكتفي بالقصد الجنائي العام وهذا ما أكدته غالبية الفقهاء بعكس ما ذهب إليه الفقيه شافان chavanne الذي يرى بوجود قصد خاص يتمثل في نية الإضرار بالحياة الخاصة للأشخاص.¹

ثالثا: العقوبة المقررة

عقوبة الحبس من ستة (6) أشهر إلى ثلاث (3) سنوات بغرامة من 50.000 دج إلى 300.000 كما تعاقب على الشروع بنص المادة 303 مكرر 3/1... يعاقب على الشروع في إرتكاب الجناية المنصوص عليها في هذه المادة بالعقوبات المقررة للجريمة التامة، ويضع صفح الضحية حدا للمتابعة الجزائية، إلى جانب تطبيق عقوبات تكميلية نصت عليها المادة 303 مكرر 2 ق.ع.ج "يجوز للمحكمة أن تحظر على المحكوم عليه من أجل الجرائم المنصوص عليهما في المادتين 303 مكرر-303 مكرر 1 ممارسة حق أو أكثر من الحقوق المنصوص عليها في المادة 09 مكرر 1 لمدة لا تتجاوز خمس (5) سنوات، كما يجوز لها أن تأمر بنشر حكم الإدانة طبقا للكيفيات المبينة بالمادة 18 من هذا القانون، ويتعين دائما الحكم بمصادرة الأشياء التي استعملت لإرتكاب الجريمة.

كما يعاقب الشخص المعنوي طبقا لنص المادة 303 مكرر 3 حيث يكون الشخص المعنوي مسؤولا جزائيا عن الجرائم المحددة في الأقسام 3 و4 و5 من هذا الفصل وذلك طبقا للشروط المنصوص عليها في المادة 51 مكرر وتطبق على الشخص المعنوي عقوبة الغرامة حسب الكيفيات المنصوص عليها في المادة 18 مكرر، وفي المادة 18 مكرر 2 عند الاقتضاء، يتعرض أيضا لواحدة أو أكثر من العقوبات التكميلية المنصوص عليها في المادة 18 مكرر.

¹ - عبد الرحمان خلفي، المرجع السابق، ص186.

وخلاصة القول نرى أن النصوص الواردة في المواد 303 مكرر الى 303 مكرر 3 هي نصوص صارمة تردع كل شخص يريد المساس بحرمة الحياة الخاصة للأشخاص، لقد وفق المشرع الجزائري في حمايته الجزائية لحرمة الحياة الخاصة، لكن رغم ذلك لم تشمل هذه الحماية كافة عناصر الحق في حرمة الحياة الخاصة منها المعطيات ذات الطابع الشخصي خاصة بعد ظهور ما يعرف ببنوك المعلومات، مما جعل المشرع يستدرك الأمر بسن نصوص تحمي هذا الحق متمثل في القانون رقم 07/18، كما أن تطبيق النصوص الواردة في قانون العقوبات المتعلقة بحماية حرمة الحياة الخاصة ليست مطلقة، فقد تغلب مصلحة المجتمع على مصلحة الفرد، فقد ترد استثناءات بأن تخرج بعض الأفعال من دائرة التجريم إلى دائرة الإباحة، أي قيود واردة على تجريم المساس بالحق في الخصوصية وهذا ما سوف نتطرق إليه في الباب الثاني من الدراسة.

المطلب الخامس: الإستغلال الأطفال في المواد الإباحية عبر شبكة الأنترنت

أدى ظهور الأنترنت وانفتاحها على المستوى العالمي، إلى أن أصبحت ساحة مفتوحة لارتكاب العديد من الجرائم، ومنها الجرائم المخلة بالآداب العامة والأخلاق¹، ولعل أكثرها انتشارا في الوقت الحالي تلك التي تطل فئة عمرية معينة تحظى بالحماية والرعاية القانونية من طرف التشريعات، ألا وهي فئة القاصرين وفي ظل التقنية الحديثة كثرت المواقع المشبوهة، وازدادت خطورتها على الأطفال، فيتم استدراجهم لحثهم على الفسق والرذيلة، وظهرت الجرائم الجنسية ممثلة في المواقع الإباحية، والتحرير على الدعارة والدعاية للشذوذ الجنسي واستغلال الأطفال جنسيا² فبعض التقارير الدولية تشير إلى أن حوالي 2 مليون طفل غالبتهم فتيان يتعرضون للاستغلال الجنسي، وأزيد من 100 ألف موقع إباحي يعرض صورا لاستغلال القصر³، وأمام هذا الخطر الذي يهدد الأطفال تدخلت العديد من الدول إلى سن

¹ يقصد بالآداب العامة "مجموعة القواعد الأخلاقية الأساسية والتي تكون غايتها حفظ النظام في المجتمع أو هي ما تعارف عليه الناس من خروج على الاحتشام مما تخرج رؤيته أو سماع شعور الجمهور، كالصور والأفلام وغيرها.... أيا كانت درجة الفحش الذي تمثله أو تتطوي عليه، أنظر جميل عبد الباقي الصغير، قانون العقوبات، القسم الخاص، در النهضة العربية، القاهرة، د ط، 1998، ص 128.

² عادل عبد العال إبراهيم، جرائم الإستغلال الجنسي للأطفال عبر شبكة الأنترنت وطرق مكافحتها في التشريعات الجنائية والفقهاء الجنائي الإسلامي، كلية الشريعة والقانون، جامعة الأزهر، 2013، ص 1099.

³ يوجد موقع يعرف بموقع "أرض العجائب" وهو نادي لكسب العضوية فيه يجب أن يقدم الراغب بالانضمام إليه ما يقل عن 10 آلاف صورة إباحية عن الأطفال، ففي بريطانيا جرت سنة 2001 محاكمة علنية لسبعة أشخاص أعضاء في هذا

التشريعات التي جرمت هذا الأسلوب المستحدث من الجرائم ومن بينها المشرع الجزائري، لذا سوف نتطرق إلى مفهوم جريمة الاستغلال في المواد الإباحية (الفرع الأول) وموقف المشرع الجزائري من هذه الجريمة (الفرع الثاني) وصور استغلال الأطفال في المواد الإباحية (الفرع الثالث).

الفرع الأول: مفهوم جريمة الاستغلال في المواد الإباحية¹.

لم يتضمن التشريع الجزائري أي تعريف للمواد الإباحية للأطفال غير، أنه بالرجوع إلى أحكام البرتوكول الاختياري لاتفاقية حقوق الطفل بشأن بيع الأطفال واستغلال الأطفال في البغاء وفي المواد الإباحية²، والتي انضمت إليها الجزائر وصادقت عليها، فعرفت المواد الإباحية للأطفال بموجب المادة 2 ف ج بأنها " تصوير أي طفل بأي وسيلة كانت، يمارس ممارسة حقيقية أو بالمحاكاة أنشطة جنسية صريحة أو أي تصوير للأعضاء الجنسية للطفل ولإشباع الرغبة الجنسية أساسا"، كما عرفت إتفاقية بودابست لمكافحة الجريمة الإلكترونية في الفقرة الفرعية (أ) من الفقرة 2 من المادة التاسعة منها مصطلح "المواد الإباحية المستغلة للأطفال" بأنه " أي مواد إباحية تصور بطريقة مرئية قاصرا يسلك سلوكا جنسيا فاضحا"³، وقد حددت هذه الإتفاقية ثلاثة صور، إما أن تكون مرتبطة بضرورة بوجود إعتداءات جنسية واقعية على الطفل، أو تكون متعلقة بصور مركبة كلياً أو جزئياً، وتتمثل في استبدال الوجه الأصلي للشخص الذي يظهر في الصورة بوجه طفل، أما الصورة الثالثة حيث يظهر فيها أشخاص راشدون

النادي، وخلال التحقيق صادر رجال الشرطة 750 ألف صورة إباحية و1800 شريط فيديو بصور أطفالاً في اوضاع إباحية، وتم التعرف على 236 طفلاً منهم، انظر رشا خليل عبد، جرائم الاستغلال الجنسي للأطفال عبر الأنترنت، مجلة الفتح، العدد 27، 2006، د.ص منشور على الرابط: www.lasjnet/iasj?func=fullrextald=17183 أطلع عليه يوم 2018/03/27 على الساعة 14:00.

¹ تستعمل مجموعة من المصطلحات لتعريف استغلال الأطفال في المواد الإباحية وهي استغلال الأطفال في إنتاج المواد الإباحية والميل الجنسي للأطفال، والمواد الإباحية المستغلة للأطفال، والمواد الإباحية المتعلقة بالأحداث، والمواد الإباحية القائمة على المحاكاة، والمواد الإباحية بالحاسوب، وإنتاج الإباحية والاعتداء الجنسي عبر شبكة الأنترنت وغيرها من المصطلحات.

² اعتمد هذا البرتوكول من طرف الجمعية العامة للأمم المتحدة بالقرار رقم 54/263 المؤرخ في 25 ماي 2000 دخل حيز التنفيذ في 18 جانفي 2002 صادقت الجزائر عليه هذا البرتوكول بموجب المرسوم الرئاسي 06-299 بتاريخ 2 سبتمبر 2006، ج ر عدد 55 الصادرة بتاريخ 6 سبتمبر 2006.

³ عبد اللاه أحمد هلال، إتفاقية بودابست معلقاً عليها، المرجع السابق، ص 12.

بمواصفات جسدية طفولية تجعل المشاهد يعتقد أنهم أطفال.¹

وما يمكن ملاحظته أن هذه التعاريف تفيد إلى نفس المعنى، وما تجدر الإشارة إليه كذلك إلى أن مفهوم استغلال الأطفال في المواد الإباحية يختلف عن مفهوم استغلال الأطفال جنسيا، الذي يقصد به الاتصال بين شخص بالغ وطفل قاصر لإرضاء الرغبات الجنسية لدى الشخص البالغ، الذي يستخدم القوة للسيطرة على الطفل، وعليه يمثل استغلال الطفل في المواد الإباحية أحد صور الاستغلال الجنسي للأطفال.²

الفرع الثاني: موقف المشرع الجزائري

أولى المشرع الجزائري أهمية خاصة للطفل، تجسدت من خلال إقراره نصوص تجرم الإعتداءات التي تقع عليه، وإزاء الانتشار الواسع لهذا النوع المستحدث من الجرائم، مع قصور النصوص القانونية الواردة في قانون العقوبات الجزائري، فمعظم نصوصه³، غير صالحة لمواجهة جريمة الاستغلال للأطفال في المواد الإباحية، وفي إطار مشاركة الجزائر للمجتمع الدولي جهوده لمكافحة الجرائم الواقعة على الأطفال، صادقت على العديد من اتفاقيات الدولية والبروتوكولات والمواثيق ذات الصلة بمجال حماية حقوق الأطفال ومكافحة استغلالهم في البغاء والمواد الإباحية.⁴

مما دفع بالمشرع الجزائري من أجل تعديل قوانينه كصدور قانون حماية الطفل⁵ الذي يجرم جميع أنواع الاستغلال الجنسي بما فيها الاستغلال الذي يتم عبر الأنترنت، وكذلك تعديل قانون العقوبات لسنة

¹ _ عادل عبد العال إبراهيم، المرجع السابق، ص 1117.

² _ نصيرة بن تركية، استغلال الطفل في المواد الإباحية ما بين الخطر الدولي والتجريم الوطني، المجلة الجزائرية للحقوق والعلوم السياسية، العدد 4، 2017، ص 246.

³ _ أنظر المواد 334 و 2/335 المتضمنة الأفعال المخلة بالحياء ضد قاصر، بالإضافة إلى القسم السابع من قانون العقوبات المتضمن تحريض القصر على الفسق والدعارة المواد 342-344.

⁴ _ صادقت الجزائر على اتفاقية الطفل 1989 بموجب المرسوم الرئاسي رقم 92-461 المؤرخ في 19/12/1992 الجريدة الرسمية للجمهورية الجزائرية، عدد 91، كما صادقت على البروتوكول الاختياري الملحق باتفاقية حقوق الطفل المتعلق بشأن بيع الأطفال واستغلالهم في البغاء وفي المواد الإباحية لسنة 2002 بموجب المرسوم الرئاسي رقم 06-299 بتاريخ 2 سبتمبر، الجريدة الرسمية للجمهورية الجزائرية، عدد 55 الصادر بتاريخ 06/09/2006.

⁵ _ القانون رقم 15-12 المؤرخ في 15 يوليو 2015 المتعلق بحماية الطفل، الجريدة الرسمية للجمهورية الجزائرية، عدد 39 الصادرة بتاريخ 19 يوليو 2015.

2014¹ حيث أضاف المادة 333 مكرر 1 للقسم السادس "انتهاك الآداب العامة، من الباب الثاني الجنائيات والجناح ضد الأفراد" والتي تنص على "كل من صور وبأي وسيلة كانت قاصرا لم يكمل 18 سنة وهو يمارس أنشطة جنسية بصفة حقيقية أو غير حقيقية، أو صور الأعضاء الجنسية لقاصر لأغراض جنسية، أو قام بإنتاج أو توزيع أو نشر أو ترويج أو استيراد أو تصدير أو عرض أو بيع أو حيازة مواد إباحية متعلقة بالقصر".²، وباستحداث المشرع لنص خاص يعاقب على هذه الجريمة³، تعتبر خطوة جبارة لمنح حماية أكثر للأطفال خاصة مع تزايد الإجرام المعلوماتي، وسد الفراغ التشريعي حتى لا يفلت مجرمو المعلوماتية من العقاب⁴، والملاحظ أن المشرع لم يحدد الوسيلة المستعملة في هذه الجريمة وترك المجال واسعا ليشمل الوسائل الإلكترونية، لكن كان على المشرع أن يكون أكثر دقة ووضوحا في هذه المسألة، ومع ذلك نجده قد وفق في تحديد كل صور الجرائم الإباحية، كما شدد من العقوبة كون الضحية قاصرا.

الفرع الثالث: صور الاستغلال الجنسي

استحدث قانون العقوبات مادة جديدة في موضوع استغلال الأطفال في المواد الإباحية، وهي المادة 333 مكرر 1 التي جاء فيها " يعاقب بالحبس من خمس (5) سنوات إلى عشر (10) سنوات وبغرامة من 500.000 دج إلى 1.000.000 دج كل من صور قاصرا لم يكمل سن 18 سنة بأي وسيلة كانت وهو يمارس أنشطة جنسية بصفة مبنية حقيقية أو غير حقيقية أو صور الأعضاء الجنسية للقاصر لأغراض جنسية أو قام بإنتاج أو توزيع أو نشر أو ترويج أو استيراد أو تصدير أو عرض أو بيع أو حيازة مواد

¹ _ القانون رقم 01/14 المؤرخ في 2014/02/04 يعدل ويتم الأمر رقم 156/66 المتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، عدد 7 الصادرة بتاريخ 2014/02/16.

² _ وهو تقريبا نفس التعريف الذي جاء به البرتوكول الاختياري لاتفاقية حقوق الطفل بشأن بيع الاطفال واستغلال الاطفال في البغاء وفي المواد الاباحية.

³ _ كشفت دراسة مسحية أن 33 % من الاطفال مستعملي الانترنت في الجزائر تلقوا عروضاً استغلالية من شبكات إجرامية ومنظمات عالمية مختصة في الدعارة والمتاجرة بالأطفال عبر شبكة الانترنت، في حين أثبتت دراسة علمية أخرى أن 65 % من الشباب الجزائري مدمن على المواقع الإباحية، أنظر مولود صياد، مقال بعنوان 65 بالمائة من المراهقين الجزائريين مدمنون على المواقع الإباحية، جريدة الحوار منشور على الموقع: <https://www.elhiwardz.com/rational/> أطلع عليه يوم 2019/02/17 على الساعة 14.00

⁴ _ نجاة بن مكي، محمود بوقطف، حماية الأطفال من الإستغلال الجنسي عبر الأنترنت، مجلة الدراسات والبحوث القانونية المجلد 2، العدد 3، 2017، ص17.

إباحية تتعلق بالقصر".

وتتحقق هذه الجريمة بتوافر أركانها المتمثلة في الركن المادي والركن المعنوي وعقوبة مقررة لها.

أولاً: الركن المادي

يتخذ الركن المادي في هذه الجريمة بإتيان الجاني أحد الصور المنصوص عليها في المادة 333 مكرر 1 من ق.ع.ج وتوجد في الآتي:

- تصوير قاصر يمارس نشاطاً جنسياً أو تصوير أعضائه الجنسية، ويقصد بها قيام الجاني بتصوير الأطفال في وضعية جنسية وعرضها عبر شبكة الأنترنت، أو إرسال لصور أطفال تتضمن صوراً إباحية لأشخاص آخرين عبر الوسائل والشبكات الإلكترونية¹، أو يمكن تصوير شريط فيديو لطفل في وضعيات جنسية فاضحة، سواء كانت لطفل حقيقي يمارس نشاط جنسي لوحده أو مع شخص بالغ أو قصراً مع بعضهم²، ويستوى أن يكون تصوير الأطفال بأوضاع جنسية على أطفال غير حقيقيين أي صور مزيفة غير حقيقية أي أن تكون هذه الصور عبارة عن مستخلص من أجزاء عديدة من الصورة يتم تجميعها مع بعضها لتكوين صورة واحدة الأمر الذي يشكل اعتداء على الطفولة واعتداء على ملكية الشخص لصورته³.

إنتاج أو توزيع أو نشر أو ترويج أو استيراد أو تصدير أو عرض أو بيع أو حيازة مواد إباحية للقاصر فقد يقوم الجاني بفعل إنتاج مواد إباحية بالاستعانة بأحد البرامج المتوفرة عبر شبكة الأنترنت⁴.

أما البيع فيعني قيام الجاني بنقل ملكية تلك المادة الإباحية المتعلقة بالقاصر، إلى الغير مقابل ثمن كبيع لوحاته الزيتية المتضمنة لرسومات إباحية للأطفال، عبر عرض صور عنها على الموقع الإلكتروني للجاني لأحد الزبائن الزائرين، فيما يقصد بالتوزيع تسليم تلك المواد إلى أشخاص ما⁵.

¹ نصيرة بن تركية، المرجع السابق، ص 252.

² حنان بن عزيزة، أثر استعمال الأنترنت في تنامي جرائم الاستغلال الجنسي للأطفال، المجلة المتوسطية للقانون والاقتصاد، المجلد 2، العدد 2، 2017، ص 223.

³ رشا خليل عبد، المرجع السابق، ص 61.

⁴ عثمان طارق، حماية الأطفال من الاستغلال في المواد الإباحية عبر الأنترنت في التشريع الجزائري، مجلة المفكر، العدد 13، ص 428.

⁵ حنان بن عزيزة، المرجع السابق، ص 224.

أما الحيازة فيقصد بها السيطرة المادية على الشيء المخل بالحياء سواء بصفته مالكا أو مستأجرا¹، وتتحقق الحيازة كأن يضبط في منزله المواد الإباحية مثلا في جهازه الإلكتروني أو موقعه الإلكتروني، وهذا ما قضت به محكمة مراكش على سائح فرنسي، بأربع سنوات حبسا بإرتكابه لجريمة حيازة وتوزيع أفلام خاصة باستغلال الجنسي للأطفال والتي تحتوي على 17.000 صورة إباحية، وكذا حيازته على 140.000 فيلما والتي قام بإرسالها عبر حاسوبه الخاص نحو مواقع إباحية.²

لم يشر المشرع بإرتكاب جريمة الإستغلال الجنسي عبر الأنترنت، وإنما استعمل مصطلح "بأي وسيلة كانت" مما يسمح بإحتواء كل الوسائل الإلكترونية الحديثة كالأنترنت، و كذا إستعمال الجاني آلة التصوير أو الهاتف النقال أو لوائح إلكترونية.

ثانيا: الركن المعنوي

تعتبر هذه الجريمة من الجرائم العمدية، بتوافر القصد الجنائي العام والذي يقوم على توافر عنصري العلم والإرادة، أي علم الجاني بأن سلوكه المتمثل في تصوير القاصر وهو يمارس أنشطة جنسية أو تصوير أعضائه، مع علمه أن الضحية طفل لم يتجاوز 18 سنة إلى جانب اتجاه إرادته إلى تحقيق النتيجة الإجرامية.

ثالثا: العقوبة المقررة للجريمة

كيف المشرع الجزائري جريمة استغلال الطفل في المواد الإباحية على أنها جنحة، وعاقب عليها بالحبس من خمس سنوات إلى عشر سنوات، بالإضافة إلى غرامة مالية تتراوح ما بين 500000 دج إلى 100000 دج.

وفي حالة الإدانة يمكن للقاضي الحكم بعقوبة تكميلية، ممثلة في مصادرة الوسائل المستعملة في ارتكاب الجريمة والأموال المتحصل عليها بصفة غير مشروعة، مع مراعاة حقوق الغير حسن النية.

وفي الأخير يمكن القول بالرغم ما تمثله المادة 333 مكرر 1 من ق.ع.ج من أهمية في حماية الطفل من الاستغلال في المواد الإباحية، إلا أن المشرع الجزائري لم يتدخل جديا لمواجهة هذا النوع من

¹ _عثمان طارق، المرجع السابق، ص 428.

⁽²⁾ _Ali azouzi, la cybercriminalité au Maroc, Bishop solutions, Casablanca, Maroc, 1^{er} édition, 2010, p82.

الجرائم كما واجهته بعض التشريعات المقارنة، كعقابها على التنزيل والاطلاع للمواد الإباحية المتعلقة بالأطفال، الأمر الذي يستدعي سن قواعد قانونية تعاقب صراحة وبصفة مباشرة جريمة الاستغلال الجنسي للأطفال عبر شبكة الأنترنت وتكون أحكامها رادعة، كما أغفل المشرع كذلك مسؤولية مزودي خدمات الأنترنت في حال تواطؤهم مع الأشخاص المستغلين، لما لهم دور كبير في حجب المواقع الإباحية لذا ندعو المشرع اعتباره شريكا في الجريمة مع تشديد العقوبة في هذه الجرائم، علما أن المشرع الجزائري أقر المسؤولية الجنائية لمزودي الأنترنت من خلال المادة 394 مكرر 8 من ق.ع.ج.

ولإرساء سياسة فعالة وناجحة، لم يكتف المشرع الجزائري مواجهة الجريمة الإلكترونية بقواعد عامة، وإنما دعمها بنصوص خاصة، حتى لا يفلت الجاني من العقاب وهذا ما نقوم بدراسته في المبحث الموالي.

المبحث الثاني: مواجهة الجريمة الإلكترونية بموجب قوانين خاصة

لما كانت الجريمة الإلكترونية ذات طبيعة خاصة وامتداد أثرها إلى بعض القوانين الخاصة لا يمكن أن يشملها قانون العقوبات بالحماية الكاملة والتصدي لها، واصل المشرع الجزائري سياسته الجنائية لسد الفراغ التشريعي في مجال الإجرام المعلوماتي، فبعد أن خص بعض الجرائم في قانون العقوبات التي تناولناها بالدراسة في المبحث الأول، استحدثت نصوص تجريبية خاصة لردع هذا النوع من الإجرام، سوف نتناول أهم الجرائم الواردة في مختلف القوانين الخاصة منها الجرائم الواقعة على الملكية الفكرية (المطلب الأول) والتوقيع الإلكتروني (المطلب الثاني) وجرائم الإعتداء على المعطيات الشخصية (المطلب الثالث) والجرائم الواقعة على التجارة الإلكترونية (المطلب الرابع) .

المطلب الأول: جرائم الاعتداء على الملكية الفكرية

مع تقدم عصر الثورة المعلوماتية، ظهرت إشكالات تتعلق بالتعامل مع نوع جديد من أنواع الملكية الفكرية يمكن وصفها بالملكية الرقمية، وهي تلك الملكية التي ترد على برامج الحاسب الآلي وبياناته والمصنفات الرقمية المنشورة على شبكة الأنترنت، التي بدل في إنتاجها وجمعها وإظهارها جهدا فكريا إبداعيا جعل من الواجب حمايتها، كحق ملكية فكرية أو جماعية صاحبها كمؤلف، إن مسيرة التحول نحو مجتمع المعلومات تقتضي السماح للأفراد بالنفاذ إلى هذه المعلومات مع كفالة حماية حقوق المؤلفين

بمظاهر حماية حديثة تشمل الملكية الرقمية.¹

وتعد المصنفات الرقمية من قبيل الأموال المعلوماتية المشمولة بالحماية ضد التعدي، بإعتبارها ملكا لصاحبها ولا يحق لسواه استغلالها بهدف الانتفاع بها، مما دفع بضرورة الحماية القانونية لكثرة الاعتداءات الواقعة على المصنف الرقمي²، من خلال هذا المطلب نتطرق إلى مفهوم المصنف الرقمي (الفرع الأول) وصور الجرائم الواقعة على هذه المصنفات في (الفرع الثاني).

الفرع الأول: مفهوم المصنف الرقمي

أظهر استخدام الأنترنت مشكلات قانونية متعددة تتعلق بكيفية حماية المصنفات المنشورة إلكترونيا، فأصبحت هذه الأخيرة تستخدم على نطاق واسع في نشر وتسويق المصنفات الرقمية، لذا لابد أولا من تعريف هذا المصطلح المتمثل في المصنفات الرقمية (الفقرة الأولى) وذكر أنواع المصنفات الرقمية (الفقرة الثانية).

الفقرة الأولى: تعريف المصنفات الرقمية

المصنفات الرقمية هي نتاج التطور التقني للحاسب الآلي وتقنياته، بدأت بواحد ظهورها إلى الوجود مع منتصف السبعينات من القرن العشرين، عرفها بعض الفقه بأنها " تعتبر الوسيلة التقنية التي تسمح بنقل المعلومة من ظاهرة محسوسة إلى ظاهرة تدرك بواسطة أرقام وفق الترقيم المزدوج (0.1)"، كما عرفت أيضا على " أنها تشمل أي إبداع عقلي من بيئة تكنولوجيا المعلومات"³ ويعرف بأنه " كل مصنف إبداعي عقلي ينتمي إلى بيئة تقنية المعلومات، فبرنامج الحاسب الآلي من حيث البناء والأداء مصنف رقمي، وقاعدة البيانات وطبوغرافيا الدوائر المتكاملة مصنفات رقمية ناتجة عن تطور علم الحوسبة، بخلاف أسماء النطاق وعناوين البريد الإلكتروني وغيرها ارتبط بظهور شبكة الأنترنت."⁴

أما بالنسبة للمشرع الجزائري وعبر الأمر 03-05 المؤرخ في 2003/07/19 المتعلق بحقوق المؤلف

¹ - عبد الله عبد الكريم عبد الله، ا لحماية القانونية للملكية الفكرية على شبكة الأنترنت، المرجع السابق، ص249.

² - عبد الرحمان خلفي، الحماية الجزائية لحقوق المؤلف والحقوق المجاورة، منشورات الحلبي الحقوقية، بيروت، ط1، 2007، ص 35.

³ - محمد أحمد عيسى، حماية حقوق الملكية الفكرية للمصنفات الرقمية في ظل القانون الدولي، مجلة جامعة الملك عبد العزيز، عدد7، 2020، ص65.

⁴ - يوسف مسعودي، النظام القانوني لحماية المصنفات الرقمية، مجلة الدراسات القانونية، عدد 04 2009، ص113.

والحقوق المجاورة¹، لم يعط تعريفا صريحا للمصنف وإنما اكتفى بذكر أنواع المصنفات المحمية على سبيل المثال لا الحصر، ويستشف هذا من الفقرة الثانية من المادة 3 من هذا الأمر والتي تنص على " تمنح الحماية مهما يكن نوع المصنف ونمط تعبيره ودرجة استحقاقه ووجهته، بمجرد إيداع المصنف سواء أكان المصنف مثبتا أولا بأية دعامة تسمح بإبلاغه للجمهور."، مما يفهم من العبارة الأخيرة أن المصنفات الرقمية مشمولة بالحماية بموجب هذا القانون، وبالمقابل نجد بعض التشريعات عرفت المصنف كالمشرع المصري الذي عرفه بأنه " كل عمل مبتكر أدبي أو فني أيا كان نوعه أو طريقة التعبير عنه وأهميته أو الغرض من تصنيفه."²

إذا فالمصنفات الرقمية بحقيقتها ليست نوعا جديدا أو طائفة جديدة من المصنفات، وإنما هي طريقة جديدة للتعبير عن المصنفات باستخدام الأرقام (0.1)، بحيث يتم التعبير بشكل رقمي³، ومن ثم فإن أي مصنف إبداعي مبتكر ينتمي إلى بيئة تقنية المعلومات يعد مصنفا رقميا، متى اشتمل على إبداعات الذهن البشري.⁴

الفقرة الثانية: أنواع المصنفات الرقمية

يمكن أن نميز بين طائفتين من المصنفات الرقمية، فئة ترتبط مباشرة بنظام وتقنيات الحاسب الآلي، وفئة ثانية ارتبط ظهورها بشبكة الأنترنت.

أولا: المصنفات المرتبطة بنظام الحاسب الآلي

وتتمثل هذه المصنفات في برامج الحاسب الآلي، قواعد البيانات والدوائر المتكاملة.

1- برامج الحاسب الآلي

تعد برامج الحاسب الآلي أول وأهم المصنفات الرقمية التي حظيت باهتمام كبير، من حيث وجوب الاعتراف بها وتوفير الحماية القانونية لها، والبرمجيات هي الكيان المعنوي لنظام الحاسب الآلي، دونها

¹ - أمر رقم 03-05 المؤرخ في 2003/07/19 يتعلق بحقوق المؤلف والحقوق المجاورة، الجريدة الرسمية للجمهورية الجزائرية، عدد 44 الصادر بتاريخ 2003/07/23.

² - المادة 138 من قانون حماية الملكية الفكرية المصري رقم 82 المؤرخ في 2002/06/20.

³ - فتحية حواس، حماية المصنفات الرقمية وأسماء النطاق على شبكة الأنترنت، أطروحة لنيل شهادة الدكتوراه في القانون، كلية الحقوق، جامعة الجزائر 1، 2016، ص 16.

⁴ - محمد أحمد بن عيسى، المرجع السابق، ص 66.

لا يكون ثمة أي فائدة للمكونات المادية من الأجهزة، لذلك فإن مطلع السبعينيات شهد جدلا واسعا حول حماية برامج الحاسب الآلي فهي تتطوي ضمن قوانين براءة الاختراع بوصف البرنامج من المصنفات القابلة للاستثمار في حقل صناعة الحواسيب أم أنها تصنف ضمن تشريعات حق المؤلف؟

أ- حماية برامج الحاسب الآلي وفقا لنظام براءة الاختراع

تعرف براءة الاختراع على أنها "شهادة تمنحها الدولة ويتمتع صاحبها احتكار استغلال اختراعه لمدة معينة وبمعايير معينة هي وثيقة تسلم لحماية الاختراع"¹، فيما عرف المشرع الجزائري الاختراع بموجب المادة 02 من الأمر 03-07² يتعلق ببراءة الاختراع، على أنه " فكرة لمخترع تسمح عمليا بإيجاد حل لمشكل محدد في مجال التقنية، " وباعتبار برامج الحاسب الآلي ذات أهمية وما تشكله من استثمار إقتصادي، فهناك محاولات لحمايتها بواسطة أحكام براءة الاختراع على أساس أن كل ابتكار جديد قابل للتطبيق الصناعي³، إذ يجب لتطبيق أحكام براءة الاختراع على المنتج وجب توافر شرطي الابتكار والجدة، والقابلية للتطبيق الصناعي، وما يجب تأكيده أن مختلف التشريعات لم تدرج برامج الحاسب الآلي ضمن الابتكار التي تمنح براءات إختراع، إذا خلصت إلى استنتاج مفاده أن برامج الحاسوب الآلي غير مؤهلة لتكون محلا لبراءة الاختراع⁴، بسبب التعارض بين طبيعة البرامج كعامل ذهني مهمته معالجة

¹ - زيدان زبيحة، المرجع السابق، ص 90.

² - الأمر رقم 03-07 المؤرخ 2003/07/19 يتعلق ببراءة الاختراع، الجريمة الرسمية للجمهورية الجزائرية، عدد 44 الصادر بتاريخ 2003/07/23.

³ - حنان مناصرية، الحماية القانونية لبرامج الحاسب الآلي بين التشريع الجزائري والاتفاقية الدولية، مجلة الباحث للدراسات الأكاديمية، المجلد 06، عدد 01، 2019، ص 782.

⁴ - أول قضية من نوعها عرضت على المحكمة العليا الأمريكية حول برامج الحاسب الآلي ومدى إمكانية منحها براءة اختراع، وعرفت بقضية بنسن Benson-software pre، فقد قضت المحكمة بعدم أحقية أو أهلية برامج الحاسب الآلي بالإبراء، ويصب هذا القرار حول مدى إمكانية حماية برامج الحاسب الآلي، بنظام براءة الاختراع، وذات الاتجاه الذي ذهب إليه الديوان الأمريكي لبراءة الاختراع العلامات التجارية "UPSTO" الذي قضى هو الآخر بعدم أحقية برامج الحاسب الآلي بالحماية بموجب نظام براءة الاختراع ردا منه على بعض الطلبات الواردة له من قبل بعض معدي هذه البرامج ومسببا رأيه بخلو هذه البرامج من أية مصلحة نفعية" بالإضافة إلى غياب السند القانوني الذي يقضي بحماية برامج الحاسب الآلي عموما بنظام براءة الاختراع أنظر: أسامة بن يطو، حماية برامج الحاسب الآلي بين نظامي حقوق المؤلف وبراءة الاختراع، مذكرة لنيل شهادة الماجستير في الحقوق، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2015، ص 48.

البيانات والمعلومات، وبين النظام القانوني لمنح براءة الاختراع¹، لذلك تم إستبعاد أحكام براءة الاختراع كوسيلة قانونية لحماية برامج الحاسب الآلي، وهو ما ذهب إليه المشرع الجزائري بحيث استبعد برامج الحاسب الآلي صراحة من نطاق الحماية بواسطة قانون براءة الاختراع وذلك طبقا للمادة 07 من الأمر 07-03 المؤرخ في 2003/07/19 "لا تعد قبيل الاختراعات في مفهوم هذا الأمر... برامج الحاسوب..."

ومن هذا المنطلق يمكننا القول أن المشرع الجزائري قد تبني نظام حق المؤلف كبيئة لحماية برامج الحاسب الآلي وهذا ما سنوضحه

ب- حماية برامج الحاسب الآلي لنصوص الملكية الأدبية والفنية

أدت الدراسة التي قام بها الفقيه BANZHOF في الولايات المتحدة الأمريكية حول حماية مصنفات الحاسب الآلي بواسطة حقوق المؤلف، وواكب ذلك شروع المصلحة المشرفة على حماية حقوق المؤلف بتسجيل مصنفات الحاسب الآلي، وكان لهذه الدراسة أثر كبير في تبني المنظمة العالمية للملكية الفكرية مبدأ إعتبار برامج الحاسب الآلي مصنفات أدبية وذلك سنة 1979²، وبذلك حسمت هذه المنظمة الجدل القائم لتكون حماية برامج الحاسب الآلي ضمن قوانين حق المؤلف، وبذلك سايرت أغلب التشريعات هذا الإتجاه، وهو نفس المسلك الذي سلكه المشرع الجزائري وبموجب المادة 04 من الأمر 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة اعتبر برامج الحاسب الآلي مصنفا أدبيا إذ نص على ما يلي " تعتبر هذه النصوص كمصنفات أدبية وفنية محمية ما يلي:

أ- المصنفات الأدبية المكتوبة.....برامج الحاسوب....."

لهذا فإن برامج الحاسب تخضع لنفس الشروط التي تخضع لها المصنفات الأدبية، وبالتالي فوجب أن يتوافر فيها شرط موضوعي وهو شرط الابتكار وشرط شكلي وهو الوجود أو التعبير عن البرامج عن طريق تثبيته على دعامة مادية.

¹ - زيدان زبيحة، المرجع السابق، ص90.

² - بدره عمارة، فتيحة عمارة، الحماية الجنائية للمعلومات الإلكترونية في إطار قانون الملكية الفكرية، مجلة الحقيقة، المجلد 13، عدد 31، 2014، ص، ص221-221.

❖ شرط الابتكار في برامج الحاسب الآلي

حتى نقول بأن المصنف خاضع لقانون حماية المؤلف، يجب أن يكون مصنفًا مبتكرًا ويقصد بالابتكار بأنه " بصمة المؤلف الشخصية على المصنف والتي تسمح للجمهور بالنطق باسمه بمجرد مطالعة المصنف إذا كان من المشهورين أو بالقول بانتهاء نسب هذا المصنف إلى مؤلف لديه قدرة ابتكارية على التعبير ' عن أفكاره.¹"

وقد اختلف الفقه بخصوص برامج الحاسب الآلي حول احتوائها على عنصر الابتكار، حيث انقسم في ذلك بين معارض ومؤيد لذلك.

حيث ذهب الفريق المعارض إلى القول بعدم وجود شرط الابتكار في برنامج الكمبيوتر، لأنه يصعب البحث عن الطابع الشخصي للمؤلف من خلال البرنامج، وذلك على عكس المصنفات الأخرى، بسبب أن معد البرنامج²، مارس نشاطه الذهني من خلال تقنيات قائمة وطرق محددة مما لا يدع مجالاً لظهور لمسة شخصيته، فيما يتبنى الاتجاه المؤيد الإعتراف بالطابع الابتكاري لبرنامج الحاسب الآلي، وبالتالي تخضع لأحكام القانون، فلا ينصرف معنى الابتكار فقط إلى الخلق الذهني الذي لم يتوصل إليه البشر، بل يمتد ليشمل كل إنتاج ذهني ينطوي على مقدار معين من الابتكار، فلا يلزم لإسباغ الحماية القانونية أن يكون المصنف من تأليف صاحبه، وإنما يكون عمل واضعه حديثاً يتميز بطابع شخصي خاص يضيف عليه وصف الابتكار³، وقد أكدت أغلب الإتفاقيات والتشريعات على ضرورة وجود هذا الشرط في برنامج الحاسب الآلي.⁴

¹ - محمد أمين الرومي، المرجع السابق، ص 79.

² - مسعود خثير، المرجع السابق، ص 81.

³ - محمد أمين الرومي، المرجع السابق، ص 86.

⁴ - وهو ما ذهبت إليه التوجيهية الأوروبية المتعلقة بالحماية القانونية لبرامج الكمبيوتر بالقول أن الدول الأعضاء تحمي برامج الكمبيوتر كونها أعمالاً أدبية بالمعنى المعطى لها في معاهدة برن الخاصة بحماية الأعمال الأدبية والفنية وهو نفس المفهوم تبنته إتفاقية Gatt. الموقعة في إطار الاتفاقية العامة للتعريف والجمارك "أن برامج الكمبيوتر سواء كانت ملحوظة في إطار نظام أو موضوع تعتبر أعمالاً أدبية بمقتضى اتفاقية برن . أنظر مسعود خثير، المرجع السابق، ص، ص، 82-83.

❖ شرط التجسيد المادي للمصنف (برنامج الحاسب الآلي)

ويقصد بالتجسيد المادي للمصنف إخراجة إلى عالم الوجود، بحيث يسمح بإدراكه من قبل الآخرين بأي شكل من الأشكال، وبغض النظر عن الأسلوب أو الشكل المتخذ¹، فالمصنفات المبتكرة يحميها القانون أيا كان الشكل الذي يتخذه، وأيا كانت وسيلة توصيلها للغير بما فيها الوسائل السلكية واللاسلكية، غير أنه يشترط أن يكون المصنف قد أفرغ في صورة مادية يبرز فيها للوجود ويكون معد للنشر²، وهذا ما أكدته المشرع الجزائري في المادة 7 من الأمر 03-05 السالف الذكر " أن لا يحمي الأفكار بدون ظهورها في شكل ما"، لهذا تمنح الحماية مهما يكن نوع المصنف ونمط تعبيره ودرجة استحقاقه ووجهته بمجرد إيداع المصنف سواء كان المصنف مثبتا أم لا بأية دعامة تسمح بإبلاغه للجمهور، ومنها يتبين أن الحماية تفرض وجود المصنف شكلا³.

ومن هذا المنطلق نجد أن المشرع الجزائري قد فرض حماية للمصنفات الأدبية والفنية التي تفرغ في قالب أو في صورة معينة، وعليه فإن برامج الحاسب الآلي تكتسي طابع المصنف، عندما توضع هذه البرامج وتصاغ في ثوبها النهائي وتصبح قابلة للاستعمال وفق ما وضعت له هذه البرمجة⁴.

2- قواعد البيانات

تعرف قواعد البيانات على أنها "أعمال إختيار وجمع وتجميع لمؤلفات أدبية أو فنية أو موسيقية أو برامج حاسب آلي، أو أية بيانات أخرى كالنصوص والصور والوثائق، والأرقام والوقائع يجري ترتيبها أو تخزينها بصورة منظمة ومنهجية، ويمكن الوصول أو استرجاع هذه المعلومات منها بالوسائل المعلوماتية⁵."

كما تعرف على أنها "مجموعة بيانات مسجلة في ملفات على نحو يحدد الروابط المنطقية بين

¹ - فتحية حواس، المرجع السابق، ص 20.

² - تنص المادة 02/02 من اتفاقية برن "لحماية المصنفات الأدبية والفنية على أنه "المصنفات الأدبية والفنية أو مجموعة أو أكثر منها لا تتمتع بالحماية طالما أنها لم تتخذ شكلا ماديا معيناً."

³ - شريف هنية، الحقوق المعنوية وحمايتها في القانون الجزائري، حق المؤلف، العلامات الرسوم والنماذج الصناعية، (براءة الاختراع)، دار الجامعة الجديدة، الإسكندرية، د ط، 2018، ص 56.

⁴ - مسعود خثير، المرجع السابق، ص 85.

⁵ - نجاة جدي، المعلوماتية وحقوق المؤلف، مجلة دراسات وأبحاث، المجلد 12، العدد 6، 2012، ص 190.

نوعيتها المختلفة"¹، وتعني كذلك القواعد التي تؤسس أو تتضمن دلالة البيانات كالحقائق والإحصائيات والرموز والأنشطة الرقمية كعمليات التحويل الرقمية (0.1) دون أن يكون هناك رابط بينها سوى حين تحويلها بالمعالجة الآلية إلى المعلومات، كما عرفت أيضا أنها " مجموعة المعلومات التي تتكون من معطيات ووقائع وغيرها سواء كانت في شكل مطبوعة أو مجموعات ذاكرة الكمبيوتر أو في شكل آخر²، ولهذا تعتبر قواعد البيانات أداة مهمة في تنمية سوق المعلومات وفي تطويره، فضلا عن فوائدها في كثير من المجالات الإنتاجية والاقتصادية³، وبالتالي تستوجب الحماية باعتبارها عملا إبداعيا مثل قاعدة البيانات المكتبة الرقمية العالمية أو قاعدة بيانات الجريدة الرسمية للجمهورية الجزائرية⁴، مما أدى إلى بسط الحماية لقواعد البيانات من طرف مختلف التشريعات فعلى مستوى التوجيه الأوروبي، فإن القرار التوجيهي بشأن الحماية القانونية لقواعد البيانات قد نص في المادة 01 على "لأغراض هذا القرار، فإن تعبر قواعد البيانات يعني جميع أعمال أو بيانات أو أية مواد أخرى منتجة بشكل مستقل، متى كانت مرتبطة بطريقة نظامية ومنهجية، ويمكن الوصول إليها بصورة فردية أو بوسيلة إلكترونية، أو بأية طريق أخرى وهو نفس التعريف الذي أخذ به المشرع الفرنسي بموجب قانون الملكية رقمة 536/98 الصادر بتاريخ 98/07/01 من خلال المادة 3.112⁵.

كذلك هو الحال بالنسبة للمشرع الجزائري فقد نص على قاعدة البيانات بموجب المادة 02/05 من الأمر 03-05 التي تنص على "...المجموعات والمختارات من المصنفات، مجموعات من مصنفات التراث التقليدي وقواعد البيانات سواء كانت مستنسخة على دعامة قابلة للاستغلال بواسطة آلة أو بأي شكل من الأشكال الأخرى....." حيث اعتبرها من المصنفات المحمية بقانون حماية حق المؤلف.

¹ - محمد علي فارس الزعبي، الحماية القانونية لقواعد وفقا لقانون حق المؤلف، منشأة المعارف الإسكندرية، د ط، 2003، ص 76.

² - راضية مشري، الحماية الجزائرية للمصنفات الرقمية في ظل قانون حق المؤلف، مجلة التواصل في العلوم الإنسانية والاجتماعية، المجلد 19، عدد 2، 2013، ص 138.

³ - طوني عيسى، حماية برامج الكمبيوتر وقواعد البيانات، بحث منشور على الموقع: <https://www.Lipa-ib.org/my files/ itEURS files. Computer/ program.Pdft> أطلع عليه يوم 2018/07/25 على الساعة 15:30.

⁴ - تجدر الإشارة هنا إلى أن القوانين والإجتهادات القضائية ليست محل حماية وهذا ما جاء في نص المادة 11 من قانون حق المؤلف الجزائري، لكنها متى أفرغت ضمن قاعدة بيانات وفق تصنيف معين بآلية استرجاع معينة فإنها تتحول إلى قاعدة بيانات وتستوجب الحماية، باعتبارها عمل إبداعي وفق قانون حق المؤلف .

⁵ -Brunocinelli,., propriété intellectuelle. 2010-2011. top actuel,., Hachette février, 2010, .p22.

3- طبوغرافيا الدوائر المتكاملة

ويطلق عليها طبوغرافيا المدمجة، أو إسم التصميمات التخطيطية، وهي عبارة عن " دائرة كهربائية تصمم بطريقة مصغرة على رقائق أو شرائح، أو هي عبارة رقائق إلكترونية صغيرة جدا تؤدي وظيفة إلكترونية"، وتسمى أيضا بأشباه الموصلات، حيث يتم دمج الدارة الكهربائية على الشريحة للقيام بمهام ووظائف إلكترونية، وقد ساهمت هذه التقنية في تطوير أداء نظم الحاسب الآلي، غير أن جانبا من الفقه يؤكد خصوصيتها واختلافها في طبيعتها عن المصنفات الرقمية لاسيما من حيث واقعها التشريعي¹، الذي يؤكد أنها تخضع في حمايتها لنصوص خاصة مستقلة² عن قانون حماية حق المؤلف أو على الأقل لها بنود خاصة في قوانين الملكية الفكرية.

ثانيا: المصنفات المرتبطة بظهور الأنترنت

هناك مصنفات ارتبط ظهورها بظهور تقنية الأنترنت وهي:

1- أسماء ونطاق (عناوين) الأنترنت

وتسمى أيضا حقول الأنترنت، واختلف الفقه في تعريفها، ومناطق الاختلاف إلى الزاوية التي ينظر إليها كل طرف إلى طبيعة هذا المصنف الرقمي، حيث تم حصر ثلاثة تعاريف مختلفة³:

التعريف الأول: ربط مفهوم عنوان أو موقع الأنترنت بطبيعة التقنية الفنية التي تقوم على استبدال الأرقام بأحرف بسيطة يسهل التعامل معها وحفظها، تلك الأحرف هي التي يتشكل منها اسم الموقع فبمجرد كتابة بعض الأحرف يظهر اسم الموقع أو النطاق كاملا.

■ التعريف الثاني: ربط مفهوم الموقع الإلكتروني بمكونات هذا العنوان، باعتباره يتكون من جزئين أحدهما ثابت ويعبر عنه ب WWW وجزء متغير يميز اسم الموقع عن غيره من المواقع.

¹ - محمد حماد مرهج الهيتي، نطاق الحماية الجنائية للمصنفات الرقمية، - دراسة مقارنة بين القوانين العربية لحماية حق المؤلف، - مجلة الشريعة والقانون، جامعة الإمارات العربية، العدد 48، أكتوبر 2011، ص142.

² - أمر رقم 08/03 المؤرخ في 2003/07/19، يتعلق بحماية التصميمات الشكلية للدوائر المتكاملة الجريدة الرسمية للجمهورية الجزائرية، عدد44 الصادرة بتاريخ 2003/07/23.

³ - فتح الله لفيقي، كريمة كريم، الحماية الجزائرية لقانون الملكية الفكرية للمصنف الإلكتروني في بيئة الأنترنت ومدى استفادة الصحفي من هذه الحماية، مجلة الصورة والاتصال، المجلد7، عدد22، 2018، ص7.

■ التعريف الثالث: يربط مفهوم الموقع الإلكتروني بالجانب الوظيفي للموقع، فالموقع الإلكتروني يعبر عن العنوان الافتراضي للمشروع على شبكة الأنترنت.

ومهما كان تعريف إسم النطاق فثمة حقيقة لا يمكن الإختلاف عليها، وهي أن لهذا الإسم أهمية فنية وإقتصادية خاصة بالنسبة للمشروعات على شبكة الأنترنت، فمن الناحية الفنية نجده سهل التعامل مع شبكة الأنترنت، فبعد أن كان هذا الإسم رقميا يتكون من مجموعة من الأرقام الكثيرة التي يصعب تخزينها أو حفظها في الذاكرة، أصبح سهلا بسيطا يتكون من مجموعة من الحروف يتم ترجمتها تلقائيا إلى أرقام.¹

2- مصنفات الوسائط المتعددة

ظهر هذا المصنف بعد وضوح معالم التقنية الرقمية، وتعرف هذه المصنفات على أنها " كل مصنف مبتكر يدمج في دعامة واحدة أحد أو كل الإجراء التالية نص، صوت، صورة متحركة، برنامج إعلام آلي، ويكون تسيير هيكله ومدخله ببرنامج إعلام آلي يسمح بالتفاعلية² .

وبالرجوع إلى التشريع الجزائري خاصة المرسوم التنفيذي رقم 257/98³ المتعلق بضبط وشروط إقامة خدمات الأنترنت واستغلالها نجده اعتبر حسب نص المادة 02 صفحة الواب متعددة الوسائط تتكون من نصوص، رسوم بيانية، صور أو صورة بينها عن طريق وصلات تسمى نصوص متعددة.

3- البريد الإلكتروني

وهو عبارة عن خدمة تقدم لأي مستخدم لشبكة الأنترنت بطريقة مجانية، بحيث يسمح للمستخدمين وعن طريق العلبة الإلكترونية (la boîte – email)، بإرسال رسالة أو ملف أو موضوع إلى من يرغبون ولكل مستخدم الأنترنت عنوان خاص لبريده الإلكتروني يتكون من إسم حساب المستخدم على شبكة الأنترنت مضافا إليه علامة وإسم الشبكة وأحد الرموز المتعامل بها

¹ - ليندة بلاش، مكانة الملكية الفكرية في توجهات القانون الخاص بالفضاء الإلكتروني، ورقة علمية مقدمة في إطار الملتقى الوطني الملكية الفكرية بين مقتضيات العولمة وتحديات التنمية، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمان ميرة، بجاية، المنعقد في الفترة 28-29/04/2013، ص57.

² - نجاه جدي، المرجع السابق، ص190.

³ - المرسوم التنفيذي رقم 257/98 المتعلق بضبط شروط إقامة خدمات الأنترنت وإستغلالها المؤرخ في 25/08/1998، الجريدة الرسمية للجمهورية الجزائرية، عدد63 الصادرة بتاريخ 26/08/1998.

في الأنترنت، ويتم الإعتداء عبر البريد الإلكتروني بطريقة إرسال مصنف محمي قانونا، في شكل مقال أو صورة أو غير ذلك دون الرجوع بالإذن على المؤلف أو صاحب الحق.¹

4- مصنفات النشر الإلكتروني

مصنفات النشر تنقسم إلى قسمين: مصنفات ذات أصل مادي تمت معالجتها إلكترونيا مثل الكتب، محاضرات، أناشيد، مسرحيات، أغاني... وأخرى متاحة على شبكة الأنترنت دون أن يكون لها أصل مادي، فكثير من الهيئات والمؤسسات لها وجود افتراضي في عالم الأنترنت، دون أن يكون لها وجود مادي، واعتبرت هذه المصنفات سواء تلك التي لها أصل مادي أو تلك المعالجة إلكترونيا إنتاجا فكريا مبتكر محميا بقواعد حق المؤلف والحقوق المجاورة.²

وبهذا يكون المشرع الجزائري قد نجح في تحقيق قدر معين من الحماية لحقوق الملكية الفكرية من خلال توسيع مجال الحماية ليشمل برامج الحاسب الآلي وقواعد البيانات، لكن عليه أن يدخل في مجال الحماية المصنفات المرتبطة بظهور الأنترنت، وذلك من خلال تعديل قانون حق المؤلف والحقوق المجاورة ليواكب التطورات التكنولوجية خاصة مع سرعة انتشارها في هذا العصر.

الفرع الثاني: صور جرائم التعدي على حق الملكية الأدبية والفنية

لقد عالج المشرع الجزائري الحماية الجنائية لبرامج الحاسب الآلي، عن طريق تشريع حقوق المؤلف بموجب الأمر 10/97 المعدل بموجب الأمر 03-05 المؤرخ في 2003/07/19 المتضمن حقوق المؤلف، حيث نص على جرائم الإعتداء على حقوق مؤلفي البرامج وذلك في المواد 151، 153 إلى 159 من الأمر السالف الذكر، حيث عدد المشرع مجموعة من الأفعال الماسة بالمصنفات وبحقوق مؤلفيها كما أدخل جميع جرائم الإعتداء ضمن وصف جريمة التقليد والجرائم الملحق بها .

الفقرة الأولى: جريمة تقليد

لم تضع غالبية التشريعات المقارنة تعريفا محددا لجريمة التقليد، حيث يستوجب الرجوع إلى الفقه من أجل بيان مفهوم التقليد، فعرفها الفقه الفرنسي على أنه "نقل مصنف لم يحل وإلى الملك العام"³ وذلك دون

¹ - عبد الرحمان خلفي، المرجع السابق، ص44.

² - فتح الله لفيقي، جريمة كريمة، المرجع السابق، ص8.

³ - الملك العام هو الوضع الذي تؤول إليه المصنفات الأدبية والفنية التي انقضت مدة حماية حقوقها المادية لفائدة مؤلفها ودوي الحقوق وفقا لمفهوم المادة 03/08 من الأمر 03-05 المؤرخ في 2003/07/19 .

إذن من مؤلفه أو صاحبه وهي كل استعمال لمصنف محمي دون الحصول على رخصة لذلك"،¹ وعرفت كذلك بأنها "القيام بعمل لا يقوم به سوى المؤلف أو يخصص به"،² كما عرفت منظمة wipo بأنها "استنساخ للمصنفات المنشورة أو الفوتوغرافية بأي طريقة مناسبة من أجل توزيعها على الجمهور وإعادة إذاعة البرامج الإذاعية دون تصريح"³، كما عرف Claude colimbet جريمة التقليد على أنه "يرتكز على استنساخ ونشر بطريقة غير شرعية لمصنف بدون تعديل أو بإدخال تغييرات أو إضافات".⁴

وقد سار المشرع الجزائري في الاتجاه نفسه، حيث لم يضع تعريفا لمصطلح جريمة التقليد، وإنما اكتفى بتعداد الأفعال والسلوكات المشكلة لهذه الجريمة فنص في المادة 151 من الأمر 03-05 على أنه "يعد مرتكبا لجنحة التقليد كل من يقوم بالأعمال الآتية:

- الكشف غير المشروع للمصنف أو المساس بسلامة المصنف أو أداء فنان أو مؤد أو عازف.

- استنساخ مصنف أو أداء بأي أسلوب من الأساليب في شكل نسخ مقلدة."

وعليه لقيام هذه الجريمة يستلزم توافر ركنان أساسيان هما الركن المادي والركن المعنوي.

أولاً: الركن المادي

النشاط الإجرامي في جريمة التقليد يأخذ أحد الأفعال الواردة في نص المادة السابقة الذكر وهي:

1- الكشف غير المشروع للمصنف

للمؤلف وحده الحق في الكشف عن المصنف الصادر بإسمه، واختياره الوقت أو الطريقة التي يتم بها إذاعة أو نشر برنامجه، ويتمثل الإعتداء عليه عندما يذاع أو ينشر البرنامج في وقت غير الوقت الذي يراه مناسباً وملائماً، أو بطريقة غير تلك التي يراها مناسبة.⁵

¹ - Tafforeau patrick, droit de propriété intellectuelle, 2ém édition , édition gualino ,France , 2007, p201.

² - مسعود خثير، المرجع السابق، ص88.

³ - بدره عمارة، فتحة عمارة المرجع السابق، 231.

⁴ - Claude colimbet ,propriété littéraire et artistique et droit voisins, Dalloz ,paris,9ém édition, 1999, p194.

⁵ - آمال قارة، المرجع السابق، ص85.

وبلاحظ أن طرق الكشف عن البرمجيات أصبحت كثيرة ومتنوعة، ومن بينها الحصول على الشفرة السرية (craquage) التي تسمح بالدخول للبرمجية واستغلالها كصاحب حق، أو كمستعمل مرخص له، وفي هذا الشأن أدانت المحكمة الإصلاحيّة المدنية (Metz) الفرنسية شابين قرصانين قاما بالهندسة العكسية¹ والنسخ لبرمجيات ألعاب، وكشفهما عنها في ذات اليوم الذي كانت الشركة قد قررت الإطلاق التجاري لها.²

المساس بسلامة المصنف

يدخل في المساس بسلامة المصنف كل التعديلات أو التغييرات أو الإضافات غير المرخص بها التي يمكن أن تقع على المصنفات المنشورة عبر شبكة الأنترنت، إذ كثيرا ما يعتمد أصحاب المواقع نشر مصنفات غير محمية، بموجب قانون حماية المؤلف على مواقعهم، وهذا دون أخذ الإذن من أصحابها.³

غير أنه لا يمكن لأي كان أن يدخل تعديلات على المصنف بتصحيح أو إضافة أو حذف، إلا بموافقة المؤلف وهذا ما نصت عليه المادة 90 من ذات الأمر⁴، إلا أنه استثناء على هذه المادة "يحق للمؤلف اشتراط احترام سلامة مصنفه والاعتراض على أي تعديل يدخل عليه أو تشويهه أو إفساده إذا كان ذلك من شأنه المساس بسمعته كمؤلف أو بشرفه أو بمصالحه المشروعة"، وهذا ما نصت عليه المادة 25 من الأمر نفسه.

وبمفهوم المخالفة أنه إذا لم يكن من شأن هذه التعديلات المساس بسمعة المؤلف أو شرفه أو بمصالحه المشروعة، فإنه لا يمكن الاعتراض عليها من طرفه ومثال على ذلك تعديل معدل ضربية القيمة المضافة في أحد البرامج المصممة لمأمورية الضرائب العقارية.⁵

¹ - الهندسة العكسية هي أكثر الطرق إنتشارا لتقليد البرمجيات، وهي تقنية تعمل على فك ترميز البرامج الكاملة الموجهة إلى الاستعمال من أجل الوصول إلى البرنامج المصدري الخاص بها.

² - مسعود خثير، المرجع السابق، ص 90.

³ - فتحية حواس، المرجع السابق، ص 91.

⁴ - تنص المادة 90 "لا يمكن الناشر أن يدخل تعديلات على المصنف بتصحيح أو إضافة أو حذف إلا بموافقة من المؤلف.

⁵ - مسعود خثير، المرجع السابق، ص 91.

استنساخ البرنامج بأي أسلوب من الأساليب في شكل نسخ مقلد

يقوم السلوك المجرم لهذه الجريمة بإرتكاب سلوك إجرامي، يتمثل في نشر مصنف محمي عبر أجهزة الحاسب الآلي أو شبكة الأنترنت بدون موافقة لصاحب الحق، حيث كفل المشرع للمؤلف الحق في استغلال مصنفه بأي شكل من الأشكال، حتى ولو كان ذلك باستنساخه بأية وسيلة كانت وهذا ضمنته المادة 27 من الأمر 03-05، إلا أن المشرع استثنى بموجب المادة 52 من الأمر 05/03 استنساخ نسخة واحدة من البرنامج في حالتين.

- الإستنساخ بغرض استعمال برنامج الحاسب الآلي للغرض الذي اكتسب من أجله ووفقا للشروط التي كانت قائمة عند اكتسابه، وفي هذا تدعيما لحقوق مؤلفي البرامج، وفي كل حالة يتجاوز فيها من يوجد في حيازته البرنامج حيازة مشروعة حدود القانون أو الاتفاق المرخص به، وبين مؤلف البرنامج يكون فعله مكونا لجريمة التقليد.

- أن يكون الاستنساخ تعويضا لنسخة مشروعة الحيازة من البرنامج وذلك بغرض التوثيق أو خشية ضياعه أو تلفه أو عدم صلاحيته للاستعمال.¹

كما يشترط لقيام الجريمة عدم وجود إذن كتابي من المؤلف أو من أصحاب الحقوق.

ثانيا: الركن المعنوي

لا يكفي لقيام جريمة التقليد وجود الركن المادي وحده، بل لا بد من توافر علم وإرادة لدى الجاني أثناء قيامه بأي اعتداء في صورة من الصور السابقة، وإن كان المشرع لم ينص على ذلك صراحة والقصد المتطلب هو قصد عام في هذه الجريمة.

ثالثا: العقوبة المقررة

نصت المادة 153 من الأمر 05/03 على عقوبة التقليد بقولها "يعاقب مرتكب جنحة تقليد مصنف أو أداء كما هو منصوص عليه في المادتين 151 و152 بالحبس من ستة (6) أشهر إلى ثلاثة (3) سنوات وبغرامة مالية من خمسمائة ألف دينار 500.000 دج إلى مليون دينار

¹ - صالح شنين، الحماية الجنائية للمصنفات الرقمية في إطار قانون حق المؤلف الجزائري، ورقة علمية مقدمة للملتقى الملكية الفكرية بين مقتضيات التنمية، كلية الحقوق والعلوم السياسية، جامعة بجاية، المنعقد يومي 28-29/04/2013، ص 171.

1000.000 دج سواء كان النشر قد حصل في الجزائر أو في الخارج.

الفقرة الثانية: الجرائم الملحقة بجريمة التقليد

إلى جانب الاعتداء المباشر الذي تناولناه في الفقرة الأولى، أضاف المشرع الجزائري أفعالا أخرى وجرمها تحت نفس الاسم وهي التقليد، إلا أنه في الحقيقة هي جنح مشابهة لفعل التقليد، وقد نصت عليها المادة 151 في الفقرات الثالثة والرابعة والخامسة من الأمر 03-05 المتعلق بحق المؤلف والحقوق المجاورة.

أولا: الركن المادي

لكي يتوافر الركن المادي للجرائم الملحقة بجريمة التقليد لا بد وأن يقع سلوك من السلوكات التالية:

- استيراد أو تصدير نسخ مقلدة من مصنف أو أداء.
- بيع نسخ مقلدة أو أداء.
- تأجير أو وضع رهن التداول لنسخ مقلدة لمصنف أو أداء.

كما أضافت المادتان 154 و 155 جريمتي:

- المشاركة في التقليد
- رفض دفع المكافأة المستحقة للمؤلف.

1- استيراد أو تصدير برامج مقلدة

ويستشف من هذه الفقرة أن المشرع الجزائري قد بسط حمايته على جميع البرامج المحمية، سواء بقانون الدولة الجزائري أو بقانون دولة أجنبية أن يكون متمتعا بالحماية في دولته، وبالتالي فيستوي بذلك أن يكون مؤلف البرنامج جزائريا وأجنبيا، كما يستوي أن يكون الجاني جزائري الجنسية أم أجنبيا كذلك¹، كما يشترط لقيام هذه الجريمة كذلك عدم موافقة المؤلف، وهي بذلك تشترك مع جرائم التقليد في ذلك كون أن الموافقة ضمنية أو شفهية أو الموافقة اللاحقة كذلك لا تغني عن المتابعة.²

¹ - بدره عمارة، فتيحة عمارة، المرجع السابق، ص 240.

² - مسعود خنير، المرجع السابق، ص 97.

2- بيع نسخ مقلدة أو أداء

إن البيع المجرم هنا، هو الذي بمقتضاه يتم نقل حق استغلال البرنامج إلى المشتري مقابل ثمن معين، وسواء كان الاستغلال ينطوي على نشر أم استعمال أم ترجمة للبرنامج المقلد.¹

3- تأجير أو وضع نسخ مقلدة

يتصور الركن المادي لهذه الجريمة في حالة التعامل في البرامج سواء كان بالإيجار أو التداول، ويقصد بعملية التأجير لمصنف أو أداء، تمكين مستأجر هذا العمل المقلد باستعمال لمدة معينة لكي يتمتع به، يكفي لتوافر الجريمة عملية إستئجار واحدة، ويشترط في عملية التأجير أن يكون المصنف مقلداً، أما التداول لنسخ مقلدة تعني التصرف في المصنف بقابل أو غير مقابل وسواء كان التصرف نقل ملكية أم حق الاستغلال.²

4- المشاركة في تقليد البرنامج

وتعد هذه الصورة من التقليد طبقاً للقواعد العامة بمعاقبة الشريك وهو الشخص الذي يساهم في أداء هذه الجريمة سواء بعمله أو بوسائله.

5- رفض دفع المكافأة المستحقة عمدا لمؤلف البرنامج

يقوم الركن المادي لهذه الجريمة، في حالة رفض الشخص المكلف بدفع المكافأة المستحقة للمؤلف، وتكون هذه المكافأة في أغلب الأحوال من جراء تنازل مؤلف البرنامج عن حق من حقوقه المادية سواء كلية أو بصفة مؤقتة.³

ثانياً: الركن المعنوي

القصد الجنائي بالنسبة لهذه الجرائم مفترض، بحيث يقوم الركن المعنوي من مجرد إتجاه إرادة الجاني إلى القيام بسلوك من السلوكات السابقة، وبالتالي فالقصد المتطلب في هذه الجريمة هو القصد العام فقط، ما عدا جريمة الإستيراد والتصدير للبرامج المقلدة تتطلب توافر القصد الخاص المتمثل في

¹ - عفيفي كامل عفيفي، المرجع السابق، ص 82

² - عبد الرحمان خلفي، المرجع السابق، ص 181.

³ - انظر المادة 95 من الأمر 03-05.

الاستغلال التجاري .

في الأخير نقول أن المشرع الجزائري ساوى وأخضع الحماية الجزائية للمصنفات الرقمية، لنفس الأحكام المطبقة على المصنفات التقليدية، الواردة في الأمر 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة، فهذه الأخيرة لا تتناسب وطبيعة المصنفات الرقمية خاصة في مجال العقوبة المقررة فهي لا تتناسب مع قيمة الخسائر التي تقع على المصنفات الرقمية، من خلال الجرائم الواقعة عليها، لهذا وجب على المشرع استدراك الأمر بوضع نصوص تكون أكثر ملائمة من خلال تعديلها، أو إضافة نصوص لحماية المصنفات الرقمية.

المطلب الثاني: التوقيع الإلكتروني

لقد بدأت ملامح عصر التعاملات الإلكترونية بالظهور والانتشار بعد الاعتراف بالتوقيع الإلكتروني قانونيا، وبدأت الخطوات العملية لتعميم استخدامه، ليكون أداة التعاملات المستقبلية بين الناس، حيث أنها تسهل عليهم أعمالهم ومهامهم¹، واهتمت التشريعات المقارنة بالتوقيع الإلكتروني كأداة للإثبات ووسيلة فنية لحماية التجارة الإلكترونية في نفس الوقت، وهو الاتجاه الذي تبناه المشرع الجزائري في إطار مشروع قانون التجارة الإلكترونية، ولتعزيز منظومته القانونية سعيا منه للإقرار بالوسائل الإلكترونية والاعتراف بحجيتها في الإثبات أصدر القانون المتعلق بالتوقيع والتصديق الإلكترونيين بموجب القانون رقم 04/15 المؤرخ في 02/01/2015² سنتطرق أولا إلى مفهوم التوقيع الإلكتروني (الفرع الأول) ثم الجرائم الواقعة عليه في (الفرع الثاني).

الفرع الأول: مفهوم التوقيع الإلكتروني

إن الانتقال من العالم المادي الملموس إلى العالم الافتراضي، أفرز عن ظهور الكتابة الإلكترونية التي تقتضي وجود توقيع عليها، كي يمكن نسبتها لصاحبها لاستحالة تطبيق التوقيع العادي عليها فظهر بديل عرف بالتوقيع الإلكتروني، مما أدى إلى تدخل الفقه والتشريع لضبط هذه

¹ - محمد عبيد الكعبي، المرجع السابق، ص284.

² - القانون رقم 15-04 المؤرخ في 01/02/2015، يحدد القواعد المتعلقة بالتوقيع والتصديق الإلكترونيين، الجريدة الرسمية للجمهورية الجزائرية، عدد 06، الصادرة بتاريخ 10/02/2015.

الظاهرة القانونية وإعطاء تعريف لها¹، فتباينت حسب الزاوية التي ينظر إليها.

أولاً: تعريف التوقيع الإلكتروني

عرف قانون الأونسيتال بشأن التوقيعات الإلكترونية التوقيع الإلكتروني بأنه " يعني بيانات في شكل إلكتروني مدرجة في رسالة بيانات أو مضافة إليها أو مرتبطة بها منطقياً يجوز أن تستخدم لتعيين هوية الموقع بالنسبة رسالة البيانات وليبان موافقة الموقع على المعلومات الواردة في رسالة البيانات".²

كما عرفه التوجيه الأوروبي رقم 1999/93 الصادر 1999/12/13 المتعلق بالتوقيع الإلكتروني بموجب المادة 02 منه أنه "بيان أو معلومات معالجة إلكترونياً، ترتبط منطقياً بمعلومات أو بيانات إلكترونية أخرى كرسالة أو محرر، والتي تصلح وسيلة لتمييز الشخص وتحديد هويته".⁴

وعرف أيضاً في قانون التوقيع الإلكتروني الأمريكي الصادر في 30 جوان 2000 على أنه " شهادة رقمية تصدر عن إحدى الهيئات المستقلة، ويتميز كل مستخدم يمكن أن يستعملها في إرسال أي وثيقة أو عقد تجاري أو تعهد أو إقرار".⁵

كما اعترف القانون الفرنسي بالتوقيع الإلكتروني من خلال القانون رقم 2000/230 الصادر بتاريخ 13 مارس 2000، بموجب المادة 4/1316 من القانون المدني بعد تعديلها حيث نص على أنه " التوقيع الضروري لإكمال التصرف القانوني والذي يحدد هوية من يحتج به عليه، ويعبر عن رضا الأطراف بالالتزامات الناشئة عن هذا التصرف وعندما يكون التوقيع إلكترونياً، ينبغي استخدام وسيلة آمنة لتحديد الشخص بحيث تضمن صلته بالتصرف الذي وقع عليه ".⁶، فيما عرفه القانون الأردني من خلال

¹ - الزهرة جقريف، التوقيع الإلكتروني، وحماية لعملية الدفع الإلكتروني، مجلة الدراسات القانونية، المجلد 1، العدد 30 ص 156.

² - المادة 02 من قانون الأونسيتال النموذجي بشأن التوقيعات الإلكترونية المعتمد من طرف الأمم المتحدة في 05 جوان 2001.

³ - الإطلاع على نصوص قانون التوجيه الأوروبي، أنظر الموقع: <https://www.ec.europa.eu>
⁴ - Art 2 D E: « signature électronique, une données sous forme électronique qui est jointe ou liée logiquement a d' autres données électronique et qui sert méthode d'authentification »

⁵ - عبد الفتاح بيومي، مكافحة جرائم الكمبيوتر والانترنت في القانون النموذجي، المرجع السابق، ص 74.

⁶ - راضية لالوش، أمن التوقيع الإلكتروني، مذكرة لنيل شهادة الماجستير في القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزوزو، 2012، ص 17.

المادة 02 من قانون المعاملات الأردني المؤقت رقم 75 لسنة 2001، بأن التوقيع الإلكتروني " هو " البيانات التي تتخذ هيئة حروف أو أرقام أو رموز أو إشارات أو غيرها، وتكون مدرجة بشكل إلكتروني أو رقمي أو ضوئي يسمح بتحديد هوية الشخص الذي وقعها ويميزه عن غيره من انتحل توقيعته بغرض الموافقة على مضمونه.¹

و لم يخالف المشرع الجزائري التشريعات المقارنة وسار على نهجها في تعريف للتوقيع الإلكتروني، حيث عرف التوقيع الإلكتروني بموجب المادة 1/02 من القانون 04/15 المؤرخ في 2015/02/01 المتعلق بالقواعد العامة بالتوقيع والتصديق الإلكترونيين² بأنه " بيانات في شكل إلكتروني مرفقة أو مرتبطة منطقيا ببيانات إلكترونية تستعمل كوسيلة توثيق".

وقد نصت المادة 06 من نفس القانون على "يستعمل التوقيع الإلكتروني للتوثيق هوية الموقع وإثبات قبوله مضمون الكتابة في الشكل الإلكتروني".

ونستخلص من هذه التعاريف أن المشرع الجزائري تبني المعيار الوظيفي للتوقيع، أي ركز على وظيفة التوقيع، دون أن يتطرق إلى طريقة إنشائه، كما أعتبر التوقيع الموصوف وحده ممثلا للتوقيع المكتوب، وهو التوقيع الذي يتم وفقا للمتطلبات الواردة بأحكام المادة 7 من القانون السالف الذكر والتي نصت على " التوقيع الإلكتروني الموصوف هو التوقيع الإلكتروني الذي تتوفر فيه المتطلبات التالية:

- أن ينشأ على أساس شهادة تصديق إلكترونية موصوفة.
- أن يرتبط بموقع دون سواء.
- أن يمكن من تحديد هوية الموقع.
- أن يكون مصمما بواسطة آلية مؤمنة خاصة بإنشاء التوقيع الإلكتروني.
- أن يكون مرتبطا بالبيانات الخاصة به بحيث يمكن الكشف عن التغيرات اللاحقة بهذه البيانات مما يدل على تأثير المشرع الجزائري بالتوجيه الأوروبي رقم 1929/93 عندما نص على التوقيع المسبق أو المتقدم.³

¹ - عباس العبودي، تحديات الإثبات بالسندات الإلكترونية ومتطلبات النظام القانوني لتجاوزها، منشورات الحلبي الحقوقية، لبنان، ط 1، 2010، ص 165.

² - قانون 04/15 في 2015/02/10 يحدد القواعد العامة للتوقيع والتصديق الإلكترونيين، الجريدة الرسمية للجمهورية الجزائرية، عدد 06 الصادرة بتاريخ 2015/02/10.

³ - الربيع سعدي، حجية التوقيع الإلكتروني في التشريع الجزائري، رسالة لنيل شهادة دكتوراه علوم، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2016، ص 44.

-لذا يتم اللجوء إلى التوقيع الإلكتروني حتى يتم رفع مستوى الأمن والخصوصية بالنسبة للمتعاملين عبر شبكة الأنترنت، كما يمكن الحفاظ على سرية الرسائل المرسلة، ولا يستطيع أي شخص مهما كانت قدرته معرفة مضمون الرسائل أو الاطلاع أو تحريفها أو تعديلها، لأنه عن طريق التوقيع الإلكتروني يمكن تحديد هوية المرسل والمرسل إليه إلكترونياً.¹

ثانياً: صور التوقيع الإلكتروني

للتوقيع الإلكتروني صور وأشكالا مختلفة ومتعددة بين توقيع رقمي، وتوقيع بيومتري، وتوقيع كودي وسري وتوقيع بالقلم الإلكتروني والذي يجمع بينهما قيامهما على وسائط إلكترونية واستخدامها لتقنيات نستطيع أن تحول بعض الصفات المميزة للشخص والأرقام والحروف إلى بيانات ينفرد صاحبها باستعمال من أجل مستندات وإجراء معاملات إلكترونية² وهي كما يلي:

1- التوقيع الرقمي

يعتبر من أهم صور التوقيع الإلكتروني، وهو عبارة عن أرقام مطبوعة لمحتوى المعاملة التي يتم التوقيع عليها بالطريقة نفسها، وتتم الكتابة الرقمية للتوقيع عن طرق التشفير، وذلك بإستخدام مفاتيح سريين مختلفين ومرتبطين ببعضهما بمعادلات رياضية بإستخدام اللوغاريتمات، وتتحول بواسطة المعاملة من رسالة مقروءة ومفهومة إلى رسالة رقمية غير مقروءة وغير مفهومة، لا يمكن قراءتها إلا من قبل مالك المفاتيح لفك التشفير، وهذا النظام يحتاج إلى مفاتيح: مفتاح خاص يستخدم للتشفير ومفتاح عام لفك التشفير³، إذ يظل المفتاح الخاص سرياً عند صاحب التوقيع، أما المفتاح العام فيرسل إلى المرسل إليه لفك التشفير وقراءة الرسالة وفهمها.⁴

¹ - شمسان ناجي صالح الخليلي، المرجع السابق، ص 244.

² - الزهرة جقريف، المرجع السابق، ص 161.

³ - المفتاح العام عبارة عن أداء إلكترونية متاحة للكافة، تنشأ بواسطة عملية حسابية خاصة وتستخدم في التحقق من شخصية الموقع الإلكتروني، للتأكد من سلامة وصحة محتوى المحرر الإلكتروني الأصلي أما المفتاح الخاص عبارة أداة الكترونية خاصة بصاحبها، تنشأ بواسطة عملية حسابية خاصة وتستخدم في وضع التوقيع الإلكتروني عل المحررات الإلكترونية، ويتم الاحتفاظ بها في بطاقة مؤمنة انظر أمير فرج، التوقيع الإلكتروني، دار المطبوعات الجامعية، الإسكندرية، 2008، ص 53.

⁴ - إيهاب فوزي السقا، جريمة التزوير في المحررات الإلكترونية، دار الجامعة الجديدة، الإسكندرية، د. ط.، 2008،

2- التوقيع البيومتري

تقوم هذه الصورة على حقيقة علمية، مفادها أن لكل شخص صفات ذاتية خاصة به، تختلف من شخص إلى آخر تتميز بالثبات النسبي، الذي يجعل لها قدرا كبيرا من الحجية في التوثيق والإثبات¹، ويقوم على أساس التحقق من شخصية المتعامل بالإعتماد على الصفات الجسمانية للأفراد مثل البصمة الشخصية، مسح العين البشرية، التعرف على الوجه البشري..... إلخ ويتم التأكد من شخصية المتعامل عن طريق إدخال المعلومات للحاسب الآلي أو الوسائل الحديثة مثل النقاط صورة دقيقة لعين المستخدم أو صوته أو يده، ويتم تخزينها بطريقة مشفرة في ذاكرة الحاسب الآلي ليقوم ذلك بالمطابقة²، ويعتمد هذا النوع من التوقيع على جهة مختصة ومعتمدة بشكل رسمي تقوم بتوثيق التوقيع وتصديقه وتربط بينه وبين الموقع زيادة في الموثوقية وتحقيق الأمان في التعامل الإلكتروني وحماية المتعاملين من التقنية الاحتيالية المتبعة لفك رموز التشفير³.

ولقد تم تطبيق هذا النوع من التوقيع، وذلك من خلال إصدار القرار المؤرخ في 19 جويلية 2000 والمتضمن إصدار جواز السفر وبطاقة التعريف البيومترية، وهذا استجابة للمنظمة العالمية للطيران والتي دعت دول العالم إلى إصدار جواز سفر بيومتري⁴.

3- التوقيع الكودي والسري

ويقصد به استخدام مجموعة من الأرقام أو الحروف أو كليهما يختارها صاحب التوقيع لتحديد هويته وشخصيته، ويتم تركيبها في شكل كودي معين بحيث لا يعلمها إلا صاحب التوقيع ومن يبلغه بها، وتسمى هذه الطريقة (Personal identification membre) يرمز إليها اختصار ب(P I N)⁵، ويستخدم التوقيع الكودي أو السري في المراسلات وإبرام عقود التجارة الإلكترونية والمعاملات البنكية، وذلك من أجل سحب

¹ -راضية لالوش، المرجع السابق، ص 64.

² - عبد الصبور عبد القوي على المصري، التنظيم القانونية للتجارة الإلكترونية، د.ب.ن، د.د. ش، ط1، 2012، ص70.

³ - ياسين جبري، الحماية الجنائية للتصديق والتوقيع الإلكتروني، دراسة مقارنة، مجلة جامعة الأمير عبد القادر للعلوم الإسلامية، قسنطينة، المجلد 32، العدد 01، 2018، ص420.

⁴ - الزهرة جقريف، المرجع السابق، ص163.

⁵ - ممدوح محمد علي مبروك، مدى حجية التوقيع الإلكتروني في الإثبات-دراسة مقارنة بالفقه الإسلامي-دار النهضة العربية، القاهرة، 2005، ص9.

النقود عبر أجهزة الصراف الآلي أو الدفع الإلكتروني، والخدمات في المتاجر وإدخال البطاقة البنكية في الجهاز المخصص لذلك.¹

4- التوقيع باستخدام القلم الإلكتروني

وفي هذا النوع من الصور يتم نقل التوقيع المحرر بخط اليد، على المحرر إلى الملف المراد نقل هذا المحرر إليه، باستخدام جهاز الماسح الضوئي (scanner) وإيصال هذا التوقيع مع المحرر إلى الشخص الآخر باستخدام شبكة الأنترنت، وتم تطوير هذا النوع من التوقيع باستخدام قلم إلكتروني حاسبي، يمكنه الكتابة على شاشة الحاسب الآلي، وذلك عن طريق استخدام برنامج خاص بذلك، يقوم بالنقاط التوقيع والتحقق من صحة التوقيع، وقبوله إذا كان صحيحا، ورفضه إذا كان غير ذلك.²

رغم المزايا الكثيرة لهذا النوع من التوقيع إلا أنها تؤدي إلى زعزعة الثقة، لأنه باستطاعة الشخص المستقبل الاحتفاظ بهذا التوقيع ووضعه على مستندات أخرى، وذلك بنفس الطريقة التي وضع بها هذا التوقيع على المحرر المرسل، كما أنه لا يمكن التأكد من أن الشخص صاحب التوقيع وهو من قام بالتوقيع على المحرر لأن باستطاعة أي شخص أن يضع هذا التوقيع، على ما يشاء من المستندات وإرسالها إلى أي جهة.³

الفرع الثاني: صور الجرائم الواقعة على التوقيع الإلكتروني

يتحقق الإعتداء على التوقيع الإلكتروني من خلال الإعتداء على المنظومة المعلوماتية، وفي هذا المجال كان يخضع للقواعد العامة المنصوص عليها في الفصل السابع مكرر من قانون العقوبات، لكن بصدر القانون 04/15 المتعلق بالتوقيع والتصديق الإلكترونيين، أقر المشرع الجزائري مجموعة من العقوبات الإدارية والمالية والجزائية وما يهمننا في هذا البحث هي الجرائم الواقعة التوقيع الإلكتروني التي تتمثل فيما يلي:

¹ - فاتح بهلولي، المرجع السابق، ص340.

² - محمد عبيد الكعبي، المرجع السابق، ص292.

³ - ثروت عبد الحميد، التوقيع الإلكتروني، ماهيته، مخاطره وكيفية مواجهتها مدى حجيته في الإثبات، دار الجامعة الجديدة، الإسكندرية، د ط، 2007، ص55.

أولاً: جريمة حيازة أو إفشاء أو استعمال بيانات توقيع موصوفة خاصة بالغير

تنص المادة 68 من القانون 04/15 على " يعاقب بالحبس من ثلاثة (3) أشهر إلى ثلاث (3) سنوات وبغرامة من مليون دينار (1000.000) دج إلى خمسة ملايين دينار (5000.000) دج أو إحدى هاتين العقوبتين فقط، كل من يقوم بحيازة أو إفشاء أو استعمال بيانات إنشاء توقيع إلكتروني موصوف خاص بالغير".

1- الركن المادي

يتحقق الركن المادي لهذه الجريمة بقيام الجاني بأحد الأفعال المنصوص في نص المادة السالفة الذكر هي:

- **الحيازة:** يعرف جارسون الحيازة بأنها " سيطرة واقعية وإرادية للحائز على المنقول تخوله مكنة الانتفاع به أو تعديله أو تحطيمه أو نقله فهي سيطرة إرادية للشخص على الشيء، فنقوم الجريمة حيازة الجاني بيانات خاصة بالغير، فهي مسؤولية تقع على مؤدي خدمات التصديق الإلكتروني عن حيازة الجاني بيانات غير مشروعة.¹

- **الإفشاء:** ويتمثل في إيداع ونشر بيانات التوقيع الإلكتروني، بحيث يمكن للغير الإطلاع على محتواها وقراءتها، سواء تم الإطلاع على محتواها من قبل الغير أو لم يتم ذلك، كنشره في المواقع الإلكترونية وشبكات التواصل الاجتماعي، كالفيسبوك أو التويتر أو الواتس أب.²

- **الاستعمال:** يعد الاستعمال أخطر سلوك يقوم به الجاني بالمساس بأمن وسرية بيانات الموقع، وكذلك المساس بعنصري الثقة والائتمان، خاصة في مجال التعاملات المالية الإلكترونية كاستعمال بيانات الموقع في إنشاء توقيع إلكتروني، ومنه يتحصل على شهادة التصديق الإلكتروني لاستعمالها بطريقة غير مشروعة.³

¹ - نجاة من مكي، المرجع السابق، ص 196.

² - فارس خطابي، الحماية الجزائية للتوقيع الإلكتروني، أطروحة لنيل شهادة دكتوراه علوم، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2020-2021، ص 149.

³ - يزيد بوحليط، المرجع السابق، ص 189.

لا تحتاج هذه الجريمة إلى نتيجة معينة، فالسلوك الإجرامي كاف لقيامها باعتبارها من الجرائم الشكلية.

2-الركن المعنوي

جريمة حيازة أو إفشاء أو استعمال بيانات توقيع خاصة بالغير جريمة عمدية، تتطلب توافر القصد الجنائي العام بعنصره العلم والإرادة، أي علم الجاني بأنه يأتي بأفعال غير مشروعة ومجرمة قانوناً، كما تنتج إرادته إلى تحقيق ذلك.

3-العقوبة المقررة

يعاقب على هذه الجريمة بالحبس من ثلاثة اشهر إلى ثلاثة (3) سنوات وبغرامة من 1000.000دج إلى 5000.000دج أو بإحدى هاتين العقوبتين وهذا ما نصت عليه المادة 68 منه القانون 04/15.

ثانياً: جريمة جمع البيانات الشخصية دون الموافقة الصريحة من صاحبها

نصت على ذلك المادة 71 من ق 04/ 15 على " يعاقب بالحبس من ستة 6 أشهر إلى ثلاثة (3) سنوات، وبغرامة من مائتي ألف دينار(200.000دج إلى مليون دينار 1000.000دج أو بإحدى هاتين العقوبتين فقط، كل مؤدي خدمات التصديق الإلكتروني أخل بأحكام المادة 43 من هذا القانون."

يتبين من المادة السالفة الذكر اشتراط صفة معينة في الجاني إضافة إلى الركن المادي والمعنوي

1- صفة الجاني

يتطلب قيام هذه الجريمة أن تقع من مؤدي خدمات التصديق الإلكتروني وأن يستخدم هذه البيانات التي جمعها دون رضا صاحب التوقيع وبالتالي لا تقوم الجريمة في حالة جمع هذه البيانات بموافقة صريحة من الموقع.

2- الركن المادي

يتحقق الركن المادي بإتيان الجاني فعل إيجابي، يتمثل في إستخدام البيانات المتعلقة بالتوقيع الإلكتروني وذلك يتحقق في غير الغرض المخصص لها، أو جمع البيانات الشخصية للموقع أو المعني

دون الحصول على الموافقة الصريحة منه.¹

3- الركن المعنوي

جريمة عمدية لتوافر القصد الجنائي العام، ويتمثل بعلم الجاني بصفة البيانات الشخصية، وعلمه لا يمكن جمعها إلا بموافقة صاحبها، كما تتجه إرادته إلى جمع البيانات الشخصية دون صاحب الأمر أو استعمال هذه البيانات في غرض غير مشروع.

4- العقوبة المقررة

عقوبة الجريمة الحبس من ستة أشهر إلى ثلاث سنوات وبغرامة مالية تقدر 200.000 دج الى 1000.000 دج أو بإحدى هاتين العقوبتين.

إضافة إلى العقوبات الجزائية، يمكن أن تطبق عقوبات إدارية ومالية والمتمثلة في فرض عقوبات مالية تتراوح ما بين 200.000 دج إلى 5000.000 دج وعقوبات إدارية كسحب الترخيص الممنوح له لمؤدي خدمات التصديق الإلكتروني كالإخلال بأحكام دفتر الأعباء أو سياسة التصديق الإلكتروني، وهذا ما نصت عليه المادة 64 من القانون 04/15 بقولها " في حالة عدم احترام مؤدي خدمات التصديق الإلكتروني أحكام دفتر الأعباء أو سياسة التصديق الإلكتروني الخاصة به والموافقة عليها من طرف السلطة الاقتصادية، نطبق عليه هذه السلطة عقوبة مالية يتراوح مبلغها بين مائتي ألف دينار (200.000 دج) وخمسة ملايين دينار (5000.000 دج)."

أما الشخص المعنوي تضاعف عقوبة الغرامة خمس (5) مرات الحد الأقصى للشخص الطبيعي إذا ارتكب إحدى هذه الجرائم.

¹ - عزيزة لرقط، الحماية الجنائية للتوقيع والتصديق الإلكترونيين في التشريع الجزائري، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد 6، عدد 1، 2017، ص122.

المطلب الثالث: جرائم الاعتداء على المعطيات الشخصية

حظيت الحياة الخاصة بحماية دستورية وقانونية في مختلف تشريعات الدول المتقدمة لما لخصوصية الأفراد من أهمية قصوى على كيان الفرد والمجتمع معاً¹، حيث حرصت على ضرورة احترام خصوصيات الأفراد ومراسلاتهم وكل ما من شأنه المساس بسمعتهم وشرفهم²، إذ تعتبر المعطيات الشخصية جزءاً لا يتجزأ من الحياة الخاصة للأفراد، ونظراً للاستعمال الواسع لوسائل التكنولوجيا الحديثة في شتى المجالات خاصة في مجال معالجة المعطيات الشخصية، وسهولة الحصول على البيانات الشخصية وتداولها، الأمر الذي أثار مسألة حماية المعطيات الشخصية، للأفراد إهتمام المنظمات العالمية والإقليمية³، التي أكدت على حق الإنسان في حماية حياته الخاصة من الإعتداء على معطياته الشخصية، وهذا ما قام به المشرع الجزائري، حيث أدرج مفهوم المعطيات الشخصية لأول مرة في دستور 2016 بإضافة الفقرة الأولى من المادة 46 والتي نصت على أن "حماية الأشخاص الطبيعيين⁴ في مجال معالجة المعطيات ذات الطابع الشخصي حق أساسي يضمنه القانون ويعاقب على انتهاكه " ثم أصدر بعد ذلك القانون 07/18 المؤرخ في 10/06/2018⁵ المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الذي أقر الحماية للمعطيات الشخصية للأفراد، لسد الفراغ التشريعي في هذا المجال، بإعتبار أن المواد 303 مكرر إلى 303 مكرر 3 الواردة في قانون العقوبات قاصرة لحماية هذه

¹ - محمد أمين أحمد الشوابكة، المرجع السابق، ص 58.

² - نسرین مشتة، إخلاص بن عبيد، الحماية القانونية للمعطيات الشخصية في ظل القانون 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، المجلة الجزائرية للحقوق والعلوم السياسية، المجلد 06، العدد 01، 2021، ص 2.

³ - لدينا على سبيل المثال الإعلان العالمي لحقوق الإنسان 1948 من خلال المادة 12، كذلك منظمة التعاون الاقتصادي والتنمية التي وضعت الدليل الإرشادي بشأن حماية الخصوصية ونقل البيانات الشخصية الذي سنة 1980 هذا إلى جانب اتفاقية المجلس الأوروبي المؤرخة في 28 جانفي 1981 والمعروفة بالاتفاقية عدد 108 الخاصة بحماية الأشخاص تجاه المعالجة الآلية للمعطيات الشخصية، وكذلك الإرشاد الأوروبي المؤرخ في 24 أكتوبر 1995 المتعلق بحماية الأشخاص الطبيعيين تجاه معالجة المعطيات الشخصية، كما أصدرت اللائحة التنظيمية الأوروبية المؤرخة في 127 أبريل 2016 المتعلقة بحماية المعطيات الشخصية ودخلت حيز التنفيذ في 25 ماي 2018.

⁴ - قانون رقم 16-01 المؤرخ في 6 مارس 2016، المتضمن التعديل الدستوري، الجريدة الرسمية للجمهورية الجزائرية، عدد 14 الصادرة بتاريخ 07/03/2016.

⁵ - قانون 07/18 المؤرخ في 10/07/2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي الجريدة الرسمية للجمهورية الجزائرية، عدد 34 الصادرة بتاريخ 10/07/2018.

المعطيات الشخصية.

سنتطرق إلى مفهوم المعطيات ذات الطابع الشخصي في (الفرع الأول) وبيان صور الجرائم الماسة بالمعطيات الشخصية في (الفرع الثاني).

الفرع الأول: مفهوم المعطيات ذات الطابع الشخصي¹

عرفت منظمة التعاون الإقتصادي والتنمية البيانات الشخصية سنة 1980 على أنها " تعتبر البيانات الشخصية كل معلومة عائدة لشخص طبيعي محدد أو قابل للتحديد " كما عرفتة الإتفاقية الأوروبية رقم 108 الصادرة عن مجلس أوروبا في المادة 2/أ على أن " المعطيات ذات الطابع الشخصي، هي كل المعلومات المتعلقة بشخص طبيعي معرف أو قابل للتعرف عليه²، فهذا التعريف الوارد في هذه الاتفاقية يعتبر مصدرا مهما لمختلف التشريعات سواء الأوروبية منها أو غيرها.

فيما عرف المشرع الفرنسي المعطيات ذات الطابع الشخصي بموجب القانون رقم 108 لسنة 2004 الخاص بحماية البيانات الشخصية بموجب المادة 02 على أنها "يعتبر بيانا شخصا أي معلومة تتعلق بشخص طبيعي محددة هويته أو من الممكن تحديد هويته بطريقة مباشرة أو غير مباشرة سواء تم تحديد هويت بالرجوع إلى رقمه الشخصي أو إلى أي شيء يخصه³.

أما المشرع المغربي عرف المعطيات ذات الطابع الشخصي في المادة الأولى من القانون 08/09 المؤرخ في 2009/02/18 بقوله " كل معلومة كيفما كان نوعها بغض النظر عن دعائها بما في ذلك الصوت والصورة، والمتعلقة بشخص ذاتي معرف أو قابل للتعرف عليه والمسمى بعده " بالشخص المعني⁴ " ويكون الشخص عليه إذا كان بالإمكان التعرف عليه بصفة مباشرة أو غير مباشرة ... " أما

¹ - تطلق على البيانات المتعلقة بالأفراد عدة تسميات منها المعطيات الإسمية، المعطيات الشخصية، المعطيات ذات الطابع الشخصي واستعمل المشرع الجزائري المصطلح الأخير.

² - يحي تومي، الحماية القانونية للمعطيات ذات الطابع الشخصي على ضوء القانون رقم 18-07 دراسة تحليلية، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 04، العدد 02، 2019، ص 1525.

³ - Art2 : constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres, pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne.,modifié par loi n°2004-801 du 6 aout 2004,jorf 7aout 2004.

⁴ - قانون مغربي رقم 08-09 يتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية، عدد 5711 الصادرة بتاريخ 2009/02/23.

المشرع التونسي عرفها بأنها " كل البيانات مهما كان مصدرها أو شكلها والتي تجعل شخصا طبيعيا معرّفا أو قابل للتعريف بطريق مباشرة أو غير مباشرة باستثناء المعلومات المتصلة بالحياة العامة أو المبتكرة كذلك قانونا".¹

بالرجوع إلى المشرع الجزائري، نجده تأخر بعض الشيء عن التشريعات في سن قانون يخص المعطيات الشخصية خاصة منها العربية، فقد عرف المعطيات الشخصية من خلال المادة 03 من القانون 07/18 على أن " كل معلومة بغض النظر عن دعائها متعلقة بشخص معرف أو قابل للتعرف عليه والمشار إليه أدناه " الشخص المعني "بصفة مباشرة أو غير مباشرة لا سيما بالرجوع إلى رقم التعريف أو عنصر أو عدة عناصر خاصة بهويته البدنية أو الفيزيولوجية أو البيومترية أو النفسية أو الإقتصادية أو الثقافية أو الاجتماعية".

وما يمكن ملاحظة أن هذه التعاريف تصب في قالب واحد بأنها كل معلومة تتعلق بشخص طبيعي معرف أو غير معرف، لكن الاختلاف كان في العبارات والمصطلحات المستعملة في كل تعريف، أي أن هذه التعاريف جاءت مواكبة مع القوانين والتوصيات المعمول بها دوليا.

كما يلاحظ أيضا أن التعريف الذي جاء به المشرع الجزائري ضمن خاصيتين أولاهما تتعلق بالمعطيات ذات الطابع الشخصي، وهي متعلقة بالشخص الطبيعي وليس المعنوي إلا أن هناك إتجاها فقهي يرى إلى أن الشخص المعنوي أو الاعتباري يملك معطيات تتطلب الحماية القانونية.²

أما الخاصية الثانية فهي تلك المعطيات التي تمكن من تعريف والتعرف على الشخص المعني³، من خلال بعض العناصر المميزة له والمتعلقة بالهوية البدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية دون حصر لصفات التي تمكن من التعرف على صاحب المعطيات.

كما تجدر الإشارة إلى أن هذه المعطيات ذات الطابع الشخصي يجب أن تخضع للمعالجة حتى تدخل في نطاق الحماية القانونية، فالمعالجة تعتبر السبب الرئيسي في إستفادة المعطيات الشخصية من الحماية

¹ - قانون أساسي تونسي، عدد 63 المؤرخ في 27 جويلية 2004، يتعلق بحماية المعطيات الشخصية الفصل 4، ص2.

² - مريم لوكال، الحماية القانونية الدولية الوطنية للمعطيات ذات الطابع الشخصي في الفضاء الرقمي في ضوء قانون

حماية المعطيات، رقم 07/18، مجلة العلوم القانونية والسياسية، المجلد 10، العدد 01، أبريل 2019، ص 6.

³ - يحي تومي، المرجع السابق، ص1526.

القانونية¹، لذا فقد نص المشرع على هذا الإجراء في المادة 03 من القانون 07-18 المذكورة سابقا بقوله: " يقصد بمعالجة المعطيات ذات الطابع الشخصي " كل عملية أو مجموعة عمليات منجزة بطرق أو وسائل آلية أو بدونها على المعطيات ذات طابع شخصي، مثل الجمع أو التسجيل، أو التنظيم أو الحفظ أو الملائمة، أو التغيير أو الاستخراج أو الاطلاع، أو الاستعمال أو الإيصال عن طريق الإرسال أو النشر أو أي شكل آخر من أشكال الإتاحة، أو التعريف أو الربط البيني وكذا للإغلاق أو التشفير أو المسح أو الإتلاف².

الفرع الثاني: صور الجرائم الماسة بمعطيات ذات الطابع الشخصي

تقتضي أهمية المعطيات ذات الطابع الشخصي بالنسبة للحق في الحياة الخاصة للأفراد، ضرورة وضع قواعد عقابية لحمايتها من المخاطر التي تهددها³، وهذا ما قام به المشرع الجزائري فعلا من خلال إصداره قانون لحماية معالجة المعطيات ذات الطابع الشخصي رقم 07/18 فنص في الفصل الثالث من الباب السادس على الأحكام الجزائية وذلك من خلال المواد من 54 إلى 73 من القانون السالف الذكر سنتطرق لتحديد صور الجرائم الماسة بالمعطيات الشخصية كما يلي:

الفقرة الأولى: التجريم المتعلق بالجمع غير المشروع للمعطيات ذات الطابع الشخصي

و يدخل ضمن هذا التجريم الجرائم التالية:

أولا: جريمة جمع معطيات ذات طابع شخصي بطريقة تدليسية أو غير نزيهة

نصت المادة 59 من القانون 05/18 على أنه " يعاقب بالحبس من سنة إلى ثلاث 3 سنوات وبغرامة من 100 ألف دج 300 ألف دج كل من قام بجمع معطيات ذات طابع شخصي بطريقة تدليسية أو غير نزيهة أو غير مشروعة⁴.

¹ - نعيم سعيداني، الحماية الجنائية للحق في الخصوصية في مجال المعلوماتية، أطروحة دكتوراه العلوم في القانون، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2020-2021، ص145.

² - المادة 03 من القانون رقم 07-18.

³ - عائشة بن قارة مصطفى، آليات حماية المعطيات ذات الطابع الشخصي في التشريع الجزائري وفقا لأحكام القانون رقم 07-18، مجلة العلوم القانونية والسياسية، المجلد 01، أبريل 2019، ص537.

⁴ - تقابلها المادة 16/226 من القانون الفرنسي وجاء نصها كما يلي:

Art 226-16 du c.p.f « le fait y compris par négligence, de procéder ou de faire procéder à des traitements des données à caractères personnel de procéder ou respectées les formalités préalables à leur mise en œuvre preuves par la loi est puni de cinq ans d'emprisonnement et de 300.000euros d'amende ,est puni des mêmes peines le fait ,y compris par négligence de procéder ou de faire

1- الركن المادي

تقع هذه الجريمة في المراحل الأولى من عملية المعالجة، حيث يتمثل السلوك الإجرامي في جمع معطيات ذات طابع شخصي صحيحة لكن على نحو غير مشروع وغير قانوني، و يستمد هذا الجمع أو التجميع صفته غير المشروعة إما من الأساليب غير المشروعة المستعملة للحصول على هذه المعطيات، أو من طبيعة مضمونها،¹ وهذا ما قامت به اللجنة الوطنية في فرنسا حيث فرضت غرامة مالية على شركة جوجل (Google) بسبب جمعها بيانات المحتوى (الهويات، كلمات المرور، تبادل البريد الإلكتروني) عبر شبكات الـ wifi من أجل خدمة جوجل الجديدة (Google street view) دون علم من أصحاب هذه البيانات وقد تعهدت شركة جوجل بالتخلص من هذه البيانات التي تم جمعها²، ونعني بالوسائل التدلسية وغير النزيهة أي استعمال وسائل الخداع والإحتيال بما فيها الكذب على الشخص المعني للتأثير على إرادته، ليقنتع بصحة ما يدعيه الجاني، أما الوسائل غير النزيهة فهي مخالفة الجاني لواجباته الأخلاقية أثناء ممارسته لمهنته³، كما تقع هذه الجريمة سواء كانت عملية الجمع للمعطيات الشخصية آليا أو يدويا وهذا ما نصت عليه المادة 4 من القانون 407 / 18⁴، سواء على جهاز معلوماتي عن طريق إدراجها في سجلات أو ملفات رقمية، أو يتم جمعها من خلال وثائق ورقمية موجودة مسبقا.⁵

كما يجب أن تنصب عملية الجمع على المعطيات ذات طابع شخصي، بالتالي فالمعطيات هي تلك المعلومات التي تخص شخصا طبيعيا والمحصل عليها، والتي تؤدي إلى التعرف على شخص ما بشكل مباشر أو غير مباشر، كاللجوء إلى رقم تسجيل معين كرقم الهاتف أو رقم تسجيل السيارة أو رقم تسجيل الضمان الاجتماعي⁶، أما فيما يخص الطرق غير المشروعة يتحقق ذلك من خلال استعمال وسائل تقنية كالنقاط الموجات التي تحدثها الأصوات من الجدران الإسمنتية للحجرات، ومعالجتها بحاسوب مزود

procéder à un traitement qui a fait l'objet de l'une de mesures prévues au 3° du Lill de l'article 20 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et au libéré.

¹ - نهلا عبد القادر المومني، المرجع السابق، ص 174.

² - نعيم سعيداني، الحماية الجنائية للحق في الخصوصية في مجال المعلوماتية، المرجع السابق، ص 149.

³ - راضية زرقيني، الحماية الجزائية للمعطيات الشخصية، أطروحة لنيل شهادة الدكتوراه علوم، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2021-2022، ص 155.

⁴ - أنظر المادة 04 من القانون 07-18.

⁵ - عزالدين طباش، المرجع السابق، ص 30.

⁶ - Ibrahim Coulibaly, . la protection des données à caractère personnel dans le domaine de recherche scientifique, . Thèse de doctorat. université de Grenoble ,2011 ,.p19.

ببرنامج خاص لترجمتها إلى كلمات أو عبارات، أو مراقبة أو إعتراض وتفرغ الرسائل المتبادلة عن طريق البريد الإلكتروني.¹

2- الركن المعنوي

الجريمة المنصوص عليها في المادة 59 من ق. 07-18 جريمة عمدية، ويتبين ذلك من خلال استعمال المشرع لمصطلحات طرق تدليسية، غير مشروعة وغير نزيهة، فهي جريمة تقوم على القصد الجنائي العام المتمثل في عنصريه العلم والإرادة، أي علم الجاني بقيامه جمع معطيات شخصية بطرق غير مشروعة، وإتجاه إرادته إلى تحقيق النتيجة، إذ لا تتطلب قصدا جنائيا خاصا.

3- العقوبة المقررة

عاقب المشرع الجزائري مرتكب جريمة جمع معطيات ذات طابع شخصي بطريقة تدليسية وغير نزيهة بعقوبة الحبس من سنة إلى ثلاث سنوات وغرامة قدرها 100.000 دج إلى 300.000 دج، لكل قام بجمع معطيات شخصية بطريقة تدليسية أو غير مشروعة أو غير نزيهة، على خلاف المشرع الفرنسي الذي شدد في العقوبة في هذه الجريمة، إذ أقر عقوبة الحبس لمدة خمس سنوات وغرامة قدرها ب 300.000 أورو وهذا ما تضمنته المادة 16/226 من قانون العقوبات.

ثانيا: جريمة جمع المعطيات المتعلقة بالوضعية الجزائية للشخص المعني

تنص المادة 68 من ق. 07-18 على "يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 60.000 دج إلى 300.000 دج كل من قام في غير الحالات المنصوص عليها قانونا، بوضع أو حفظ في الذاكرة الآلية المعطيات ذات الطابع الشخصي جرائم أو إدانات أو تدبير أمن".²

¹ - بولين أنطونيوس أيوب، الحماية القانونية للحياة الشخصية في مجال المعلوماتية دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت، ط1، 2009، ص395.

² - تقابلها المادة 19/226 من القانون الفرنسي. والتي تنص على:

Art 226-19 : « le fait, hors les cas prévus par la loi
Et puni des mêmes peines le fait, or les cas prévus par la loi ,de mettre ou de conserver en mémoire informatisées des données à caractère personnel concernant des infractions , des condamnations ou des mesures sureté. »

1- الركن المادي

يتحقق الركن المادي لهذه الجريمة بمجرد ارتكاب الجاني لسلوك إجرامي، يتمثل في عملية الوضع أو الحفظ للمعطيات ذات الطابع الشخصي في الذاكرة الآلية، ويقصد بالوضع إدراج أو إدخال المعطيات الشخصية والتي تتعلق بالماضي الجزائي للشخص المعني في سجلات معلوماتية، للرجوع إليها عند الحاجة إليها، أما الحفظ فيقصد به الاحتفاظ والإبقاء على المعطيات الشخصية داخل الذاكرة الآلية وتسجيلها¹، مما يدل استبعاد المشرع الجزائي تجريم الوضع والحفظ للمعطيات الشخصية التي تتم بشكل يدوي أو تقليدي.

إن المادة السالفة الذكر بينت نوع المعطيات التي تقع تحت طائلة التجريم والمتمثلة في المعطيات المتعلقة بالوضعية الجزائية للشخص المعني، أو ما يعرف بالماضي الجزائي، والتي تتمثل أساسا في الجرائم والإدانات وتدابير الأمن، و يقصد بالإدانات كل العقوبات الموقعة على المحكوم عليه لارتكابه جناية أو جنحة أو مخالفة، أما تدابير الأمن فهي الإجراءات المنصوص عليها في المادة 19 من قانون العقوبات الجزائي²، ولهذا فهذه الجريمة تقع مخالفة أحكام المادة 10 من ق 07-18 التي حددت الأشخاص المسؤولين عن معالجة المعطيات ذات الطابع الشخصي المتعلقة بالماضي الجزائي للشخص المعني على سبيل الحصر.³

2- الركن المعنوي

تعد جريمة جمع المعطيات المتعلقة بالوضعية الجزائية للشخص المعني، جريمة عمدية لتوافرها لعناصر القصد الجنائي العام المتمثلة في العلم والإرادة، أي علم الجاني أنه يرتكب أفعالا إجرامية تتعلق بمعالجة معطيات ذات طابع شخصي تتعلق بالوضعية الجزائية للشخص المعني، وعلمه كذلك أنه ليس من الجهات المخول لهم القانون هذا الاختصاص، ومع ذلك تتجه إرادته إلى إتيان هذا السلوك المجرم.

¹ - عزالدين، طباش، المرجع السابق، ص33.

² - تنص المادة 19 من ق.ع.ج على " تدابير الأمن هي : 1- الحجز القضائي في مؤسسة استشفائية للأمراض العقلية 2- الوضع القضائي في مؤسسة علاجية."

³ - تنص المادة 10 من ق 07-18 على " لا يمكن معالجة المعطيات ذات الطابع الشخصي المتعلقة بالجرائم والعقوبات وتدابير الأمن إلا من قبل السلطة القضائية والسلطات العمومية والأشخاص المعنويين الذين يسيرون مصلحة عمومية، ومساعدتي العدالة في إطار اختصاصهم."

3- العقوبة المقررة

يعاقب مرتكب الجريمة الواردة في المادة 68 من القانون 07-18 بالحبس من ستة أشهر إلى ثلاث سنوات وغرامة قدرها من 60.000 إلى 300.000 دج.

الفقرة الثانية: الجرائم المتعلقة بالأفعال المرتكبة خلال المعالجة الآلية للمعطيات الشخصية

تناول المشرع الجزائري مجموعة من الجرائم ضمنها قانون 07-18 المتعلق بحماية المعطيات ذات الطابع الشخصي، والتي يمكن ارتكابها أثناء معالجة المعطيات الشخصية وتتمثل في:

أولاً: جريمة معالجة المعطيات ذات الطابع الشخصي دون موافقة أو رغم اعتراض الشخص المعني

تنص المادة 55 من ق 07-18 على "يعاقب بالحبس من سنة (1) إلى ثلاث(3) سنوات وبغرامة من 100.000 دج إلى 300.000 دج كل من قام بمعالجة المعطيات ذات الطابع الشخصي طبقاً لأحكام المادة 7 من هذا القانون.

ويعاقب بنفس العقوبة كل من يقوم بمعالجة معطيات ذات طابع شخصي رغم اعتراض الشخص المعني عندما تستهدف هذه المعالجة لا سيما الإشهار التجاري أو عندما يكون الاعتراض مبنيًا على أسباب شرعية."

طبقاً لما جاء في المادة السالفة الذكر، نجد أن المشرع الجزائري يجرم كل من يقوم بمعالجة المعطيات الشخصية دون موافقة ورضا المعني، أو معالجة معطيات شخصية خاصة بالشخص المعني رغم إعتراضه على ذلك.

1- الركن المادي

يقوم النشاط الإجرامي لهذه الجريمة، عن كل معالجة يقوم بها المسؤول عن المعالجة دون رضا وموافقة من الشخص المعني، ودون أن تكون هذه المعالجة تندرج ضمن إحدى الحالات الضرورية المنصوص عليها قانوناً، فكل من خرق أحكام المادة 17¹ من القانون 07-18 وقام بمعالجة المعطيات ذات الطابع الشخصي دون الموافقة الصريحة والمسبقة للشخص المعني، تقوم الجريمة المنصوص عليها

¹ - تنص المادة 7 من ق 07-18 على أنه "لا يمكن القيام بمعالجة المعطيات ذات الطابع الشخصي إلا بالموافقة الصريحة للشخص المعني."

في الفقرة الأولى من المادة 55 من ق 18-07.

أما الصورة الثانية تتمثل في منح الشخص المعني حق الاعتراض على ذلك، إذا ما توافرت أسباب مشروعة، أو كان الغرض من هذه المعالجة الآلية للمعطيات الشخصية هو الإشهار التجاري، ومن بين الأسباب المشروعة التي يمكن الإحتجاج بها لممارسة حق الاعتراض على القيام بالمعالجة الآلية للمعطيات الشخصية، هي الحدود المذكورة في المادة 54 من ق 18-07، والمتمثلة في عدم إحترام الكرامة الإنسانية أو الحياة الخاصة أو الحريات العامة، أو المساس بحقوق الأشخاص أو شرفهم أو سمعتهم.¹

2- الركن المعنوي

إن جريمة معالجة المعطيات الشخصية دون موافقة أو اعتراض الشخص المعني، هي جريمة عمدية تقتضي اتجاه إرادة الجاني إلى معالجة معطيات الأفراد ذات الطابع الشخصي، دون أن يحصل على الموافقة الصريحة من المعني بالأمر أو إقدامه على ذلك بالرغم من إعتراضه، مع علم الجاني بأن ذلك محظور قانونا.²

3- العقوبة المقررة

قرر المشرع الجزائري لهذه الجريمة عقوبة الحبس من سنة إلى ثلاث سنوات وغرامة قدرها من 100.000 دج إلى 300.000 دج.

ثانيا: جريمة معالجة المعطيات ذات الطابع الشخصي دون تصريح أو ترخيص

تنص المادة 56 من ق 18-07 بقولها " يعاقب بالحبس من سنتين (2) إلى خمس (5) سنوات وبغرامة من 200.000 دج إلى 500.000 دج كل من ينجز أو يأمر بإنجاز معالجة معطيات ذات طابع شخصي دون احترام الشروط المنصوص عليها في المادة 12 من هذا القانون.

¹ - عبد الغاني بوجراف، آليات حماية المعطيات الشخصية -دراسة مقارنة بين القانونين الجزائري والمغربي، مجلة الدراسات القانونية المقارنة، المجلد 08، عدد 01، 2022، ص 992.

² - نسمة بطيجي، الجرائم المتعلقة بانتهاك الأحكام الإجرائية المقررة لحماية الحق في الخصوصية الرقمية في التشريع الجزائري، بحث مقدم في إطار الملتقى الدولي الخصوصية في مجتمع المعلوماتية، مركز جيل البحث العلمي، طرابلس، لبنان، الفترة الممتدة من 19-20/7/2019، ص 77.

ويعاقب بنفس العقوبات كل من قام بتصريحات كاذبة أو واصل نشاط معالجة المعطيات رغم سحب وصل التصريح أو الترخيص الممنوح له."

تقوم هذه الجريمة على ركن مادي ومعنوي وعقوبة مقررة.

1- الركن المادي

تنشأ هذه الجريمة بمجرد مباشرة القائمين على المعالجة للمعطيات الشخصية أنشطة المعالجة في الأحوال التي يمنحون فيها ترخيصا بذلك من قبل الجهات المختصة المحددة قانونا، كما تنشأ كذلك في الأحوال التي يلغى فيها الترخيص أو ينتهي مدته وتستمر جهة المعالجة بنشاطها.¹

ويتحقق السلوك الإجرامي بمجرد إنجاز معالجة معطيات ذات طابع شخصي، أو الأمر بذلك في غياب التصريح المسبق أو الترخيص من السلطة الوطنية، وتقع مسؤولية السلوك الإجرامي على المسؤول عن المعالج، إذا هذه الصورة جاءت مخالفة لأحكام المادة 12 من قانون 07-18 السالف الذكر، التي تلزم أن تخضع كل عملية معالجة للمعطيات ذات الطابع الشخصي، إلى إجرائي التصريح والترخيص من طرف السلطة الوطنية لحماية المعطيات الشخصية.

وقد تعرض القضاء الفرنسي لهذه المسألة، حيث قضى بعدم قيام جريمة إنجاز معالجة لمعطيات شخصية دون تصريح مسبق في حالة شخص قام بعملية تفسير اختيارات الشخصية لشخص آخر عن طريق برنامج معلوماتي، حيث جاء تبرير القضاء لهذا الحكم أن اعتبار النظام المعلوماتي خاصا بحاسوب قديم ومخصص للاستعمال الشخصي، ولم يكن موصولا بأجهزة أخرى، كما أن عدم وجود طابعة ولا قرص صلب، فالمعلومات كانت مخزنة في أقراص مرنة فقط، لكن في قضية مماثلة قضى بتوافر أركان الجريمة في حق المسؤول عن موقع إلكتروني، حيث أدرج إسم شخص بالمحتوى التحريري للموقع، وهذا ما اعتبرته المحكمة معالجة آلية للمعطيات الشخصية، مما يستوجب الحصول على تصريح مسبق.²

¹ - بولين انطونيوس أيوب، المرجع السابق، ص 414.

² - راضية زرقيني، المرجع السابق، ص، ص 130-131.

2- الركن المعنوي

جريمة معالجة المعطيات ذات طابع شخصي دون تصريح أو ترخيص جريمة عمدية، تقوم على القصد الجنائي العام بعنصري العلم والإرادة، أي علم الجاني بأنه يقوم بمعالجة للمعطيات الشخصية دون ترخيص أو تصريح من الشخص المعني، أو مباشرة المعالجة في غياب الترخيص والتصريح، وتتجه إرادته إلى إجراء المعالجة المخالفة لما توجبه المادة 12 من القانون 07-18 السالف الذكر الخاصة بالحصول على تصريح وترخيص من السلطة الوطنية.

ولم يشترط المشرع الجزائري لقيام الجريمة قصدا خاصا الجريمة، وإنما اكتفى لقيام هذه الجريمة بوجود القصد العام.

3- العقوبة المقررة

يعاقب مرتكب جريمة معالجة المعطيات ذات الطابع الشخصي، بالحبس من سنتين إلى خمس سنوات وغرامة تتراوح ما بين 200.000 دج إلى 500.000 دج، أما إذا تعلق الأمر بنقل معطيات ذات طابع شخصي نحو دولة أجنبية بدون ترخيص وفق ما نص عليه في المادة 44، فإن العقوبة المقررة هي الحبس من سنة إلى خمس سنوات وغرامة من 500.000 دج إلى 1000.000 دج وهذا ما تضمنته المادة 67 من القانون 07-18.

ثالثا: جريمة عدم الاعتراف بحقوق الشخص المعني

تناول المشرع هذه الجريمة من خلال المادة 64 من ق 07-18 التي تنص على "يعاقب بالحبس من شهرين (2) إلى سنتين (2) وبغرامة من 20.000 دج إلى 200.000 دج أو بإحدى هاتين العقوبتين فقط، كل مسؤول عن المعالجة يرفض دون سبب مشروع، حقوق الإعلام أو الولوج أو التصحيح أو الاعتراض المنصوص عليها في المواد 32 و34 و35 من هذا القانون."

لقد وردت هذه الحقوق في الباب الرابع من القانون 07-18 تحت "عنوان حقوق الشخص المعني" وأوجبت على المسؤول عن المعالجة ضرورة ضمانها لصالح كل شخص تكون معطياته الشخصية محل المعالجة، وتتمثل هذه الحقوق في حق الإعلام (المادة 32) وحق الولوج (المادة 34) وحق التصحيح

(المادة 35) والحق في الاعتراض (المادة 36)، وكل من يخالف الإلتزامات بضمان الحقوق يقع¹ ضمن الجريمة المنصوص عليها في المادة 64 من القانون السابق الذكر.

1- الركن المادي

يقوم الركن المادي بمجرد رفض المسؤول عن المعالجة دون سبب مشروع الحقوق التي كفلها له القانون 07-18، المتمثلة في حق الإعلام، أو الولوج أو الحق في التصحيح، أو حق الاعتراض، وكذلك خولها له المشرع من أجل ممارسة نوع من الرقابة على معطاته ذات الطابع الشخصي الخاضعة للمعالجة.²

2- الركن المعنوي

فمن خلال المادة 64 من القانون 07-18 الذي سبق ذكره فهذه الجريمة عمدية، لتوافر القصد الجنائي العام بعنصره العلم والإرادة، أي علم الجاني أنه يأتي أفعالا تشكل رفضا للحقوق المنصوص عليها في قانون 07-18، كرفض الاعتراف بحق الإعلام أو الولوج أو التصحيح أو الاعتراض، ومع ذلك تتجه إرادته إلى ارتكاب السلوك المجرم.

3- العقوبة المقررة

يعاقب المشرع الجزائري على جريمة عدم الاعتراف بحقوق الشخص المعني، بالحبس من شهرين إلى سنتين وبغرامة مالية من 20.000 دج إلى 200.000 دج أو بإحدى هاتين العقوبتين، حيث ترك للقاضي السلطة التقديرية في توقيع العقوبة التي يراها مناسبة.

الفقرة الثالثة: تجريم الأفعال المتعلقة بالإستغلال غير المشروع للمعطيات ذات الطابع الشخصي

نص المشرع الجزائري بموجب القانون 07-18 على مجموعة من الجرائم تتمثل في:

أولا: جريمة إستعمال المعالجة لأغراض غير تلك المصرح بها أو المرخص بها

وهي الجريمة الواردة في المادة 58 من ق 07-18 والتي جاء نصها كما يلي:

¹ - عزالدين طباش، المرجع السابق، ص 43.

² - يحي تومي، المرجع السابق، ص 1545.

"يعاقب بالحبس من ستة (6) أشهر إلى سنة (1) وبغرامة مالية من 60000 إلى 100.000 دج أو بإحدى هاتين العقوبتين فقط، كل من قام بإنجاز أو باستعمال معالجة معطيات لأغراض أخرى غير تلك المصرح بها أو المرخص بها".¹

1- الركن المادي

يتحقق النشاط الإجرامي لهذه الجريمة، بمجرد الانحراف عن الغرض من المعالجة الآلية للمعطيات، والغرض أو الغاية هي موضوع المعالجة الآلية أي الغرض المتوخى من معالجة المعطيات الشخصية²، حيث تفترض هذه الجريمة الحصول على هذه المعطيات بصورة مشروعة، أي بإذن من السلطة الوطنية المختصة، ولكن الجاني ينحرف عن الغرض المقصود منها.³ وعلى سبيل المثال يعد الجاني مرتكباً لهذه الجريمة لو استغل المعطيات الخاصة بشخص آخر في الكشف عن مصادر ثروته أو لمعرفة مركزه المالي أو في الاستدلال عليه لخدمة مصلحة الضرائب.⁴

أما بالنسبة للأشخاص الذين يتحملون المسؤولية عن هذه الجريمة، هم الأشخاص الذين قاموا بإنجاز أو استعمال المعالجة، أي كل الأشخاص الحائزين للمعطيات الذين يشاركون في كل مراحل المعالجة من التجميع إلى التنظيم، وإلى غاية هؤلاء المعنيين لتصلهم المعالجة أو المعطيات.⁵

¹ - نص المشرع الفرنسي على هذه الجريمة في المادة 226-21 من قانون العقوبات الفرنسي

Art 226-21c.p.f: « le fait ,par toute personne détentrice de données à caractère personnel à l'occasion de leur enregistrement, de leur classement , de leur transmission ou de toute autre de forme de traitement , de détourner ces informative leur finalité que définie par la disposition législative, lacté réglementaire ou la décision de la commission nationale de l'informatique est de libertés autorisant le traitement automatisé, ou par les déclarations préalables à la mise en œuvre de ce traitement ,est puni de cinq ans d'emprisonnement et de 300.000euros d'amende. »

² - محمد أمين الشوابكة، المرجع السابق، ص 99.

³ - Hervé Bonnard.la répression de la criminalité .c .p. cahiers de droit de l'entreprise.

مشار إليه : بولين انطونيوس أيوب، المرجع السابق، ص 420. 2002.n.4.p.42.

⁴ - عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والأنترنترنت في القانون العربي النموذجي، المرجع السابق، ص 645.

⁵ - عزالدين طباش، المرجع السابق، ص 53.

2- الركن المعنوي

فيما يتعلق بجريمة استعمال المعالجة لأغراض غير تلك المصرح بها أو المرخص بها، جريمة عمدية وتتخذ صورة القصد الجنائي العام، والذي يقوم بتوافر عنصرين هما العلم والإرادة، فيتعين أن يعلم الجاني بأن من شأن فعله أن يشكل إنحرافا عن الغرض أو الغاية من المعالجة الآلية للمعطيات الشخصية، وأن تتجه إرادته إلى إتيان السلوك الإجرامي، لكن ذهب الفقه الفرنسي إلى القول بضرورة توافر القصد الخاص إلى جانب القصد العام، الذي يتمثل في إثبات نية الغش لدى الجاني، أي لابد أن تملك الأغراض التي تم التصريح بها فقط لإخفاء الأغراض الحقيقية التي أراد الجاني الوصول إليها من خلال المعالجة.¹

العقوبة المقررة

عاقبت المادة 58 من ق 07-18 على هذه الجريمة بالحبس من ستة أشهر إلى سنة وغرامة من 60.000 دج إلى 100.000 دج أو بإحدى العقوبتين، إذ ترك للقاضي السلطة التقديرية للاختيار بين تطبيق الحبس أو الغرامة المالية.

ثانيا: جريمة الاحتفاظ بالمعطيات خارج المدة القانونية

وهي الجريمة الواردة في المادة 2/65 من القانون 07-18 والتي نصت "... يعاقب بنفس العقوبة كل من قام بالاحتفاظ بالمعطيات ذات الطابع الشخصي بعد المدة المنصوص عليها في التشريع الساري المفعول أو تلك الواردة في التصريح أو الترخيص."²

يتبين من هذه المادة أن الجريمة لقيامها لابد من ركنين مادي ومعنوي وعقوبة مقررة لها.

1- الركن المادي

يتحقق الركن المادي لجريمة الحفظ غير المشروع للمعطيات الشخصية، بمجرد حفظ المعطيات ذات

¹ - زاضية زرقيني، المرجع السابق، ص 164.

² - تقابلها المادة 20-226 من قنون العقوبات الفرنسي.

Art 226-20 du c.p.f: « le fait personnel au de la durée prévus par la loi ou le règlement, par la demande d'autorisation ou davis ou par -là de déclaration préalable adressée à la commission nationale de l'informatique et des libertés , et puni de cinq ans d'emprisonnement et de 300.00 euros d'amende, fais si cette conservation est effectuée à des fins historique , statistique ou scientifique dans les conditions prévus par la loi et puni des memes peines le fait , or les cas prévus par la loi , de traiter à des fins autres qu'historiques, statistique des données à caractère personnel conservées au-delà de la durée mentionnée au premier alinéa. »

الطابع الشخصي لمدة أكبر من المدة الواردة في التصريح أو الترخيص، وبناء على ذلك تقع الجريمة إذا كانت معالجة المعطيات الشخصية التي تأخذ شكل الحفظ قد تمت وفق أحكام القانون، ولكن تم حفظ هذه المعطيات لمدة تتجاوز المدة المطلوبة للحفظ، حيث أن هذه المعطيات لا يمكن أن تحفظ لمدة غير محدودة إلا في حالات إستثنائية يفترض أن تكون محددة صراحة وقانوناً¹، وقد نصت المادة 9 فقرة هـ من القانون 07-18 على "يجب أن تكون المعطيات الشخصية...هـ- محفوظة بشكل يسمح بالتعرف على الأشخاص المعنيين خلال مدة لا تتجاوز المدة اللازمة لإنجاز الأغراض التي من أجلها تم جمعها ومعالجتها."، كما أجازت المادة نفسها في الفقرة الأخيرة إمكانية أن تأذن السلطة الوطنية بحفظ المعطيات ذات الطابع الشخصي بعد المدة المقررة لغايات تاريخية أو إحصائية أو علمية.²

2- الركن المعنوي

تعد جريمة الإحتفاظ بالمعطيات خارج المدة القانونية من الجرائم العمدية، والتي يتخذ فيها الركن المعنوي صورة القصد الجنائي العام الذي يقوم بتوافر العلم والإرادة، فيتعين أن يكون الجاني عالماً بأنه يحتفظ بمعطيات شخصية لمدة أكثر من المدة التي سبق طلبها أو التي تضمنها الإخطار المسبق، وأن يعلم أن ذلك الإحتفاظ يتم بغير موافقة السلطة الوطنية، كما تتجه إرادة الجاني إلى تحقيق ذلك من خلال الإحتفاظ بالمعطيات.³

3- العقوبة المقررة

عقوبة جريمة الإحتفاظ بالمعطيات خارج المدة القانونية هي الغرامة من 200.000 دج إلى 500.000 دج.

ثالثاً: جريمة السماح لغير المؤهلين بالولوج إلى المعطيات الشخصية

تناول المشرع الجزائري هذه الجريمة في المادة 60 من القانون 07-18 حيث جاءت نصها " يعاقب بالحبس من سنتين (2) إلى خمس (5) سنوات وغرامة من 200.000 دج إلى 500.000 دج

¹ - مدحت رمضان، الحماية الجنائية للتجارة الإلكترونية، دراسة مقارنة، درار النهضة العربية، ط1، 2001، ص 102.

² - انظر المادة 9 من القانون 07-18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، المؤرخ في 2018/07/10.

³ - محمد أمين الشوابكة، المرجع السابق، ص97.

كل من سمح لأشخاص غير مؤهلين بالولوج لمعطيات ذات طابع شخصي."

1- الركن المادي

تقوم هذه الجريمة في حق كل شخص يحوز المعطيات ذات الطابع الشخصي بحكم المهام المنوطة بهم، كأعضاء السلطة الوطنية والموظفين التابعين لها، بالإضافة إلى المسؤول عن المعالجة والمعالج من الباطن وكل المكلفين بجميع مراحل المعالجة، مما يعني أن هذا الفعل يشكل خرقاً للالتزام بالمحافظة على السر المهني الذي أقره القانون لحماية المعطيات الشخصية، ومنه فالسلوك الإجرامي يتمثل في السماح للغير وإيصالهم إلى المعطيات الشخصية أي بتمكينهم من الاطلاع عليها،¹ وما يمكن ملاحظته نجد أن المشرع الجزائري استعمل عبارة "الولوج" مما يدل أنه يقصد بها المعالجة الآلية للمعطيات التي تحتوي على هذه المعطيات الشخصية، وهذا يعني إخراج المعطيات الشخصية غير الآلية من التجريم، إن كان يقصد كلاهما فيمكن استبدال كلمة الولوج بعبارة الإطلاع.²

2- الركن المعنوي

تعتبر جريمة السماح لغير المؤهلين بالولوج إلى المعطيات الشخصية، جريمة عمدية وهذا لتوافر عناصر القصد الجنائي العام، المتمثل في علم الجاني بأنه يقوم بالسماح لغير المؤهلين بالولوج إلى المعطيات الشخصية، وتتجه إرادته لإتيان السلوك الإجرامي، أما في حالة وقوع الجريمة نتيجة خطأ معتقداً أن الغير من المؤهلين فلا تقوم الجريمة في حق المسؤول عن المعالجة، وإنما يمكن إدخال هذا السلوك الإجرامي ضمن جريمة أخرى وهي الجريمة الواردة في المادة 65 من القانون 07-18 الخاصة بخرق الالتزام بسرية وسلامة المعطيات الشخصية.

3- العقوبة المقررة

طبقاً للمادة 60 من القانون 07-18 يعاقب مرتكب جريمة السماح لغير المؤهلين بالولوج إلى المعطيات الشخصية، بالحبس من سنتين إلى خمس سنوات وبغرامة تتراوح ما بين 200.000 دج إلى 500.000 دج.

¹ - عز الدين طباش، المرجع السابق، ص 56.

² - عز الدين طباش، المرجع نفسه، ص 56.

رابعاً: جريمة إيصال المعطيات المعالجة إلى غير المؤهلين لها

تنص المادة 69 من ق 07-18 على " يعاقب بالحبس من سنة (1) إلى خمس (5) سنوات وبغرامة من 100.000 دج إلى 500.000 دج، كل مسؤول عن معالجة وكل معالج من الباطن وكل شخص مكلف بالنظر إلى مهامه، بمعالجة معطيات ذات طابع شخصي، يتسبب أو يسهل، ولو عن إهمال الاستعمال التعسفي أو التدليسي للمعطيات المعالجة أو المستلمة أو يوصلها إلى غير المؤهلين لذلك."

1- الركن المادي

حدد القانون 07-18 الأشخاص التي تقوم في حقهم هذه الجريمة على سبيل الحصر، وهم كل من المسؤول عن المعالجة¹، أو كل معالج من الباطن²، أو كل شخص مكلف بحكم مهامه معالجة المعطيات ذات الطابع الشخصي.

ويتحقق السلوك الإجرامي بارتكاب الجاني لعدة أفعال، تتمثل في الإستعمال التعسفي أو التدليسي للمعطيات الشخصية سواء كانت في مرحلة المعالجة أو استلمها لمعالجتها.

كما يشترط لقيام الجريمة أن يتخذ الجاني سلوك يتمثل في إيصال المعطيات الشخصية لغير المؤهل لذلك، وهو سلوك إيجابي يتمثل في إرسال أو تقديم المعطيات أو وضعها في متناول الغير، أي أن هذا الأخير يستقبل المعطيات الشخصية فقط، عكس جريمة السماح للغير بالولوج فالشخص غير المؤهل يقوم بنفسه بالولوج لمعطيات لا حق له أن يطلع عليها.³

2- الركن المعنوي

تقوم هذه الجريمة سواء تم إيصال المعلومات عمداً أو خطأ، وهذا ما جاء في مضمون المادة 69 من القانون 07-18 بقولها "... يتسبب أو يسهل ولو عن إهمال..." " فإذا وصلت إلى شخص غير مؤهل للإطلاع على المعطيات الشخصية، من مسؤول مكلفاً بالمعالجة نتيجة إهمال أو قلة

¹ - يقصد بالمسؤول عن المعالجة طبقاً للمادة 12/3 من ق 07/18 " شخص طبيعي معنوي عمومي أو خاص أو أي كيان آخر يقوم بموارده أو بالاشتراك مع الغير بتحديد الغايات من معالجة المعطيات ووسائله."

² - يقصد بمصطلح "المعالج من الباطن" حسب المادة 13/3 من ق 07-18 "كل شخص طبيعي أو معنوي أو خاص أو أي كيان آخر يعالج معطيات ذات طابع شخصي لحساب المسؤول عن المعالجة".

³ - عزالدين طباش، المرجع السابق، ص 58.

الحيلة والحذر لتأمين سرية المعطيات يكون مسؤولاً عن الإفشاء بغير عمد¹، فقد قضي بقيام موظف النظام المعلوماتي في المستشفى بالإفشاء للغير، عن طريق الخطأ عن معلومات صحية تخص المريض (أ) في حين كان عليه الإفشاء عن معلومات (ب)، ففي هذا الغرض تقوم المسؤولية الجزائية على أساس الخطأ من قبل الجاني.²

كما قضي كذلك بقيام جريمة إفشاء المعطيات، عن طريق الخطأ في حق الشخص المكلف بالمعالجة، قام بتقديم وثيقة لأحد الهيئات ورد فيها رقم الهاتف لأحد الأشخاص دون أن ينتبه إلى ذلك، إذ اعتبر القضاء أن رقم الهاتف يعتبر من المعطيات الشخصية التي يمكن التعرف على صاحبه مباشرة، أدين الشخص المسؤول عن المعالجة رغم أنها أثار الدفع بتوافر القوة القاهرة ما دام أنه كان ملزماً بتقديم الوثيقة.³

3- العقوبة المقررة

يعاقب مرتكب هذه الجريمة بالحبس من سنة الى خمس سنوات وبغرامة مالية من 100.000 دج إلى 500.000 دج.

الفقرة الرابعة: تجريم أفعال المساس بصلاحيات السلطة الوطنية لحماية المعطيات

تتمثل في الجرائم المنصوص عليها في المادتين 61 و 66 من القانون 18-07 وهما جريمتا عرقلة عمل السلطة الوطنية لحماية المعطيات، والامتناع عن إعلام السلطة الوطنية عن الانتهاكات المتعلقة بالمعطيات الشخصية في مجال الاتصالات الإلكترونية.

أولاً: جريمة عرقلة عمل السلطة الوطنية لحماية المعطيات

نظم المشرع هذه الجريمة في المادة 61 من ق. 18 07 والتي تنص على " يعاقب بالحبس من ستة (6) أشهر إلى سنتين (2) وبغرامة من 60.000 دج إلى 200.000 دج أو بإحدى هاتين العقوبتين فقط، كل من عرقل عمل السلطة الوطنية.

¹ - عز الدين طباش، المرجع نفسه، ص 58.

² - عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والأنترنت في القانون العربي النموذجي، المرجع السابق، ص 652.

³ - عز الدين طباش، المرجع السابق، ص 58.

1- بالإعتراض على إجراء عملية التحقق في عين المكان .

2- عن طريق رفض تزويد أعضائها أو الأعوان الذين وضعوا تحت تصرفها بالمعلومات والوثائق الضرورية لتنفيذ المهمة الموكلة لهم من طرف السلطة الوطنية، أو إخفاء أو إزالة الوثائق أو المعلومات المذكورة.

عن طريق إرسال معلومات غير مطابقة لمحتوى التسجيلات وقت تقديم الطلب أو عدم تقديمها بشكل مباشر وواضح. "

1- الركن المادي

يتخذ السلوك الإجرامي إتيان أحد الأفعال المنصوص عليها في المادة 61 من القانون 07-18 المتمثلة في:

- فعل الإعتراض على إجراء التحقيق، ومعناه استعمال كل الطرق من أجل عرقلة عمل السلطة الوطنية، فلقد نصت المادة 1/49 من القانون 07-18، أن السلطة الوطنية لها صلاحية القيام بالتحريات المطلوبة ومعاينة المحلات والأماكن التي تتم فيها عملية المعالجة، بإستثناء محلات السكن، وعدم سماح القائم بالمعالجة لأعضاء السلطة الوطنية من القيام بذلك يعتبر جريمة معاقب عليها بموجب المادة 61 من القانون 07-18.¹

- فعل الرفض أو الامتناع عن تزويد أعضاء السلطة الوطنية بالمعلومات والوثائق الضرورية لتنفيذ مهامهم أو القيام بإخفائها أو إزالتها بالمسح أو الحذف إذا كانت المعالجة آلية وإتلافها أو تمزيقها إذا كانت المعالجة يدوية.

- عن طريق إرسال معلومات غير مطابقة لمحتوى التسجيلات، وقت تقديم الطلب أو عدم تقديمها بشكل مباشر وواضح، ويمكن أن تتخذ هذه العرقلة عدة أشكال كإرسال وثائق ناقصة، أو تحتوي أخطاء عمدية، أو إرسالها بعد انتهاء الآجال المحددة من قبل السلطة الوطنية.²

¹ - نسمة بطيحي، المرجع السابق، ص80.

² - يحي تومي، المرجع السابق، ص1547.

2- الركن المعنوي

تعتبر هذه الجريمة عمدية، لتوافر القصد الجنائي العام بعنصرية العلم والإرادة، وذلك من خلال علمه أن الأفعال التي يرتكبها تعد عرقلة لممارسة عمل السلطة الوطنية لمهامها في المراقبة، أو رفضها لإستقبال المراقبين وعدم السماح لهم بإنجاز تفويضهم، ولا يمكن تصور إرتكاب هذه الجريمة عن طريق الخطأ ويظهر ذلك من طبيعة الأفعال المعاقب عليها.¹

3- العقوبة المقررة

عاقب المشرع مرتكب جريمة عرقلة عمل السلطة الوطنية لحماية المعطيات الشخصية بالحبس من ستة أشهر إلى سنتين وبغرامة من 60.000 دج إلى 200.000 دج أو إحدى هاتين العقوبتين، مما يعني إعطاء القاضي السلطة التقديرية في اختيار العقوبة.

ثانيا: جريمة الامتناع عن إعلام السلطة الوطنية عن الانتهاكات المتعلقة بالمعطيات الشخصية في مجال الاتصالات الإلكترونية.

تنص المادة 66 من القانون 07-18 على "يعاقب بالحبس من سنة (1) إلى ثلاث (3) سنوات وبغرامة من 100.000 دج إلى 300.000 دج أو بإحدى هاتين العقوبتين فقط، مقدم الخدمات الذي لا يقوم بإعلام السلطة الوطنية والشخص المعني عن انتهاك للمعطيات الشخصية خلافا لأحكام المادة 43 من هذا القانون."

1- الركن المادي

تقوم هذه الجريمة في حق مقدم الخدمة، فلهذا يتحقق السلوك الإجرامي في حالة امتناع مقدمي الخدمات² بإبلاغ السلطة الوطنية أو الشخص المعني في حالة انتهاك المعطيات الشخصية، والتي يتم اكتشافها أثناء أداء خدمة الاتصالات الإلكترونية³ المفتوحة للجمهور¹، وتتمثل هذه الانتهاكات وفقا لنص

¹ - يحي تومي، المرجع نفسه، ص1547.

² - نصت المادة 10/9 من قانون 07/08 على أن مقدم الخدمات أي ككيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية، أو نظام الاتصالات. أو أي كيان آخر يقوم بمعالجة معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو المستعملين وهو نفس التعريف الموجود في القانون 04/09 الوارد في المادة 2/د".

³ - الإتصالات الإلكترونية ورد تعريفها في المادة 11/3 من ق 07/18 وهو كل إرسال أو ترسل أو استقبال علامات أو

المادة 43 من ق 07-18 عندما تكون المعطيات معرضة للإتلاف أو الضياع أو الإفشاء أو الولوج غير المرخص به، أي عندما تكون محل قرصنة، أو تعرض النظام المعلوماتي الذي يحتويها للاختراق من مجرمي المعلوماتية.

2- الركن المعنوي

تعد جريمة الإمتناع عن إعلام السلطة الوطنية، عن الانتهاكات المتعلقة بالمعطيات الشخصية في مجال الاتصالات الإلكترونية جريمة عمدية، لتوافر القصد الجنائي العام بعنصريه العلم والإرادة، رغم علم مقدمي الخدمة بالانتهاكات التي تمس محتوى المعطيات الشخصية، يمتنع عن إعلام السلطة الوطنية، وكذا الشخص المعني بهذا الانتهاك، وتنتج إرادته إلى إتيان هذا السلوك الإجرامي.

3- العقوبة المقررة

قرر المشرع الجزائري لمرتكب الجريمة المنصوص عليها في المادة 66 من القانون 07-18 بعقوبة الحبس من سنة إلى ثلاث سنوات، وغرامة تتراوح بين 100.000 دج إلى 300.000 دج أو بإحدى العقوبتين.

لقد نص القانون 07-18 على أحكام أخرى متعلقة بالعقاب، التي يمكن تطبيقها على جميع الجرائم الواردة في القانون 07/18، منها ما أجازته المادة 71 على إمكانية تطبيق العقوبات التكميلية الواردة في قانون العقوبات، وكذا إضافة تدبير آخر يتمثل في مسح، كل أو جزء من المعطيات ذات الطابع الشخصي.

كما يمكن مصادرة محل الجريمة بغرض إعادة تخصيصه أو تدميره، وهذا حسب نص المادة 72 من القانون السابق الذكر.

إشارات أو كتابات أو صور أو أصوات أو بيانات أو معلومات، مهما كانت طبيعتها عبر الأسلاك أو الألياف البصرية أو بطريقة كهرومغناطيسية، كما ورد تعريف الإتصال الإلكتروني في المادة 10/ف1 من قانون 04/18 المتعلق بالبريد والاتصالات الإلكترونية، وكذا في المادة 2/ "و" في القانون 04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

¹ - خدمة الاتصالات الإلكترونية للجمهور فيقصد بها طبقا للمادة 10/ف16 من القانون 07-18 " كل خدمة تتمثل كليا أو أساسا في تزويد الجمهور بالاتصالات الإلكترونية، وكذا الخدمات التي تستعمل قدرات شبكات الاتصالات الإلكترونية والتي تتطلب زيادة على خدمة الاتصالات الإلكترونية القاعدية وظائف المعالجة والتخزين."

حيث أقرت المادة 70 من القانون السابق الذكر، مسؤولية الشخص المعنوي وتقرير العقوبة وفقا للقواعد المنصوص عليها في قانون العقوبات، وذلك طبقا للمادة 18 مكرر من قانون العقوبات التي تطلق على الشخص المعنوي هي:

الغرامة التي تساوي من مرة إلى خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي في القانون الذي يعاقب على الجريمة وهو القانون رقم 07/18 وتقدر الغرامة حسب كل جريمة على حدة.

كما عاقب القانون 07-18 على الشروع في ارتكاب إحدى هذه الجرائم، وهذا ما تضمنته المادة 73 حيث جاء فيها "يعاقب على محاولة ارتكاب إحدى الجرائم المنصوص في هذا القانون، بنفس العقوبات المقررة للجريمة التامة.

وفي الأخير نقول رغم تأخر المشرع الجزائري في وضع قانون خاص بالحماية القانونية للمعطيات ذات الطابع الشخصي، إلا أنه استدرك الوضع وسائر التشريعات المقارنة الغربية والعربية منها، فسن القانون 07-18 من أجل التصدي للإنتهاكات التي تتعرض لها المعطيات الشخصية، بسبب الإنتشار الواسع للتكنولوجيا الحديثة واستخدامها في بنوك المعلومات، فالقانون السالف الذكر جاء لتغطية القصور المتعلق بالحماية للحق في الخصوصية الوارد في نصوص متفرقة كقانون العقوبات، والقانون 04-09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، فأحكام هذا القانون صيغت لحماية المعطيات الشخصية سواء كانت آلية أو يدوية، إلا أن أغلب قواعده تدل على المعالجة الآلية، مع إنشاء سلطة وطنية تقوم بالإشراف والرقابة على معالجة هذه المعطيات، فقد أحسن المشرع بإضافة هذا القانون للترسانة القانونية الموجودة، وغايته إرساء سياسة جنائية فعالة لمكافحة الإجرام المعلوماتي.

المطلب الرابع: جرائم الاعتداء على التجارة الإلكترونية

أدت ثورة المعلومات والاتصالات وما رافقها من تطور علمي وتقني إلى ظهور ما يعرف بالتجارة الإلكترونية، التي تعتمد على الوسائل التكنولوجية التي أصبحت أمرا مفروضا وحتميا لإبرام وتنفيذ المعاملات الإلكترونية، وتعتبر ظاهرة التجارة الإلكترونية من أبرز المنجزات في تاريخ البشرية، فهي تعد أداة مهمة في تغيير أنماط الحياة الاقتصادية¹، فبادر المشرع الجزائري بسن أول قانون ينظم المعاملات

¹ - علي ساحلي، راوية مطماطي، التجارة الإلكترونية... قراءة في المفاهيم والأثر الاستهلاكي، مجلة العلوم القانونية والاجتماعية، المجلد 4، العدد 02، جوان 2019، ص 709.

التجارية الإلكترونية وهو القانون 05/18 المؤرخ 10 /05/ 2018¹، حيث تضمن مجموعة من المبادئ والأسس التي تقوم عليها المعاملات الإلكترونية في الجزائر، فقام بإعطاء تعاريف ومفاهيم مختلفة لكل ما يتعلق بالتجارة الإلكترونية (الفرع الأول)، كما خص المستهلك الإلكتروني أهمية كبيرة باعتباره الطرف الضعيف في العقد (الفرع الثاني)، وأقر وسائل الدفع الإلكترونية التي يمكن الإعتماد عليها في التجارة الإلكترونية (الفرع الثالث)، وهذا ما سنحاول التطرق إليه خلال هذا المطلب.

الفرع الأول: التجارة الإلكترونية والجرائم الواقعة عليها

إن الثورة المعلوماتية التي يشهدها العالم اليوم في مجال تكنولوجيا الإعلام والاتصال، والمزايا التي حققتها في جميع المجالات، وكنتيجة لذلك ازداد الترابط بين الأسواق في العالم، مما أضفى على المعاملات التجارية صفة العالمية، وظهرت التجارة الإلكترونية كأسلوب جديد لعرض السلع والخدمات، و عقد الصفقات إلكترونيا بين مختلف الدول² (مفهوم التجارة الإلكترونية)، ومن ناحية أخرى فهي تعد مجالا خصبا لأن تكون محلا للاعتداء عليها (الفقرة الثانية).

الفقرة الأولى: مفهوم التجارة الإلكترونية

يعتبر مصطلح التجارة الإلكترونية حديث النشأة، لا يمكن تحديد مفهومه بصفة دقيقة، فهو يتكون من جزأين هما الأول مصطلح "التجارة" ويعني كل نشاط تجاري وإقتصادي يتم من خلاله تداول السلع والخدمات، ذلك وفقا لقواعد ونظم متفق عليها، أما الثاني "الإلكترونية" ويقصد به القيام بأداء النشاط الإقتصادي عن طريق إستعمال وسائل تكنولوجيا الاتصال الحديثة³ كشبكة الأنترنت، الهواتف المحمولة، مما يدفعنا إلى تعريف التجارة الإلكترونية (أولا) والتطرق لأهم أشكالها (ثانيا).

أولا: تعريف التجارة الإلكترونية

لا يوجد تعريف جامع ومتفق عليه للتجارة الإلكترونية، هذا ما جعل كل من الفقهاء والمختصون

¹ - القانون رقم 05-18 المؤرخ في 10 ماي 2018، يتعلق بالتجارة الإلكترونية، الجريدة الرسمية للجمهورية الجزائرية، عدد 28، الصادرة بتاريخ 2018/05/16.

² - بودالية بوراس، واقع التجارة الإلكترونية في الجزائر، مجلة البصائر للدراسات القانونية والإقتصادية، المجلد 1، عدد 1، 2021، ص 20.

³ - آمال مشتي، التجارة الإلكترونية في الجزائر، مجلة البحوث والدراسات القانونية والسياسية، المجلد 1، عدد 13، 2018، ص 241.

والمنظمات يجتهدون لإدراج العديد من التعريفات، ومن أهم التعريفات عرفت المنظمة العالمية للتجارة مصطلح التجارة الإلكترونية على أنها " إنتاج وتوزيع وتسويق وبيع السلع والخدمات أو تسليمها عبر الوسائل الإلكترونية ¹ فيما عرفت اللجنة الأوروبية على أنها "أداء الأعمال إلكترونيا، حيث تقوم على أساس التبادل الإلكتروني للبيانات مكتوبة كانت أو مرئية أو مسموعة، كما أنها تتضمن العديد من الأنشطة التجارية الخاصة بتبادل السلع والخدمات، وإتمام عمليات البيع والشراء والتسليم بالنسبة للمحتويات الرقمية والتحويلات الإلكترونية للأموال والفواتير الإلكترونية، وعمليات التسويق وخدمات ما بعد البيع، وهي تشمل كلا من السلع والخدمات وكذلك الأنشطة التقليدية وغير التقليدية ²."

وفيما عرفها جانب من الفقه عرفها على أنها "عملية ترويج وتبادل السلع وإتمام صفقاتها باستخدام وسائل الاتصال وتكنولوجيا تبادل المعلومات الحديثة عن بعد، خاصة شبكة الأنترنت دون حاجة إلى النقاء الأطراف والتقاءهم في مكان ما، وذلك سواء أمكن تنفيذ الالتزامات المتبادلة إلكترونيا، أم تطلب الأمر تنفيذها بشكل مادي ملموس ³."

بالرجوع للمشرع الجزائري نجده عرف التجارة الإلكترونية من خلال المادة 1/6 من القانون 18/05 المتعلق بالتجارة الإلكترونية بقوله " النشاط الذي يقوم بموجبه مورد إلكتروني باقتراح أو ضمان أو توفر سلع وخدمات من بعد لمستهلك إلكتروني عن طريق الاتصالات الإلكترونية."

إذا فالتجارة الإلكترونية هي " عبارة عن ممارسة عدة عمليات من إنتاج وتسويق، وبيع وشراء للمنتجات والخدمات، والتي تتم بين المتعاملين الإقتصاديين سواء كانوا أفراد أو مؤسسات أو حكومات، وذلك باستخدام الوسائط الإلكترونية ⁴ كالفاكس أو التلكس أو الهاتف المحمول والأنترنت.

ثانيا: أشكال التجارة الإلكترونية

للتجارة الإلكترونية عدة أشكال، ويمكن توضيح ذلك من خلال المصنوفة التي استعملها كوبل(coppel) والتي تتمثل فيما يلي:

¹ - إبراهيم أحمد عبد الخالق الدوري، التجارة الإلكترونية دراسة تطبيقية على المكتبات، مكتبة الملك فهد الوطنية، الرياض، ط 2، 2010، ص، ص 29-30.

² - أحمد عبد الخالق، التجارة الإلكترونية والعولمة، منشورات المنظمة العربية للتنمية الإدارية، مصر، د ط، 2008، ص 32.

³ - عمر عبد الفتاح علي يونس، جوانب قانونية للتعاقد الإلكتروني في إطار القانون المدني، د.د نشر، ط 1، 2009، ص 85.

⁴ - ساحلي علي، مطماطي راوية، المرجع السابق، ص 702.

- 1 - التجارة الإلكترونية بين الحكومات وبعض البعض (G2G)، ويتم هذا النوع من الأعمال بين حكومات الدول المختلفة، وقد تم تطبيقه وتفعيله في عام 2005، كما يمكن لهذه الأعمال أن تتم داخل نفس الدولة بين أجهزتها الحكومية.
- 2- التجارة الإلكترونية بين المنظمات business to business (B2B) وتمثل جميع الجهات المشاركة في هذه الفئة من التجارة الإلكترونية منظمات أعمال.
- 3 - التجارة الإلكترونية بين المنظمات والمستهلكين business to consumer (B2C) ويشمل هذا النوع جميع مبيعات التجزئة الإلكترونية للمنتجات والخدمات من منظمات الأعمال إلى المستهلكين.
- 4- التجارة الإلكترونية بين المستهلكين consumer to consumer (C2C) يتم هذا النوع من البيع بين المستهلكين فيما بينهم.¹

الفقرة الثانية: صور الإعتداء على التجارة الإلكترونية

تعتبر شبكة الأنترنت سلاح ذو حدين في مجال التجارة الإلكترونية، فمن جهة يعتبر مجالا سهلا ومتطورا للمبادلات التجارية لما يوفره من سرعة وأمان للتاجر، ومن جهة أخرى يعد من أسهل الأدوات لإرتكاب الجرائم، ومن بينها الإعتداء على مواقع التجارة الإلكترونية أو بما يعرف بأسماء النطاق، فأغلب التشريعات المقارنة تشترط لممارسة النشاط التجاري الإلكتروني وجود موقع إلكتروني، أو صفحة على الأنترنت وهذا ما تطلبه المشرع الجزائري في القانون 18/05 المتعلق بالتجارة الإلكترونية بموجب المادة 8 منه²، وبما أن التجارة الإلكترونية تعتمد على الحواسيب وأنظمتها المعلوماتية، فإن الإعتداء على مواقعها يعد إعتداء على نظم المعالجة الآلية للمعطيات، ومن ثم فإن إختراق موقع التجارة الإلكترونية هو إختراق لنظامها المعلوماتي³، لهذا سوف نتناول مفهوم الموقع الإلكتروني (أولا) ثم نرجع إلى أهم جرائم الإعتداء عليها (ثانيا)

¹ - محمد التوجي، الحماية الجنائية من الجرائم المرتكبة بواسطة الهاتف النقال، اطروحة لنيل شهادة الدكتوراه، كلية الحقوق والعلوم السياسية، جامعة احمد دراية، أدرار، الجزائر، 2018 . 2019، ص 81.

² - تنص المادة 8 من قانون 18/05 المتعلق بالتجارة الإلكترونية على أنه " يخضع نشاط التجارة الإلكترونية للتسجيل في السجل التجاري أو في سجل الصناعات التقليدية والحرفية، حسب الحالة، ونشر موقع إلكتروني أو صفحة إلكترونية على الأنترنت، مستضاف في الجزائر بامتداد "com.dz" يجب أن يتوفر الموقع الإلكتروني للمورد الإلكتروني على وسائل تسمح بالتأكد من صحته"

³ - مريم خليفي، الحماية الجنائية لمواقع التجارة الإلكترونية عبر الأنترنت، مجلة العلوم القانونية، المجلد 2، عدد 1، 2011، ص 171.

أولاً: مفهوم المواقع الإلكترونية (أسماء النطاق)

مع تطور التجارة الإلكترونية، ظهرت إشارات يطلق عليها أسماء مواقع الأنترنت، كذلك أسماء النطاق، أو أسماء الحقول ولقيت هذه الأسماء إهتمام كبير من طرف الدول، حيث يستخدم الموقع في مجال التجارة الإلكترونية لغرض تجاري أو اقتصادي، ليميز المؤسسة أو موقع التاجر من غيره من التجار والمؤسسات¹، وهو يشبه العلامة التجارية بالنسبة للتجارة التقليدية.²

وتعرف أسماء النطاق، أو مواقع الأنترنت بأنها " مجموعة من الحروف أو الأرقام تستخدم للدلالة على عنوان، أو موقع لحاسوب يستخدمه شخص طبيعي أو معنوي على شبكة الأنترنت، لتحديد هذا الموقع وتمييزه عن غيره من المواقع الأخرى عبر الأنترنت.³، كما تعرف كذلك "الارتباط الدولي المتصل بشبكة الحواسيب حول العالم".⁴ أما المشرع الجزائري فقد عرف اسم النطاق بأنه "عبارة عن أحرف أو أرقام مقيسة ومسجلة لدى السجل الوطني لأسماء النطاق، وتسمح بالتعرف والولوج إلى الموقع الإلكتروني".⁵

اسم النطاق غالبا يتكون من ثلاثة أجزاء رئيسية هي: الأول وهو الجزء الثابت دائما ويتمثل في المقطع WWW وهي اختصار للعبارات التالية (world, wide, web) ويشير إلى البروتوكول المستخدم ويحدد أن الموقع يتواجد على شبكة الأنترنت.

أما الجزء الثاني يمكن أن يحمل إسمن أو رمز، أو إختصاص للمؤسسة، أو الشخص أو الجهة

¹ - ناصر حمودي، الحماية الجنائية للتجارة الإلكترونية، المرجع السابق، ص73.

² - رغم علاقة الشبه بين إسم النطاق والعلامة التجارية إلا أن هناك اختلاف بينهما فأسماء النطاق هو مجرد عنوان أو اسم نطاق معين على شبكة الأنترنت أي موقع يمكن من خلاله الوصول إلى مؤسسة اقتصادية أو تجارية، أما العلامة التجارية فهي علامة أو شعار يتخذه الصانع أو التاجر لتمييز منتجاته عن المنتجات الأخرى، وقد أفرد لها القانون حماية من الاعتداء عليها، أنظر هدى حامد قشقوش، الحماية الجنائية للتجارة الإلكترونية عبر الأنترنت، دار النهضة العربية، القاهرة، د ط، 2000، ص 82 .

³ - حمدون الشيخ، إبراهيم يامة، حماية أسماء النطاق، ورقة علمية قدمت في إطار الملتقى الوطني حول المستهلك والاقتصاد الرقمي: ضرورة الانتقال وتحديات الحماية، المركز الجامعي عبد الحفيظ بوصوف، ميله، المنعقد في الفترة 23-24 أبريل 2018، د رص.

⁴ - حسين بن سعيد الغافري، الجرائم الواقعة على التجارة الإلكترونية، ص 12 منشور على الموقع الإلكتروني <https://www.eastlow.com>، أطلع عليه بتاريخ 2018/09/15 الساعة 14. h30

⁵ - انظر المادة 8/16 من قانون 18/05 المتعلق بالتجارة الإلكترونية المؤرخ في 10 ماي 2018.

صاحبة الموقع مثل Google، فيما يعتبر الجزء الثالث أكثر أهمية عن باقي الأجزاء، ويعرف بإسم نطاق المستوى الأعلى top – lovel Domain وهو يتكون من فئتين هما: الأولى هي نطاق المستوى الأعلى العام¹ (gtld) الذي يدل على هوية أو نشاط أو شكل صاحب الموقع مثل (com)، (org)، (net)، وهي توجه بالدرجة الأولى إلى المستهلكين في كل دول العالم، الثانية تتمثل في نطاقات المستويات العليا لرموز الدول² (cc tcd) وهي تستخدم للدلالة على إسم القطاع أو المنطقة الجغرافية.³، مثل dz للجزائر eg مصر Fr فرنسا.

ثانيا: الإعتداء على أسماء النطاق

سبق القول أن التجارة الإلكترونية تعتمد على تقنية المعالجة الآلية للمعطيات، فإن الإعتداء على المواقع الإلكترونية لا يخرج عن كونه أحد تطبيقات الإعتداء على نظم المعالجة الآلية للمعطيات، لم يتضمن القانون 18/05 المتعلق بالتجارة الإلكترونية على تجريم الإعتداء على المواقع، ولكن يمكن أن تكون محلا لتطبيق صور للجرائم الواردة في الفصل السابع مكرر من قانون العقوبات خاصة جريمتي الدخول والبقاء غير المشروع، وجرائم التلاعب بمعطيات نظم التجارة الإلكترونية، وهي الجرائم المنصوص عليها في المواد من 394 مكرر إلى 394 مكرر 7، والتي تناولناها بالدراسة في المبحث الأول من هذا الفصل فيمكن الرجوع إليها تفاديا للتكرار.

ولكن يمكن ذكر لأبرز الطرق التي يتم فيها الإعتداء على مواقع الأنترنت على سبيل المثال مايلي:

1- تدمير المواقع

بإمكان مجرمي المعلوماتية خاصة منهم محترفي الإجرام، تدمير أيا موقع موجود عبر شبكة الأنترنت، وذلك بإستعمال عدة وسائل منها ضخ آلاف الرسائل الإلكترونية إلى الموقع المستهدف مما يؤدي إلى تفجيره وإتلاف بياناته ومعلوماته، مما قد يكبد الشركات والمؤسسات خسائر مادية ومعنوية، وقد تعرض موقع Hotmail عام 2002 لبعض الهجمات أدت إلى تدميره، وتعرضه إلى خسائر مالية تعدت

¹ - اختصارا بالإنجليزية ل: General top level Domain

² - اختصارا بالإنجليزية ل: Country code top level domain

³ - حسين بن سعيد الغافري، المرجع السابق، ص 13.

ملايين الدولارات.¹

2 - تشويه صورة الموقع

صورة أخرى من صور الإضرار بمواقع التجارة الإلكترونية، وتتمثل في تغيير محتوى الصفحة الرئيسية للموقع بصورة أخرى فتجعلها مزيفة، ويقصد من ورائها إبراز المجرم المعلوماتي لقدراته التقنية وإظهار الضعف للموقع المستهدف، والإضرار بسمعة الجهة المالكة للموقع.

ويتم تشويه صورة الموقع عن طريق الدخول بهوية مخفية (anonymous) حيث تمكن هذه الطريقة المخترق من الحصول على كلمة السر الخاصة بأحد المشرفين على الموقع المستهدف، أو من يملكه حتى تعديل محتويات الموقع، والعمل على فك تشفيرها.²

3 - حجب خدمة الأنترنت

" الوصول إلى هذا الموقع غير ممكن " قد تقي الرسالة السابقة أن الموقع الذي تحاول أن تزوره، تعرض لهجمات حجب الخدمة خاصة إذا كان واحدا من المواقع الكبرى، يعني ظهور مثل هذه الرسالة في موقعها خسارة عشرات الآلاف من الدولارات.³

4 - انتحال شخصية الموقع

ويقصد بها انتحال صفة مؤسسة أو كيان يمتلك مواقع أنترنت، وعلى سبيل المثال يمكن إنتحال صفة مواقع التي تعالج أموال الدفع الإلكتروني، وذلك من أجل القيام بعمليات غير قانونية كالوصول إلى بيانات بطاقات الدفع التي يتعامل بها الأشخاص حين دخولهم للموقع، أو كشف بيانات حساباتهم البنكية للقيام بتحويل الأموال من هذه الحسابات إلى حسابات أخرى.

¹ - حسين الغافري، السياسة الجنائية في مواجهة الجريمة عبر الأنترنت، المرجع السابق، ص 261.

² - حسين الغافري، الجرائم الواقعة على التجارة الإلكترونية، المرجع السابق، ص، ص 17-18.

³ - فادي سالم، مقال بعنوان موقعك في ويب في مهبط الاختراق، صحيفة الحوار المتمدن الإلكترونية، العدد رقم 15 بتاريخ 2001/12/23، منشور على الموقع <http://www.ahewar.org/debat/show.Art.asp.aid=> 550 أطلع عليه بتاريخ 2018/12/25 على الساعة 15h30.

الفرع الثاني: المستهلك الإلكتروني¹

أدى بروز التجارة الإلكترونية إلى ما يعرف بالمستهلك الإلكتروني، والذي يمثل الطرف الضعيف في العلاقة التعاقدية، والخطر الذي يتعرض له المستهلك في إطار التجارة الإلكترونية أكبر من الخطر المحتمل في التجارة التقليدية، هذا ما جعل حمايته حتمية، لهذا لجأت أغلب الدول إلى إقرار حماية خاصة له، وهذا ما اتجه إليه المشرع الجزائري سواء من خلال قانون 05/18 المتعلق بالتجارة الإلكترونية، وقانون 09/18² المتعلق بحماية المستهلك وقمع الغش المعدل والمتمم، فمن خلال هذا الفرع نتناول مفهوم المستهلك (الفقرة الأولى) ثم صور الإعتداء عليه (الفقرة الثانية).

الفقرة الأولى: مفهوم المستهلك الإلكتروني

المستهلك في مجال معاملات التجارة الإلكترونية هو نفسه المستهلك في مجال عمليات التعاقد التقليدية، وهذا يعني أنه يتمتع بنفس الحقوق في التجاريتين، مع الأخذ في الاعتبار خصوصية العقد الإلكتروني وكونه من العقود التي تبرم عن بعد عبر شبكة الأنترنت.³

أولاً: تعريف المستهلك الإلكتروني

عرف المجلس الإقتصادي والإجتماعي للأمم المتحدة المستهلك بصفة عامة، بأنه " الشخص الذي يقوم بشراء السلع والخدمات من السوق لاستعمالها"⁴، ويعرف أيضاً " كل شخص يتعاقد بقصد إشباع حاجاته الشخصية أو العائلية وليس الغرض من الحصول على هذه السلع والخدمات للاستعمال المهني أو التجاري."⁵ أما بالنسبة للمستهلك الإلكتروني فيعرف بأنه " كل شخص طبيعي أو معنوي يتعاقد بوسيلة

¹ - إن مفهوم "المستهلك" من صنع المشرع الأمريكي وكان على يد الرئيس الأمريكي جون كينيدي، حيث دعا مجلس الشيوخ في خطابه بتاريخ 15 مارس 1962 بضرورة التحديد والأخذ بالحقوق الأربعة التي يجب أن يتمتع بها المستهلك الإعلام، الأمن، الاختيار وأن يسمع له ويؤخذ برأيه أنظر في ذلك يمينة بليمان، الإشهار الكاذب أو المضلل، مجلة العلوم الانسانية، المجلد ب، عدد 32، 2009، ص 291.

² - قانون رقم 18 / 09 المؤرخ في 10 يونيو 2018 المتعلق بحماية المستهلك وقمع الغش، الجريدة الرسمية للجمهورية الجزائرية، عدد 35، الصادرة بتاريخ 13 يونيو 2018.

³ - خالد ممدوح إبراهيم، حماية المستهلك في العقد الإلكتروني، دار الفكر الجامعي، الاسكندرية، ط1، 2008، ص 23.

⁴ - خالد ممدوح إبراهيم، أمن المستهلك الإلكتروني، دار الفكر الجامعي، الاسكندرية، ط1، 2008، ص 24.

⁵ - محمد محمد حسن الحسيني، حماية المستهلك الإلكتروني في القانون الدولي الخاص، دار النهضة العربية، القاهرة، د ط، 2012، ص 28.

الكثرونية بشأن المنتجات التي تلزمه هو وذويه، والتي لا ترتبط بمهنته أو حرفته.¹

والمشرع الجزائري لم يكن بعيدا عن هذه التطورات، فمصطلح المستهلك عرف بموجب القانون 03/09² المتعلق بحماية المستهلك قمع الغش، من خلال المادة 1/3 على أنه " كل شخص طبيعي أو معنوي يقتني بمقابل أو مجانا سلعة أو خدمة موجهة للاستعمال النهائي من أجل تلبية حاجاته الشخصية أو تلبية حاجة شخص آخر أو حيوان متكفل به"، وفي ذات السياق عرف المستهلك الإلكتروني في المادة 03/6 من القانون 05/18 المتعلق بالتجارة الإلكترونية على أنه "هو كل شخص طبيعي أو معنوي، يقتني بعوض أو بصفة مجانية سلعة أو خدمة عن طريق الاتصالات الإلكترونية من المورد الإلكتروني بغرض الاستخدام النهائي".³

ومن خلال التعريفين السابقين نستخلص أن التعاريف في كلا القانونين متشابهة لكن الفرق الوحيد بينهما في الوسيلة التي يستعملها المستهلك الإلكتروني.

ثانيا: مبررات حماية المستهلك الإلكتروني

يمكن إجمال أهم هذه المبررات في:⁴

1- التطور الحديث في شبكة الأنترنت

تعد شبكة الأنترنت من أحدث خدمات التقدم التقني التي تعتمد على تفاعل المستهلك مع الهاتف الذكي أو جهاز الحاسوب، مما ينبغي أن يقود إلى تحسين الروابط التجارية بين المنتج والمستهلك بهدف الحصول على أفضل أداء للممارسات التجارية الإلكترونية، ويتمثل ذلك في عدم قدرة المستهلك على معاينة المبيع بطريقة حقيقية، أو الالتقاء مع المنتج في مجلس عقدي تقليدي.

¹ - أبو عمر مصطفى أحمد، الالتزام بالإعلام في عقود الاستهلاك - دراسة في القانون الفرنسي والتشريعات العربية - دار الجامعة الجديدة، الإسكندرية، 2010، ص، ص 94.

² - قانون رقم 03/09 المؤرخ في 25 فبراير 2009 المتعلق بحماية المستهلك وقمع الغش، الجريدة الرسمية للجمهورية الجزائرية، عدد، الصادرة بتاريخ 08 مارس 2009.

³ - المادة 6 فقرة 3 من قانون 05/18 المؤرخ في 10 ماي 2018.

⁴ - محمد خميخم، الحماية الجنائية للمستهلك في عقود التجارة الإلكترونية، اطروحة نيل شهادة الدكتوراه علوم، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2017 - 2018، ص، ص 15-16.

2 - افتقار المستهلك إلى التنوير المعلوماتي والتقني

إن عدم معرفة المستهلك بشبكة الأنترنت، بالإضافة إلى المشاكل التي قد تواجه المستهلك عند التعمق في هذه الشبكة ويتمثل ذلك من خلال ما يواجهه المستهلك من عدم معرفته لما يحصل أمامه في الشاشة الصغيرة كما يؤدي إلى وقوع المستهلك بحيل وخداع قراصنة الأنترنت من خلال المواقع الوهمية أو التعاقد الوهمي.

3 - حاجة المستهلك إلى الخدمات الإلكترونية

إن الخدمات الإلكترونية وما تقدمه للمستهلك من منتجات وخدمات ذات جودة عالية بأسعار معقولة، بسبب كثرة المواقع التجارية الإلكترونية، مما يزيد في طابع المنافسة بين هذه المواقع على تقديم الأفضل للمستهلك، تزيد من إقبال المستهلكين على هذه الخدمات.

الفقرة الثانية: صور الإعتداء

يتعرض المستهلك الإلكتروني في إطار التجارة الإلكترونية للعديد من المخاطر، سواء أثناء إبرامه للعقد الإلكتروني أو أثناء تنفيذه من طرف المورد الإلكتروني، مما جعل المشرع الجزائري يحيط المستهلك الإلكتروني بحماية خاصة في حالة محاولة الإعتداء عليه، سواء بموجب القانون 05/18 المتعلق بالتجارة الإلكترونية، أو القانون 09/18 المتعلق بحماية المستهلك وقمع الغش المعدل والمتهم.

وسوف نتطرق إلى صور هذه الجرائم كما يلي:

أولاً: جريمة مخالفة الإشهار الإلكتروني غير المشروع

تقوم التجارة الإلكترونية على ركيزة أساسية تتمثل في الإشهار الإلكتروني، لما له من أهمية بارزة في قيام المعاملات التجارية الإلكترونية، فقد يلجأ المورد الإلكتروني إلى استخدام أساليب دعائية منطوية على غش وخداع المستهلك، من أجل التأثير على نفسيته وجذبه لأجل التعاقد والريح على حسابه، مما قد يلحق ضرراً جسيماً¹، فإذا كان الإشهار بهذا الوصف فإنه يعد جريمة رصد المشرع الجزائري لها عقوبات.

¹ - منى أبوبكر الصديق، الإلتزام بإعلام المستهلك عن المنتجات، دار الجامعة الجديدة، الإسكندرية، د ط، د.س.ن، ص

ولقد عرف الإشهار الإلكتروني بموجب المادة 6/هـ من القانون 18-05 المتعلق بالتجارة الإلكترونية على أنه " كل إعلان يهدف بصفة مباشرة إلى الترويج بين سلعة أو خدمات عن طريق الاتصالات الإلكترونية." و منه نظم المشرع الجزائري الإشهار الإلكتروني بمقتضى المواد 30 و 31 و 32 و 34 من القانون 18-05 المتعلق بالتجارة الإلكترونية، وكل مخالفة لتلك النصوص تقوم في حق المورد الإلكتروني جريمة منصوص عليها في المادة 40 من القانون السالف الذكر.

لهذا فقد نصت المادة 40 من ق 05/18 على أنه " دون المساس بحقوق الضحايا في التعويض يعاقب بغرامة من 50.000 دج إلى 500.000 دج كل من يخالف أحكام المواد 30 و 31 و 32 و 34 من هذا القانون. "

تضمن النص القانوني مجموعة من الصور والسلوكات المخالفة للالتزامات التي فرضها القانون، يرتكبها المورد الإلكتروني عند استعماله وعرضه للإشهار عن طريق الاتصالات الإلكترونية، لذا نتناول أركان هذه الجريمة كالآتي:

1 - الركن المادي

يقوم الركن المادي عن طريق إثبات المورد الإلكتروني أفعال وسلوكات، إذا أخل بشروط حددتها النصوص القانونية الواردة بموجب المواد 30، 31، 32، و 34 من القانون 18-05، تقوم في حقه جريمة معاقب عليها في المادة 40 من قانون التجارة الإلكترونية، وتتمثل في استخدام الإشهار الإلكتروني دون توافر شروطه، الاستبيان المباشر بإرسال رسائل عبر الاتصالات الإلكترونية إلى شخص لم يبد موافقته المسبقة لتلقي هذا الاستبيان، عدم وضع منظومة إلكترونية تسمح للشخص بعدم تلقي أي إشهار إلكتروني.

أ- استخدام الإشهار الإلكتروني دون توافر شروطه

وضع المشرع الجزائري مجموعة من الشروط يجب توافرها في الإشهار الإلكتروني، والتي أسماها بمقتضيات الإشهار الإلكتروني، فتضمنتها المادة 2/30 من القانون 18-05 المتعلق بالتجارة الإلكترونية والتي تتمثل في:¹

- أن يكون الإشهار محددًا بوضوح كرسالة تجارية أو إشهارية .

¹ - المادة 30 من القانون 18-05 المتعلق بالتجارة الإلكترونية.

- أن تسمح بتحديد الشخص الذي تم تصميم الرسالة لحسابه.
- ألا تمس بالآداب العامة والنظام العام.
- أن تحدد بوضوح ما إذا كان العرض التجاري يشمل تخفيضا أو مكافآت أو هدايا، في حالة ما إذا كان هذا العرض تجاريا أو تنافسيا أو ترويجيا.
- التأكد من أن جميع الشروط الواجب استيفاؤها للاستفادة من العرض التجاري، ليست مضللة ولا غامضة.
- وعليه نقول أن المورد الإلكتروني تقع عليه عاتقه توضيح الرسالة الإشهارية الإلكترونية، فإذا خالف هذا الالتزام يؤدي إلى قيام جريمة في حقه، وهي مخالفة شروط الإشهار الإلكتروني الواردة في المادة 40 من القانون 05-18.

ب- مخالفة إلزامية أخذ موافقة المستهلك الإلكتروني في تلقي رسائل الاستبيان (الإشهار غير المرغوب فيه)

لم يكتف المشرع الجزائري بتنظيم الإشهار الإلكتروني بتبيان شروطه، بل أضاف شرط آخر بالزام المورد الإلكتروني بحصوله على الموافقة المسبقة للمستهلك، في استعمال بياناته في إرسال رسائل الاستبيان المرسل إليه وهذا ما تناولته المادة 31 من القانون 05-18 المتعلق بالتجارة الإلكترونية، ويعتبر البريد الإلكتروني من وسائل الاتصال المهمة بالنسبة للمورد لإرسال رسائل الاستبيان المباشر لمجموعة من المستهلكين، لكن على النقيض من ذلك أن المستهلك الإلكتروني لا يقبل هذه الرسائل، وينزعج منها ولا يرغب فيها، علما أنه لم يسبق التعامل مع المرسل الذي يرسل تلك الاستبيانات¹، وعليه يكون المرسل محل ارتكاب جريمة الإشهار الإلكتروني غير المرغوب فيه.

يعرف الفقه الإشهار الإلكتروني غير المرغوب فيه بأنه " إغراق صندوق البريد الإلكتروني بعدة نسخ من رسالة واحدة في عدة محاولات لفرض الرسالة على الناس الذين لا يرغبون في استلامها." أو هو الرسائل غير المرغوب فيها لعدد كبير من الناس.²

¹ منيرة بن جدو، الحماية الجنائية لتعاملات التجارة الإلكترونية، أطروحة لنيل شهادة دكتوراه في الطور الثالث، كلية الحقوق والعلوم السياسية، جامعة محمد لمين دباغين، سطيف 2، 2021-2022، ص30.

² - ماشاء الله الزوي، المواجهة الجنائية للبريد الإلكتروني الدعائي المزجج أو المضلل، ورقة علمية مقدمة في إطار المؤتمر

وعليه فإن الركن المادي لهذه الجريمة، يتمثل في مخالفة إلزامية أخذ موافقة المستهلك في تلقي رسائل الاستبيان المباشر، وهي تعرف بمخالفة نظام $open - in^1$ ، ويقصد به حصول المعلن على إذن مسبق من طرف المستهلك، حيث يلتزم قبل إرساله أية رسالة إليه، يجب أن يحصل على رضائه المسبق، فإذا لم يرغب في تلقي هذه الرسائل فلا يمكن للمعلن أن يرسلها.²

ج- عدم وضع منظومة إلكترونية تسمح للشخص بعدم تلقي أي إشعار إلكتروني

فرضت المادة 32 من القانون 05-18 التزام على المورد الإلكتروني، تلزمه بوضع منظومة إلكترونية يسمح من خلالها لكل شخص طبيعي للتعبير بعدم تلقي أي إشعار إلكتروني عن طريق الاتصالات الإلكترونية، دون مصاريف أو مبررات تقع على المستهلك الإلكتروني³، وكذا احترام رغبة المستهلك عند اعتراضه هذه الإشهارات وذلك من خلال تسليم وصل استلام عن طريق الاتصال الإلكتروني يؤكد من خلاله للشخص المعني تسجيل طلبه، مع اتخاذ التدابير اللازمة لتلبية رغبته في غضون 24 ساعة⁴، ومخالفة لهذه الالتزامات تقوم الجريمة في حق المورد الإلكتروني بمجرد عدم توفير نظام يسمى بنظام $opt-out$ المعروف باسم نظام الرفض أو الاعتراض، فمن خلال هذا النظام يستطيع المورد إرسال إشهاراته إلى المستهلك عبر البريد الإلكتروني دون الحصول على الموافقة المسبقة على الإرسال، فإذا أبدى المستهلك اعتراضه وعدم رغبته في تلقي الإشهارات، وجب عليه إرسال هذه الرغبة إلى المرسل إليه، وعلى هذا الأخير إحترام هذه الرغبة.⁵

ب- الركن المعنوي

إن الركن المعنوي لهذه الجريمة غير متطلب، بحيث يكفي توافر السلوك الإجرامي بإعتبارها من

الدولي الرابع للجرائم الإلكترونية، المنعقد في الفترة 24-25 مارس 2017، مركز جيل البحث العلمي، طرابلس، ص 10.
¹ - حسين جفالي، الطاهر دلول، الحماية الجنائية من الإشهار الإلكتروني غير المرغوب فيه في التشريع الجزائري، المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد 2، عدد 2، 2018، ص 528.

² - صالح خوالف، زينب كريم، دور قانون 05-18 المتعلق بالتجارة الإلكترونية في حماية المستهلك الإلكتروني من الإشهار الإلكتروني غير المرغوب فيه، مجلة دراسات وأبحاث المجلة العربية في العلوم الإنسانية والاجتماعية، مجلد 12، عدد 3، 2020، ص 255.

³ - المادة 32 من القانون 05-18 المتعلق بالتجارة الإلكترونية.

⁴ - وهذا ما نصت عليه المادة 32 فقرة 2 من قانون 07-18.

⁵ - منيرة بن جدو، المرجع السابق، ص 31.

الجرائم الإقتصادية التي لها خصوصية، فالجريمة تتوافر إما لإرتكاب خطأ عمدي في صورة سوء النية، أو لإرتكاب فعلا غير عمدي لمجرد إهمال بسيط أو عدم الحيطة، التي تترتب عن عدم أخذ موافقة المستهلك في الاستبيان المباشر أو عدم تمكينه من الاعتراض على الرسائل الإشهارية الإلكترونية.¹

ج- العقوبة المقررة

عاقب المشرع مرتكب جنحة الإشهار الإلكتروني غير المشروع، بموجب المادة 40 من قانون 18-05، وأفرد لها عقوبة مالية بين 50.000 دج إلى 500.000 دج، أما في حالة العود فتضاعف العقوبة حيث تصبح الغرامة من 100.000 دج إلى 1.000.000 دج.²

ثانيا: صور التجريم الواقعة على حق المستهلك الإلكتروني في الاعلام

يعتبر إعلام المستهلك من الوسائل القانونية الحديثة لحماية المستهلك في التعاقد عبر الأنترنت، وهذا الإلزام يقع على عاتق المورد الإلكتروني، حيث يقوم بإعلام المستهلك الإلكتروني بجملة من المواصفات المتعلقة بالسلعة محل التعاقد قبل إبرام العقد حتى يتم ذلك بناء على رضا واضح وصريح، وحماية للمستهلك الإلكتروني من كل مورد إلكتروني يخالف هذا الإلزام تقع في حقه قيام مسؤولية الجزائية من خلال قانون التجارة الإلكترونية.

نصت المادة 39 من قانون 18-05 على أنه " يعاقب بغرامة من 50.000 دج إلى 500.000 دج كل مورد إلكتروني يخالف أحد الالتزامات المنصوص عليها في المادتين 11 و12 من هذا القانون، كما يجوز للجهة القضائية التي رفعت أمامها الدعوى أن تأمر بتعليق نفاذه إلى جميع منصات الدفع الإلكترونية لمدة لا تتجاوز ستة (6) أشهر. "

قبل أن نعالج أركان هذه الجريمة يجب التطرق إلى تعريف الحق في الإعلام وما يمكن ملاحظته أن المشرع لم يعرف الحق في الإعلام في القانون 18-05، وإنما أشار ضمنا من خلال الالتزامات الواقعة على المورد الإلكتروني قبل التعاقد وذلك بموجب المادة 12 من القانون السابق الذكر، وعرف الحق بالإعلام على أنه "جعل المستهلك في أما عن ضد مخاطر المنتج الذي يشتريه سواء كان سلعة أو خدمة

¹ - حسين جفال، الطاهر دلول، المرجع السابق، ص 531.

² - تنص المادة 48 من قانون 18.05 على أنه " يضاعف مبلغ الغرامة في حالة تكرار نفس الجريمة خلال مدة لا تتجاوز إثني عشر (12) شهرا من تاريخ العقوبة المتعلقة بالجريمة السابقة."

وهو ما يفرض على المهني التزاما بإحاطة المستهلك علما بظروف العقد وملابساته.¹ ويعرف الفقه هذا الالتزام بأنه " التزام يقع على ظروف المقابل للمستهلك في عقود التجارة الإلكترونية في مرحلة ما قبل إبرام العقد وفي مرحلة تكوينه أو إبرامه ويستمر حتى إلى إبرام العقد."²

ألزم قانون التجارة الإلكترونية على المورد الإلكتروني بموجب المادتين 11 و12 التزامات في حالة الإخلال بها تقوم في حقه صور الجريمة الواردة في المادة 39 من 05-18.

1 - جريمة مخالفة النظام القانوني للعرض التجاري الإلكتروني

إشترط المشرع الجزائري بموجب المادة 10 من ق 05-18، أن تكون كل معاملة تجارية إلكترونية مسبقة بعرض إلكتروني حتى يتم إعلام المستهلك بهذا العرض، وأوجب على المورد الإلكتروني مجموعة من الالتزامات يجب توافرها في ذمته وهي المنصوص عليها في المادة 11 من قانون 05 - 18. ومخالفة هذه الالتزامات يعد مخالفة لنظام العرض التجاري الإلكتروني وفقا للمادة 39 من القانون السابق الذكر، وهو بذلك يمثل اعتداء على حق المستهلك في الإعلام.³

أ - الركن المادي

يتمثل السلوك الإجرامي في هذه الجريمة في مخالفة الشروط الإلزامية الواجب توافرها في العرض التجاري الإلكتروني، من حيث أن يكون مرئيا ومفهوما وسهل القراءة، كذلك يقوم السلوك الإجرامي بمجرد إغفال المورد الإلكتروني أحد البيانات الإلزامية التي يتطلبها العرض التجاري، كعدم ذكر طبيعة وخصائص وأسعار السلع أو الخدمات المقترحة، أو شروط العقد أو شروط الضمان أو كفاءات مصاريف التسليم، أو مخالفة شروط العرض التجاري الإلكتروني كاشتراط العرض أن يكون مفهوم لدى المستهلك أي بلغة يفهمها المستهلك أي بطريقة مرئية ومقروءة ومفهومة وعليه إذا خالف المورد الإلكتروني هذه الالتزامات قامت الجريمة وفقا لما جاء في المادة 39 من قانون التجارة الإلكترونية.⁴

¹ - نبيل محمد أحمد صبيح، حماية المستهلك في التعاملات الإلكترونية، مجلة الحقوق، جامعة الكويت، العدد 2، 2008، ص 206.

² - خالد ممدوح إبراهيم، حماية المستهلك الإلكتروني، المرجع السابق، ص 95.

³ - حسين جفالي، الحماية الجنائية لحق المستهلك الإلكتروني في الاعلام في التشريع الجزائري، المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد الثالث، العدد الأول، 2019، ص 137.

⁴ - حسين جفالي، المرجع نفسه، ص 140.

ب- الركن المعنوي

جريمة مخالفة النظام القانوني للعرض التجاري الإلكتروني، جريمة عمدية تقتضي توافر القصد الجنائي العام علم المورد الإلكتروني، بأنه يخالف الشروط الإلزامية في العرض التجاري الواردة في المادة 11 من القانون 05-18، وإتجاه إرادته لإتيان السلوك الإجرامي.

ج- العقوبة المقررة

عاقب المشرع الجزائري على جريمة مخالفة النظام القانوني للعرض التجاري الإلكتروني بغرامة مالية تتراوح بين 50.000 دج إلى 500.000 دج، وفي حالة العود فتضاعف العقوبة تصبح الغرامة من 100.000 دج إلى 1.000.000 دج، إلى جانب ذلك يجوز للقاضي فرض عقوبات تكميلية إختيارية حيث تأمر الجهة القضائية التي رفعت أمامها الدعوى أن تأمر بتعليق نفاذ المورد الإلكتروني إلى جميع منصات الدفع الإلكتروني لمدة لا تتجاوز ستة أشهر.

2 - جريمة مخالفة مراحل التعاقد الإلكتروني

تقوم هذه الجريمة في حق المورد الإلكتروني في حالة إخلاله بالالتزامات الواردة في المادة 12 من قانون التجارة الإلكترونية.

أ- الركن المادي

تتمثل صور السلوك الإجرامي في عدم وضع الشروط التعاقدية اللازمة في متناول المستهلك، ففي مجال التجارة الإلكترونية تكون السلع معروضة على شكل صور، بحيث لا يستطيع المستهلك تفحص هذه السلع، كذلك في بعض الأحيان يصعب على المستهلك قراءة بيانات هذه السلع وشروطها وبالتالي معرفة شروط التعاقد حول المنتج المعروض للبيع عبر شبكة الأنترنت، لذا يجب على المورد الإلكتروني تقديم كل المعلومات والإرشادات التي تسمح للمستهلك تكوين فكرة واضحة عن العقد ومحلّه،¹ قد تكون من خلال إرسالها عبر البريد الإلكتروني، أو عرضها في صفحة مستقلة مع ضرورة التنويه عليها في صفحة العرض الرئيسية أو بتخصيص مكان لها على صفحة العرض.²

¹ - مريم خليفي، الالتزام بالإعلام الإلكتروني وشفافية التعامل في مجال التجارة الإلكترونية، مجلة دفاتر السياسة والقانون، العدد 4، 2011، ص 206 .

² - حسين اجفالي، المرجع السابق، ص 141.

يقوم الركن المادي أيضا في حالة عدم تمكين المستهلك من مراجعة الطلبية، قد ألزم المشرع الجزائري بموجب المادة 12 من التحقق من الطلبية من طرق المستهلك خاصة فيما يخص بماهية المنتج، أو الخدمات المطلوبة السعر الإجمالي والوحدوي، الكميات المطلوبة،¹ كذلك يحق له مراجعة شروط العقد أيضا.

أما الصورة الأخيرة تتمثل في عدم تمكين المستهلك من تأكيد الطلبية، لم ينص المشرع في قانون التجارة الإلكترونية عن كيفية ممارسة هذا الحق، وإنما فرض على المورد الإلكتروني إلزامية إعلام المستهلك طريقة تأكيد الطلبية.²

ب- الركن المعنوي

بالنظر للطبيعة المادية لجريمة مخالفة مراحل التعاقد الإلكتروني فإن الركن المعنوي غير متطلب بحيث يكفي توافر السلوك المادي المجرم.

ج- العقوبة المقررة

عاقب المشرع على هذه الجريمة في المادة 39 من القانون 18-05، بغرامة مالية 50.000 دج إلى 500.000 دج، في حالة العود تضاف الغرامة حيث تصبح من 100.000 دج إلى 1.000.000 دج، كما أعطى للجهة القضائية إمكانية فرض عقوبات تكميلية منها منع المورد الإلكتروني من الولوج في منصات الدفع الإلكتروني لمدة ستة أشهر.

الفرع الثالث: وسائل الدفع الإلكتروني وصور الاعتداء عليها

فرض ظهور التجارة الإلكترونية، ضرورة إيجاد أنظمة مصرفية تتلاءم مع الطبيعة الإلكترونية الافتراضية والرقمية، فعملت المؤسسات المالية على تطوير وسائل الدفع التقليدية، التي تعتمد على دعائم ورقية إلى شكل يتلاءم مع الطبيعة الإلكترونية عبر الأنترنت،³ إلا أنه بالرغم من المزايا التي وفرتها وسائل الدفع الإلكتروني وتزايد التعامل بها عبر الأنترنت، فقد صاحبه ذلك نموا في الجرائم المصاحبة

¹ - المادة 12 من قانون 18.05 المتعلق بالتجارة الإلكترونية.

² - حسين جفالي، المرجع السابق، ص 142.

³ - رشيدة أكسوم عيلام، المركز القانوني للمستهلك الإلكتروني، أطروحة لنيل شهادة دكتوراه طور الثالث، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2018، ص 271.

لإستخدامها.

الفقرة الأولى: مفهوم وسائل الدفع الإلكتروني

إن ظهور التجارة الإلكترونية أدى إلى بروز مصطلح وسائل الدفع الإلكتروني، التي لا يمكن الإستغناء عليها في المعاملات التجارية الإلكترونية، وكذا تعد نواة التجارة الإلكترونية والإقتصاد الرقمي، لهذا نتطرق إلى تعريفها (أولا) والتطرق إلى أنواعها (ثانيا)

أولا: تعريف وسائل الدفع الإلكتروني

اختلف الفقه والتشريع في إيجاد تعريف جامع ومانع لوسائل الدفع الإلكتروني، وهذا بسبب حداثتها وتطورها المستمر، ومن أهم هذه التعاريف تعريف اللجنة الأوروبية حيث عرفت على أنها " عبارة عن قيمة نقدية مخزنة إلكترونيا على حاملا إلكترونيا، مثل بطاقة ذات رقاقة أو ذاكرة حاسوب تصدر مقابل إيداع مبلغ مالي قيمته لا تقل عن القيمة النقدية الصادرة، ويتم قبولها كوسيلة دفع من قبل كل المؤسسات مع تلك المصدرة لها وتكون تحت تصرف مستعملها كبديل إلكتروني للقطع والأوراق النقدية".¹ كما كذلك عرفت على أنها "مجموعة الأدوات التي تصدرها البنوك والمؤسسات المالية كوسيلة دفع، والتي تتمثل في البطاقات البنكية والنقود الإلكترونية والشبكات الإلكترونية، والبطاقات الذكية".² أما بخصوص المشرع الجزائري فقد نص على تعريف وسائل الدفع الإلكترونية بموجب الأمر رقم 03/11 والمتعلق بقانون النقد والقرض وذلك في نص المادة 69 منه والتي نصت على " تعتبر وسائل الدفع كل الأدوات التي تمكن كل شخص من تحويل الأموال مهما يكن السند أو الأسلوب التقني المستعمل".³، ولكن بصدر القانون 05/18 المتعلق التجارة الإلكترونية المؤرخ في 10 ماي 2018 فقد عرفها في الباب الخاص بالأحكام العامة بموجب نص المادة 6 فقرة 5 بقوله " كل وسيلة دفع مرخص بها طبقا

¹ - article 2-c, de la recommandation n° 97/489/CE de la commission européenne du 30/7/1997 concernant les opérations effectuées d'instrument de paiement électronique : « ... instrument de monnaie électronique : « un instrument de paiement rechargeable autre qu' un instrument de paiement d' accès à distance qu' il s' agisse d'une carte prépayée ou d'une mémoire d'ordinateur sur lesquelles des unités de valeur sont stockées électroniquement qui permet à son titulaire d'effectuer les types d'opérations décrites à l'article 1^{er} paragraphe 1 ., ... » J . O. D . C . E n° L 208/52, .02/08/1997, .p52.

² - كريمة صراع، المرجع السابق، ص 58.

³ - الأمر رقم 11/03 المؤرخ في 26/08/2003 المتعلق بالنقد والقرض المعدل والمتمم، الجريدة الرسمية للجمهورية الجزائرية، عدد 52 الصادرة بتاريخ 27 غشت 2003.

للتشريع المعمول به تمكن صاحبها من القيام بالدفع عن قرب أو بعد عبر منظومة الكترونية¹ فالمشروع اعترف صراحة بتطبيق وسائل الدفع الإلكتروني، تأسيسا بالتشريعات المقارنة، وكذا إنتشار التعامل بهذه الوسائل خاصة بعد ظهور بعض المتاجر الإلكترونية في السوق الجزائرية.²

ثانيا: أنواع وسائل الدفع الإلكتروني

ظهرت وسائل الدفع الإلكتروني نتيجة التطور التكنولوجي ومحدودية وسائل الدفع التقليدية في إتمام مختلف العمليات الإلكترونية، ويوجد العديد من وسائل الدفع في الجزائر نذكر منها:

1- بطاقة السحب ما بين البنوك la carte cib والتي بدأ العمل بها منذ 1997 عن طريق شبكة الخدمات الإلكترونية المصرفية بين البنوك، حيث يمكن للزبون حامل هذه البطاقة دفع ثمن المشتريات من السلع والخدمات عبر الشبكة التابعة للتجار.

2- البطاقات الدولية: تمنح بعض البنوك الموجودة في الجزائر بطاقات دولية تسمح بإجراء العمليات بالعملة الصعبة على الموزعات الآلية للأموال، ونقاط البيع الإلكترونية مثل amex card , visa card , master card....

3- البطاقة البريدية الذهبية: يمكن لحامل هذه البطاقة أن يجري مختلف العمليات، بواسطتها كسحب الأموال، دفع وتسديد قيمة المشتريات والخدمات مثل تسديد فاتورة الكهرباء وفاتورة الهاتف.³

الفقرة الثانية: صور الإعتداء على وسائل الدفع الإلكترونية

لم يسن المشرع الجزائري نصوص تشريعية تحمي الإعتداء على وسائل الدفع الإلكترونية، وإنما اقتصر تدخله على حماية نوع من البطاقات الإلكترونية غير المتعلقة بالدفع الإلكتروني وهي " بطاقة

¹ - المادة 5/6 من قانون 05/18 المؤرخ في 10 ماي 2018 المتعلق بالتجارة الإلكترونية.

² - من بين نماذج المتاجر الإلكترونية الناشطة في سوق التجارة الإلكترونية في الجزائر منها :

سوق واد كينيسا ouedk miss .com، موقع اشريلي Echerily .com، أو بصيغة الدفع الإلكتروني عن طريق e.pay.dz، موقع قيديني gruidini.com للمزيد من المعلومات أنظر خالد بن سامي واقع التجارة الإلكترونية والامداد في الجزائر، مجلة أداء المؤسسات الجزائرية، العدد 12، 2017، ص 213.

³ - زينب نافع، جميل أحمد، التجارة الإلكترونية في الجزائر، طموحات كبيرة وإنجازات متواضعة، مجلة دراسات في الاقتصاد وإدارة الأعمال، المجلد 3، عدد6، 2020، ص7.

الشفاء"، الصادرة عن صندوق الضمان الاجتماعي¹، والتي تدخل لحمايتها القانون 08-01 المتعلق بالتأمينات الاجتماعية²، حيث نصت المادة 06 مكرر منه على أنه "تثبت صفة المؤمن له إجتماعيا ببطاقة إلكترونية..."، ولقد أفرد لها المشرع حماية جنائية في حالة سوء استعمالها من خلال النص على الجرائم والعقوبات المقررة لها المنصوص عليها في المواد من 93 مكرر 2 إلى 93 مكرر 6، لهذا سوف نتطرق إلى مختلف هذه الجرائم.

أولا: جريمة الإستعمال غير المشروع للبطاقة الإلكترونية

نصت المادة 93 مكرر 2 من ق08-01 على "دون الاخلال بالعقوبات المنصوص عليها في التشريع المعمول به يعاقب بالحبس من سنتين (2) إلى خمس (5) سنوات وبغرامة من 100.000 دج إلى 200.000 دج كل من يسلم أو يستلم بهدف الاستعمال غير المشروع البطاقة الإلكترونية للمؤمن له إجتماعيا أو المفتاح الإلكتروني لهيكل العلاج أو المفتاح لمهني الصحة".

تقوم هذه الجريمة على الركن المادي الركن المعنوي وعقوبة مقررة لها.

1 - الركن المادي

إن السلوك الإجرامي لهذه الجريمة يتحقق بقيام المؤمن له بفعل التسليم، ونعني به منح البطاقة الإلكترونية للغير بغرض استعمالها لحسابه الشخصي، والحصول على منافع منها إضرار بهيئة الضمان الإجتماعي، مثل إستعمال البطاقة الإلكترونية من قبل الغير في تعويض الأدوية بإسم المؤمن له، وعادة ما يتم هذا الأمر بعلم وموافقة المؤمن له.³

و يقصد بفعل الإستلام أي تسلم الغير للبطاقة الإلكترونية، من أجل إستخدامها على نحو غير مشروع، وقد يكون الغير المسؤول على المفتاح الإلكتروني بالنسبة لهيكل العلاج، أو مهني الصحة أو يكون شخص آخر يمكنه الإستفادة من البطاقة الإلكترونية.

¹ - محمد خليفة، دراسة نقدية لنصوص جرائم أنظمة المعالجة الآلية للمعطيات في قانون العقوبات الجزائري، المجلة النقدية، المجلد 13، عدد 1، 2018، ص 66.

² - قانون رقم 08-01 المؤرخ في 23-01-2008 يتم القانون رقم 83-11 المؤرخ في 02/07/1983 المتعلق بالتأمينات الإجتماعية، الجريدة الرسمية للجمهورية الجزائرية، عدد 04 الصادرة بتاريخ 27/01/2008.

³ - يزيد بوحليط، المرجع السابق، ص 174.

2- الركن المعنوي

تعد جريمة الإستعمال غير المشروع للبطاقة الإلكترونية، جريمة عمدية لتوافر القصد الجنائي العام المتمثل في العلم والإرادة، أي علم الجاني بأنه يسلم ويستلم بهدف الإستعمال الغير المشروع لبطاقة الإلكتروني، مع إتجاه الإرادة لإتيان السلوك الإجرامي.

3 - العقوبة المقررة

عاقب المشرع على هذه الجريمة، بعقوبة سالبة للحرية مع الغرامة والتي تتمثل بالحبس من سنتين إلى خمس سنوات وبغرامة مالية من 100.000 دج إلى 200.000 دج.

ثانيا: جريمة التلاعب في معطيات البطاقة الإلكترونية أو المفتاح الإلكتروني

تنص المادة 93 مكرر 3/ 1 على " دون الاخلال بالعقوبات المنصوص عليها في التشريع المعمول به يعاقب بالحبس من سنتين (2) إلى خمس (5) سنوات وبغرامة من 500.000 دج إلى 100.000 دج كل من يقوم عن طريق الغش بتعديل أو حذف كلي للمعطيات التقنية و/ أو الإدارية المدرجة في البطاقة الإلكترونية للمؤمن له اجتماعيا أو في المفتاح الإلكتروني لهيكل العلاج أو في المفتاح الإلكتروني لمهني الصحة..."

تقوم الجريمة على الركن المادي والمعنوي وعقوبة مقررة لها.

1 - الركن المادي

حددت المادة 93 مكرر 3/ 1 الأفعال التي تدخل في نطاق التجريم، وتتمثل في قيام الجاني عن طريق الغش بتعديل أو الحذف الكلي أو الجزئي للمعطيات أو المعلومات المدرجة في البطاقة الإلكترونية، سواء أكانت هذه المعلومات تقنية أو إدارية، وفعل التعديل نعني به تغيير المعطيات المتضمنة في بطاقة الشفاء عن طريق إستبدالها بمعلومات مغايرة¹، أما الحذف فهو شطب أو محو المعلومات أو إزالتها بصفة جزئية أو كلية من النظام المعلوماتي، ولم يكتف المشرع بتجريم المساس بمضمون البطاقة، بل تعداه إلى تجريم الاعتداء على المفتاح الإلكتروني لهيكل العلاج أو المفتاح لمهني الصحة بالتعديل أو الحذف.

¹ - نجا عباوي، الحماية الجزائية لبطاقة الشفاء الإلكترونية، مجلة الحقيقة، العدد 41، 2017، ص 304.

2- الركن المعنوي

جريمة التلاعب بمعطيات البطاقة الإلكترونية أو المفتاح الإلكتروني جريمة عمدية، ويستشف ذلك من عبارة "عن طريق الغش"، فهي تتطلب توافر القصد الجنائي العام الذي يقوم على العلم والإرادة، علم الجاني أن الأفعال التي يؤتيها تشكل اعتداء على سلامة المعطيات الموجودة داخل البطاقة، واتجاه إرادته إلى ارتكاب السلوك المجرم.

3 - العقوبة المقررة

دون الإخلال بالعقوبات المنصوص عليها في التشريع المعمول به يعاقب بالحبس من سنتين إلى خمس سنوات وبغرامة من 500.000 دج إلى 100.000 دج وهذا ما نصت عليه المادة 93 مكرر 1/3 من ق 01-08.

ثالثا: جريمة التلاعب في برمجيات البطاقة الإلكترونية أو المفتاح الإلكتروني

تنص المادة 93 مكرر 2/3 على ".... يعاقب بنفس العقوبة، كل من أعد أو عدل أو نسخ بطريقة غير مشروعة البرمجيات التي تسمح بالوصول أو إستعمال المعطيات المدرجة في البطاقة الإلكترونية للمؤمن له اجتماعيا أو المفتاح الإلكتروني لهيكل العلاج أو في المفتاح الإلكتروني لمهني الصحة..."

1 - الركن المادي

يتحقق السلوك الإجرامي بإتيان الجاني إحدى الأفعال الواردة في المادة السالفة الذكر، وهي الإعداد التعديل والنسخ، ويقصد بالإعداد قيام الجاني بتصميم برنامج معلوماتي شبيه بالبرامج المدونة على البطاقة الإلكترونية، قصد الوصول إلى معطيات البطاقة الإلكترونية أو المفتاح الإلكتروني، وهذا الفعل يرتكبه كل شخص له خبرة في مجال البرمجيات والإعلام الآلي،¹ أما النسخ فيقصد به إنشاء بطاقة تماثل البطاقة الأصلية بحيث تكون مشتملة على الخصائص ذاتها.²

2 - الركن المعنوي

¹ - يزيد بوحليط، المرجع السابق، ص 175.

² - نجاة عباوي، المرجع السابق، ص 309.

جريمة عمدية تتطلب القصد الجنائي العام بعنصره العلم والإرادة، فيجب على الجاني أن يعلم بأن الأفعال المجرمة بالمادة 93 مكرر 2/3 تشكل إعتداء على سلامة المعطيات والمعلومات الخاصة بالبطاقة أو المفتاح الإلكتروني، كما تتجه إرادته إلى القيام بهذه الأفعال.

3 - العقوبة المقررة

عاقب المشرع على هذه الجريمة بالحبس من سنتين إلى خمس سنوات وبغرامة مالية من 500.000 دج إلى 100.000 دج، ونظر لخطورة الأفعال الواردة في هذه الجريمة، عاقب المشرع على مجرد الشروع فيها وذلك بموجب الفقرة الأخيرة من المادة 93 مكرر 3 يعاقب بنفس العقوبة، على المحاولة في ارتكاب الجرح المذكورة في الفقرتين الأولى والثانية أعلاه.

رابعاً: جريمة الإتجار غير المشروع في البطاقة الإلكترونية أو المفتاح الإلكتروني

تنص المادة 93 مكرر 4 على أنه " دون الإخلال بالعقوبات المنصوص عليها في التشريع المعمول به، يعاقب بالحبس من سنتين (2) إلى خمس سنوات(5) وبغرامة من 500.000 دج إلى 5.000.000 دج كل من ينسخ أو يصنع أو يحوز أو يوزع بطريقة غير مشروعة البطاقة الإلكترونية للمؤمن له اجتماعياً أو المفتاح الإلكتروني لهيكل العلاج أو المفتاح الإلكتروني لمهني الصحة."

1 - الركن المادي

يقوم الركن المادي بإرتكاب إحدى الأفعال الواردة في المادة 39 مكرر 4 من القانون 08-01 السابق الذكر، والمتمثلة في النسخ الصنع والحيازة، و يقصد بالنسخ إنشاء بطاقة تماثل البطاقة الأصلية، أما الصناعة فهي إنشاء بطاقة جديدة من قبل الجاني ونسبتها إلى الجهة المخولة بإنشائها،¹ وتتمثل الحيازة بامتلاك الجاني للبطاقة الإلكترونية، أو المفتاح الإلكتروني بنية التملك والتصرف فيها بحرية دون علم صاحبها.

2 - الركن المعنوي

جريمة عمدية تتطلب القصد الجنائي العام، فيجب على الجاني العلم بأن هذه الأفعال تشكل النشاط الجرمي المعاقب عليه قانوناً، وتتصرف إرادته إلى ارتكاب هذه الأفعال.

¹ - نجا عباوي، المرجع السابق، ص 309 .

3- العقوبة المقررة

يعاقب المشرع على جريمة الإتجار غير المشروع في البطاقة الإلكترونية أو المفتاح الإلكتروني، بالحبس من سنتين إلى خمس سنوات وبغرامة من 500.000 دج إلى 5.000.000 دج.

إلى جانب العقوبات المقررة للشخص الطبيعي على إرتكابه للجرائم السابقة الذكر، تناولت المادة 93 مكرر 5 عقوبة الشخص المعنوي الذي يرتكب إحدى الجناح المنصوص عليها في المادة 93 مكرر 3 و 93 مكرر 4 أعلاه بغرامة تساوي خمس (5) مرات المبلغ الأقصى للغرامة المقررة للشخص الطبيعي.

اقتصر المشرع الجزائري حمايته الجنائية إلا لبطاقة الشفاء دون غيرها من البطاقات، ولهذا ندعو المشرع بالإسراع إلى سن نصوص تجرم بطاقات الدفع الإلكتروني في قانون خاص، على غرار التشريعات المقارنة لدورها الفعال في المعاملات الإلكترونية.

خلاصة القول نثمن مسعى المشرع الجزائري بسنه قانون ينظم المعاملات التجارية الإلكترونية، وهذا لإنتشار هذا النوع من التجارة، وتماشيا مع التشريعات الدولية التي أصبحت تعتمد على هذه الأخيرة في مبادلاتها التجارية، فالقانون 05-18 المتعلق بالتجارة الإلكترونية في الجزائر مازال في بداية الطريق لتطبيقه، كما يشبوه عدة نقائص وثغرات قانونية.

واصل المشرع الجزائري من أجل تدعيم سياسته الجنائية في مكافحة الجريمة الإلكترونية، فلم يكتف بسياسة التجريم والعقاب، بل بادر إلى إيجاد آليات إجرائية تساهم في مواجهة الإجرام المعلوماتي الخطير، وهذا سوف نتناوله بالدراسة في الباب الثاني من الدراسة.

الباب الثاني

الجوانب الإجرائية لمكافحة

الجريمة الالكترونية

الباب الثاني: الجوانب الإجرائية لمكافحة الجريمة الإلكترونية

ظهرت أنواع من الجرائم تتسم بالخطورة لم يعرفها الإنسان من قبل والتي أصبحت تشكل تهديدا حقيقيا بأفراد المجتمع، برزت جراء التطور العلمي والتكنولوجي الذي يعيشه العالم اليوم وهي الجريمة الإلكترونية، وقد عبرت الخبرة بمركز المعلومات الوطني الأمريكي روي جودسون بقولها "لقد أصبحت الجريمة أكثر قوة بفضل التقنية الحديثة"¹، فالجريمة الإلكترونية قلبت الموازين فألغت الحدود الجغرافية للدول بحيث أصبح العالم قرية صغيرة، كما أثرت على القواعد الجنائية الموضوعية والاجرائية التي تتصف بطابعها المستقر والثابت سواء في ظل النظم القانونية اللاتينية أو الأنجلوسكسونية، وترتب على ذلك إشكالات قانونية سواء من الناحية الموضوعية التي تناولناها في الباب الأول من البحث أو من الناحية الإجرائية التي أصبحت غير قادرة على مواجهة هذه الجريمة، فالآليات التقليدية للاستدلال والتحري عاجزة أمام هذه الجرائم الحديثة مما حتم البحث عن أساليب أخرى تكون فعالة وتساير التطور الإجرامي، فسارعت دول العالم الى سن قوانين تتناسب مع هذه الجرائم وهذا ما سعى إليه المشرع الجزائري من خلال إصدار قوانين منها القانون رقم 06-20 المؤرخ في 20/09/2006 الذي سن إجراءات مستحدثة خاصة بالبحث والتحري، تتمثل في إجراءات اعتراض المراسلات وتسجيل الأصوات، والتقاط الصور وإجراء التسريب، كما سن القانون 09-04 المؤرخ في 05/08/2009 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها نص على إجراءات تتلاءم مع هذا النوع من الإجرام، فمن خلال هذا الباب سوف نتطرق إلى أهم الإجراءات التي خصها المشرع لمكافحة الجريمة الإلكترونية، وذلك من خلال مواجهة الجريمة الإلكترونية وفقا لقانون الاجراءات الجزائية في (الفصل الأول) ثم نتناول في (الفصل الثاني) مواجهة الجريمة الإلكترونية وفقا لقانون 09-04.

¹ - علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الالي، المرجع السابق، ص7.

الفصل الأول: مواجهة الجريمة الإلكترونية وفقا لقانون الإجراءات الجزائية

لا تختلف سير الدعوى العمومية بشأن الجريمة الإلكترونية، عن المراحل التي تمر بها الدعوى العمومية في الجريمة التقليدية، إلا أن الإجراءات المتبعة في البحث والتحري عن هذه الجريمة، تتميز بإجراءات خاصة لخصوصية هذه الأخيرة، ولارتكابها في مسرح إفتراضي إلكتروني أو في مجال مفرغ يختلف كلياً عن المسرح التقليدي، الذي ترتكب جرائمه في عالم مادي ملموس سهل الإثبات، يلعب فيه السلوك المادي دوراً كبيراً ومهماً، أما الجريمة الإلكترونية أدلتها غير مرئية، وصعوبة الوصول إليها بالوسائل التقليدية لسهولة إتلافها وتدميرها من المجرم المعلوماتي، مما تجد السلطات القضائية المختصة بإجراءات البحث والتحري صعوبة كبيرة في إستخلاص الدليل منها بإعتبارها نبضات إلكترونية غير مرئية.

وهذا ما أدى بالمشروع الجزائري إلى الإسراع وعلى غرار التشريعات المقارنة إلى مواجهة هذا النوع من الجرائم، والبحث عن أساليب جديدة لمكافحتها، وللتغلب على تحديات هذه الجريمة قام بتعديل قانون الإجراءات الجزائية بموجب القانون 06-22 المؤرخ في 20 ديسمبر 2006، والذي من خلاله تم سن إجراءات تتلاءم مع طبيعة هذه الجريمة.

وعليه سوف نتطرق في هذا الفصل إلى تكييف القواعد الإجرائية التقليدية لإستخلاص الدليل الإلكتروني في (المبحث الأول) والإجراءات المستحدثة لإستخلاص الدليل الإلكتروني في (المبحث الثاني).

المبحث الأول: تكييف القواعد الإجرائية التقليدية لإستخلاص الدليل الإلكتروني

نظراً للطابع الخاص للجريمة الإلكترونية يستلزم وجود إجراءات تتماشى وطبيعة هذه الجرائم، لهذا نجد المشرع الجزائري ولمواجهة هذه الجريمة، حاول في بادئ الأمر تطويع الإجراءات التقليدية المنصوص عليها في قانون الإجراءات الجزائية من أجل إثبات هذه الجريمة، فمن خلال هذا المبحث نتطرق بالدراسة إلى إجراء تلقي الشكاوى والبلاغات في (المطلب الأول) وكذا المعاينة والخبرة التقنية في (المطلب الثاني) والتطرق إلى أحكام الشهادة في الجريمة الإلكترونية في (المطلب الثالث) وفي الأخير نعرض إلى الإختصاص القضائي في (المطلب الرابع).

المطلب الأول: الشكوى والبلاغ في الجريمة الإلكترونية

من أهم الإشكالات التي تواجه السلطات القضائية المختصة بمكافحة الجريمة الإلكترونية، هو إحجام المجني عليه عن الإبلاغ عن هذه الجرائم، ومرد ذلك خشية الضحايا من خسارة المستخدمين لديهم، أو فقد الثقة العامة من عملاتهم¹، ويترتب على ذلك عدم اكتشاف هذا النوع من الجرائم، مما يشكل عائقا في إتخاذ إجراءات التحقيق بصددتها، ورغم هذه الإشكالية فإن الجريمة الإلكترونية تكون محل متابعة بمجرد وصول نبأ وقوعها إلى الجهات القضائية المعنية، إما عن طريق تقديم شكوى أو بلاغ فالسؤال الذي يمكن طرحه هل إجراءات الشكوى نفسها في الجريمة الإلكترونية؟ هذا ما نتناوله في المطلب من خلال تلقي الشكاوى والبلاغات بصفة عامة (الفرع الأول) وكيفية تلقي الشكوى والبلاغ في الجريمة الإلكترونية في (الفرع الثاني).

الفرع الأول: تلقي البلاغات والشكاوى بصفة عامة

تظل الجريمة مستترة عادة ما لم يتم التبليغ عنها إلى الجهات القضائية المختصة، بتحريك الدعوى العمومية والتحقيق فيها، حسب القوانين والأنظمة المعمول بها²، إذن تعتبر الشكوى والبلاغ إشعار بوقوع جريمة ما، وقد أناط المشرع الجزائري لضباط الشرطة القضائية تلقي الشكاوى والبلاغات، وهذا ما نصت عليه الفقرة الأولى من المادة 17 من ق.إ.ج.ج على أنه "يباشر ضباط الشرطة القضائية السلطات الموضحة في المادتين 12 و13 ويتلقون الشكاوى والبلاغات ويقومون بجمع الاستدلالات وإجراء التحقيقات الابتدائية". كما نصت المادة 18 من ق.إ.ج.ج على " يتعين على ضباط الشرطة القضائية أن يحرر محاضر بأعمالهم وأن يبادروا بغير تمهل إلى إخطار وكيل الجمهورية بالجنایات والجنح التي تصل إلى علمهم " ولمعرفة كيفية التبليغ عن هذه الجرائم لابد أولا التعرض إلى تعريف البلاغ ثم إلى الشكوى ثانيا.

أولا: البلاغ

لم يعط المشرع تعريفا للبلاغ ولكنه استخدم ألفاظا للتعبير عنها، كما ألزم على ضابط الشرطة القضائية تلقيها مهما كانت طبيعتها، وقد تصدى لها الفقه فعرف البلاغ أنه " إخبار السلطات المختصة

¹ - أحمد المراغي، المرجع السابق، ص 118.

² - محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي والأنترنت، بحث مقدم إلى مؤتمر القانون والكمبيوتر والأنترنت، المجلد الثاني، جامعة الإمارات العربية المتحدة، أبو ظبي، 2000، ص 20.

عن وقوع جريمة أو أنها على وشك الوقوع أو هناك اتفاقا جنائيا على ارتكابها" ¹ عرف أيضا أنه " إعلام أو نقل الجريمة سواء حصل من شخص مجهول أو معلوم إلى مسموع الشرطة القضائية".²

لم يحدد القانون طريقة معينة لتلقي البلاغ فقد يتم بكافة السبل التي توصل المعلومات إلى الجهات المختصة بالبحث والتحري، فقد يكون كتابيا أو شفويا بمعرفة المجني عليه أو غيره ممن شاهدوا وقوع الجريمة أو وصل إليهم خبر وقوعها، كما لم يشترط القانون أن يكون مصدر البلاغ من معلوم الهوية، فقد يكون من مجهول الهوية ويجب على ضابط الشرطة القضائية في الحالتين ولاسيما الأولى منها تناول البلاغ بجدية كاملة، ³ كما أن المشرع الجزائري أوجب على الأفراد التبليغ عند علمهم بارتكاب جرائم الماسة بالأمن والدفاع الوطني وإلا تطبق عليهم أحكام المادة 91 من قانون العقوبات.

وحتى يكون البلاغ وافيا لا بد أن تتوفر فيه التالية: نوع الحادثة، تحديد المجني عليه، زمن وقوع الجريمة ومكانها، بيان أسباب ودوافع إرتكاب الجريمة واخيرا تحديد الشخص المتهم.⁴

ويستحب أن يكون المبلغ في الجريمة الإلكترونية على درجة مقبولة من الإلمام والمعرفة بالجوانب الفنية للحاسوب، حتى يتمكن من تقديم معلومات تصف الحادث بدقة حتى يتمكن ضابط الشرطة القضائية مباشرة البحث والتحري عنها، ويجب على المبلغ أن يقدم وصفا علميا للنشاط الإجرامي مع بيان الأسماء واللغات والبرامج وأنواع الأجهزة المستخدمة وأماكنها قدر المستطاع⁵، مما يستلزم أن يكون متلقي البلاغ على دراية ومعرفة بتقنية المعلومات حتى يتمكن من مناقشة المبلغ في الكثير من جوانب الجريمة محل البلاغ.

بالرغم من الدور الهام للبلاغ في كشف الجرائم الواقعة في المجتمع، إلا أنه يثير في مجال تحريك الدعوى العمومية في الجرائم الإلكترونية عدة إشكالات منها الإحجام على عن التبليغ الذي يشكل أكبر

¹ - خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة، عمان، ط 1، 2011، ص 192.

² - محمد محد، ضمانات المشتبه فيه أثناء التحريات الأولية، جزء 2، دار الهدى، الجزائر، ط1، 1991، ص 112.

³ - نبيلة هبة هروال، الجوانب الاجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، دار الفكر الجامعي، الاسكندرية، ط 1، 2007، ص 179.

⁴ - نبيلة هبة هروال، المرجع نفسه، ص 181.

⁵ - محمد الأمين البشري، التحقيق في الجرائم المستحدثة، جامعة نايف العربية للعلوم الأمنية، ط1، 2004، ص 111.

عائقا أمام إكتشاف الجريمة واتخاذ إجراءات التحقيق بصدها¹، وفي الغالب نجد أن المؤسسات والشركات التجارية الكبرى هم ضحايا هذه الجرائم فيترددون عن الإبلاغ خوفا على سمعتهم ومكانتهم في المجتمع. مما أدى إلى إيجاد اقتراحات تكفل تعاون المجني عليه في كشف هذه الجرائم، ومن أهم الاقتراحات حيث مطالبة الولايات المتحدة الأمريكية بأن تفرض النصوص المتعلقة بجرائم الحاسوب التزاما على عاتق موظفي الجهة المجني عليها بالإبلاغ عما يصلهم من أخبار عن وقوع تلك الجرائم على تلك الجهة مع تقدير جزاء عن الإخلال غير أن الاقتراح قوبل بالرفض عند عرضه على لجنة خبراء مجلس أوروبا.

ثانيا: الشكوى

وما قيل عن البلاغ يصدق على الشكوى فنجد المشرع الجزائري لم يعط تعريفا للشكوى، فقد عرفها الفقه بأنها "إجراء يقوم بواسطته المجني عليه بإبلاغ نبأ وقوع جريمة عليه غلى السلطة المختصة." ² كما عرفت أيضا بأنها "البلاغات المقدمة عن الجرائم والتي يدعي فيها مقدمها بحقوق مدنية فإذا لم تشمل على الإدعاء تعد من قبيل التبليغ." ³

لا تختلف أحكام الشكوى في الجريمة الإلكترونية عنها في الجريمة التقليدية، إذ لا يجوز تحريك الدعوى العمومية في ذلك إلا بعد تقديم شكوى من المجني عليه أو المتضرر منها أو وكيله القانوني. ويتبين لنا من خلال ما تناولناه أن هناك إختلاف بين الشكوى والبلاغ، هذا الأخير يقصد به الإخطار عن الجريمة الذي يقدمه أي شخص، أما الشكوى فتقدم من المجني عليه أو المتضرر من الجريمة، فالبلاغ إذن هو حق لكل شخص حتى وإن لم يصبه ضرر من الجريمة.

الفرع الثاني: كيفية الشكوى والبلاغ في الجريمة الإلكترونية

إن أهمية البلاغ تعطي للمجني عليه ولغيره من الأفراد في الجرائم الإلكترونية دورا لا يستهان به لأنه قد يكون السبيل الوحيد لكشف هذه الجرائم، وهو دور يعطي الفرصة لأجهزة الضبطية القضائية فرصة

¹ - وحسب الإحصائيات التي أجريت في بعض الدول منها فرنسا التي أظهرت دراسة أجرتها شركة التأمين الفرنسية بأن ما يتراوح ما بين 90-95 % من الجرائم الإلكترونية الواقعة في فرنسا لا يتم الإخبار عنها، بينما أظهرت دراسات أمريكية أن نسبة الجرائم المعلوماتية التي يتم الإخبار عنها تتراوح ما بين 2-6 % من مجموع الجرائم المرتكبة في الولايات المتحدة. أنظر رشاد خالد عمر، المرجع السابق، ص 87.

² - محمد طارق عبد الرؤف الخن، المرجع السابق، ص 244.

³ - أحمد فتحي سرور، الوسيط في شرح قانون الإجراءات الجزائية، ص 479.

التحرك بسرعة من أجل مواجهة الجريمة الإلكترونية ويعتبر عدم الإبلاغ عنها سببا رئيسيا في تفاقم الجرائم الإلكترونية.¹ إن التبليغ في الجرائم الإلكترونية لا يختلف عما عليه الحال في الجرائم التقليدية، إلا أنه يتمتع بنوع من الخصوصية تتماشى مع طبيعة هذه الجرائم والبلاغ يتم عن طريق الأنترنت، إن تلقي الشكاوى والبلاغات يكون عن طريق توفير نماذج للبلاغات عبر الأنترنت في عدة مواقع الكترونية مثل موقع المباحث الفيدرالية الأمريكية والبوليس الإنجليزي والشرطة الفرنسية فيما يتعلق بجرائم الأنترنت، كما قامت هذه الدول باستحداث أجهزة متخصصة لتلقي الشكاوى والبلاغات بواسطة الأنترنت واتخاذ الإجراءات اللازمة للكشف عن الجريمة وملاحقة مرتكبيها.²

ومن ناحية أخرى فإن ما يمكن ملاحظته في البلاغ الإلكتروني عن الجرائم الإلكترونية يمكن تقديم الشكاوى أو البلاغ من شخص يستعمل إسما مستعارا أو صفة غير حقيقية أو واقعة وهمية، وهو يتعارض مع كون الشكاوى لا تقبل إلا من طرف الشخص المضرور، إن قبول شكاوى الشخص الذي يحمل إسما مستعارا، مما يفتح المجال للجميع في التعامل بأسماء مستعارة، ومثل الأمر يجعل استعمال الشخصية، الوهمية مشروعة دائما،³ ولا تكون الشخصية مستعارة إلا إذا نص القانون على ذلك مثل ما نص المشرع الجزائري بخصوص إجراء التسرب.

ورغبة من المشرع الجزائري في مكافحة الجريمة الإلكترونية ومواكبة التشريعات المقارنة، إستحدث نظام الشكاوى عن طريق الأنترنت، التي تتيحها المواقع الخاصة بتقديم الشكاوى والبلاغات سواء على مستوى جهاز الشرطة أو الدرك الوطني، حيث يمكن للمواطنين الإتصال لتقديم البلاغات على الرقم 15-18 الخاص بالأمن الوطني و10-55 الخاص بالدرك الوطني، أو عن طريق البريد الإلكتروني أو المواقع الإلكترونية المخصصة لهذا الغرض كالبريد الإلكتروني للدرك الوطني cgnd@mdn.dz أو الموقع الإلكتروني www.ppgn.mdn أو موقع المديرية العامة للأمن الوطني www.dgsn.dz وفي إطار مواصلة تطوير وتحسين نوعية الخدمات المقدمة للمواطنين وأفراد الجالية الجزائرية بالخارج، وضعت وزارة العدل حيز الخدمة، أرضية إلكترونية جديدة تسمح للأشخاص الطبيعية أو المعنوية (الادارات والمؤسسات، الشركات الخاصة والجمعيات) بتقديم الشكاوى أو العرائض عن بعد للاستفادة

¹ - حسين ربيعي، المرجع السابق، ص 215.

² - يزيد بو حليط، المرجع السابق، ص 222.

³ - يزيد بوحليط، المرجع نفسه، ص 223.

من هذه الخدمة، يتعين على مقدم الشكوى الولوج إلى أرضية "النيابة الإلكترونية" « e-nyaba » المتاحة عبر البوابة الإلكترونية لوزارة العدل، ويتم تحويل هذه الشكوى أو العريضة بصفة آلية إلى ممثل وكيل الجمهورية بالمحكمة والنائب العام بالمجلس القضائي لاتخاذ الاجراء المناسب .

بعد تصرف ممثل النيابة في الشكوى، يتم إعلام المعني بمآلها والاجراءات المتخذة أو المطلوب اتخاذها، وذلك عبر أرضية "النيابة الإلكترونية" وكذا عبر رسالة نصية قصيرة (SMS) أو بريده الإلكتروني¹.

وتظهر أهمية تلقي البلاغ والشكاوى عبر الأنترنت في أنها تساعد رجال البحث والتحري على تحديد نوع الجريمة المبلغ عنها إن كانت تندرج ضمن الجرائم الإلكترونية، وكذلك وضع تصور مبدئي لخطّة العمل المناسب للبحث والتحري بشأن الجريمة².

المطلب الثاني: المعاينة والخبرة التقنية لإستخلاص الدليل الإلكتروني

إهتمت القوانين المقارنة بمسرح الجريمة لماله، من أهمية في إثبات الجريمة ونسبتها إلى مرتكبيها، ولما يحتوي عليه من آثار مادية تساعد المحقق على كشف الحقيقة، وللمعاينة مكانة بارزة منذ العصور القديمة في الإثبات على الصعيدين الجنائي والمدني، لمالها من دور خلال مرحلة الدعوى بوصفها وعاء للأدلة لضبط الجرائم ومرتكبيها³، إلا أنها في الجريمة الإلكترونية تكتسي طابعا خاصا، ومن أجل أن تؤدي المعاينة دورها في الإثبات، فإنه يستحسن أن يستعان بخبير فني متخصص في المعلوماتية وذلك حتى تمنع أي تشكيك في صحة الدليل المستمد منه⁴. سوف نتطرق إلى إجراء المعاينة في الجرائم الإلكترونية (الفرع الأول) والخبرة التقنية من خلال (الفرع الثاني).

¹ - مقال بعنوان إطلاق أرضية النيابة الإلكترونية « e- nyaba » منشور على الموقع [www. Mjustice . dz/ ar/](http://www.Mjustice.dz/ar/) ...، أطلع عليه يوم 2021/08/20 على الساعة 11h.30.

² - حسين ربيعي، المرجع السابق، ص 218.

³ - فاروق عبد الرحمان مراد، معاينة مسرح الجريمة الجزء الأول، دار النشر بالمركز العربي للدراسات الأمنية والتدريب، الرياض، د ط، 1991، ص 13.

⁴ - دلال مولاي ملياني، إشكالية الإثبات في جرائم الأنترنت في التشريع الجزائري، أطروحة لنيل شهادة الدكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، 2017-2018، ص 153.

الفرع الأول: المعاينة في الجريمة الإلكترونية

المعاينة هي من الانتقال، ولا يقصد بها مجرد رؤية المكان أو الشيء، بل تتضمن عملا ايجابيا يتمثل في البحث عن الدلائل وسائر العناصر المفيدة في كشف الحقيقة، وفي كثير من الأحيان تقتضي استخدام أحد وسائل الشرطة الفنية والعملية مثل تصوير مكان الجريمة، أخذ العينات، التقاط البصمات ... إلخ، والمعاينة عادة ما تقترب بضبط الأشياء التي يتم العثور عليها في مسرح الجريمة، ومن ثم تحريزها والإحتفاظ بها وعدم العبث بها، وذلك من أجل نسب الفعل إلى الفاعل أو نفي الفعل المكون للجريمة.¹ إلا أن المعاينة في الجريمة الإلكترونية لا تخلو من الصعوبات لوقوعها في العالم الافتراضي.

سوف نتطرق إلى مفهوم المعاينة (الفقرة الأولى) والضوابط المتبعة في المعاينة في (الفقرة الثانية)

الفقرة الأولى: مفهوم المعاينة

المعاينة في جوهرها ملاحظة وفحص حسي مباشر بمكان أو شخص له علاقة بالجريمة، وذلك لإثبات حالته، والكشف والتحفظ على ما قد يفيد من الأشياء في كشف الحقيقة قبل أن تنالها يد العبث، وهي صورة من صور الحصول على الإيضاحات، والمعاينة من الوجهة القانونية ليست وسيلة إثبات بل هي إجراء إستقصائي كاشف لأبعاد الجريمة وأركانها.²

أولا: تعريف المعاينة

تعرف المعاينة بأنها "الإجراء الذي يتضمن وصف مكان الحادث، بما فيه من أشياء وأشخاص والفحص الدقيق لكافة المحتويات، بهدف كشف مخلفات وآثار الجاني بالمكان التي تشير إلى شخصيته، أو شركاته وما يفيد في إثبات الجريمة، وتوضيح قدر من الإستنتاجات المنطقية تشكل في حد ذاتها الأساس الذي تقام عليه عملية التحقيق والبحث التالية".³، ويقصد بالمعاينة كذلك "إثبات حالة الأماكن والأشياء والأشخاص وكل ما يعتبر في كشف الحقيقة".⁴، وتعرف أيضا بأنها "رؤية بالعين لمكان أو شخص أو

¹ - أمينة علالي، الجرائم العابرة للحدود المرتكبة بتقنية الانترنت، أطروحة لنيل شهادة دكتوراه علوم في القانون، كلية الحقوق والعلوم السياسية، جامعة باجي مختار، عنابة، 2018، ص 173.

² - خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية، ط1، 2009، ص، ص، 145-146.

³ - تركي بن عبد الرحمان المويشير، المرجع السابق، ص 124.

⁴ - عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية -دراسة مقارنة في ضوء الضوابط العامة للإجراءات الجنائية -، دار النهضة العربية، القاهرة، ط1، 2009، ص 58.

شيء لإثبات حالته وضبط كل ما يلزم لكشف الحقيقة.¹ أي هي ملاحظة وفحص حسي مباشر لمكان أو شخص أو شيء له علاقة بالجريمة، لإثبات حالته والكشف على كل ما قد يفيد من الأشياء في كشف الحقيقة.²

ويمكن القيام بالمعاينة أثناء مرحلة الاستدلال في الجناية المتلبس بها، حيث نصت المادة 42 من ق.ا.ج.ج على أنه " يجب على ضابط الشرطة القضائية الذي بلغ بجناية في حالة تلبس، أن يخطر وكيل الجمهورية على الفور، ثم ينتقل بدون تمهل إلى مكان الجريمة، ويتخذ جميع التحريات اللازمة، وعليه أن يسهر على المحافظة على الآثار التي يخشى أن تختفي، وأن يضبط كل ما يمكن أن يؤدي إلى إظهار الحقيقة، وأن يعرض الأشياء المضبوطة على الأشخاص المشتبه في مساهمتهم في الجناية للتعرف عليها.³

كما تعد المعاينة من إجراءات التحقيق وهو ما نصت عليه المادة 79 من ق.ا.ج.ج على أنه "يجوز لقاضي التحقيق الانتقال إلى أماكن وقوع الجرائم، لإجراء جميع المعاينات اللازمة أو للقيام بتفتيشها، ويخطر بذلك وكيل الجمهورية الذي له الحق في مرافقته، ويستعين قاضي التحقيق، دائما بكاتب التحقيق ويحرر محضر بما يقوم به من إجراءات.⁴

إذا فالهدف من المعاينة هو ضبط ما استعمل في ارتكاب الجريمة، أو نتج عنها،⁵ أو هي تقصي الآثار المادية التي يخلفها الجناة في مسرح الجريمة.

ثانيا: أهمية المعاينة في الجريمة الإلكترونية

للمعاينة أهمية كبيرة في تسهيل جمع الأدلة المترتبة على إرتكاب الجريمة، قبل زوال معالمها كما تنتقل المعاينة صورة واضحة لمكان إرتكاب الجريمة، وأطراف الواقعة لتساعد القاضي على تصور كيفية

¹ - محمد زكي أبو عامر، الإجراءات الجنائية، منشأة المعارف، الإسكندرية، ط2، د س ن، ص 222.

² - جميل عبد الباقي الصغير، الجوانب الإجرائية المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، د ط، 2002، ص 26.

³ - المادة 42 من قانون إجراءات جزائية.

⁴ - المادة 79 من قانون إجراءات جزائية.

⁵ - آمنة محمدي بوزينة، إجراءات التحري الخاصة في مجال مكافحة الجريمة المعلوماتية، دراسة تحليلية لأحكام قانون الإجراءات الجزائية وقانون الوقاية من جرائم الإعلام، ورقة علمية مقدمة في إطار أعمال الملتقى الوطني آليات مكافحة الجريمة الإلكترونية في التشريع الجزائري، 29 مارس 2017، مركز جيل البحث العلمي، ص 60.

إرتكاب الحادث، وتبين الحقيقة وتكشف عن دليل الإدانة.¹

وحتى تأتي المعاينة بثمارها وتفي بأغراضها، أحطتها بعض التشريعات بجزاءات جنائية على كل من يحدث تعديلا، أو تغييرا في مكان وقوع الجريمة، قبل قيام سلطات التحقيق بإجراء المعاينة²، وهذا ما نصت عليه المادة 43 من ق.ا.ج.ج على أنه "يحظر في مكان إرتكاب جنائية على كل شخص لا صفة له، أن يقوم بإجراء أي تغيير على حالة الأماكن التي وقعت فيها الجريمة أو ينزع أي شيء منها قبل الإجراءات الأولية التحقيق القضائي، وإلا عوقب بغرامة من 200 إلى 1.000 دج.

غير أنه يستثنى من هذا الحظر، حالة إذا كانت التغييرات أو نزع الأشياء للسلامة والصحة العمومية أو تستلزمها معالجة المجني عليهم.³

وبالرغم أن المعاينة من أهم إجراءات التحقيق، إلا أن البعض يرى أن دورها يتضاءل في الكشف عن الجرائم الإلكترونية، وسبب ذلك مرده إلى أن الجريمة التقليدية تجري غالبا على مسرح جريمة تخلف أثارا مادية، على عكس الجريمة الإلكترونية ومرد ذلك لعدة أسباب منها:

- أن الجريمة الإلكترونية قلما تخلف أثارا مادية.

- الأعداد الكبيرة من الأشخاص الذين قد يترددون على مسرح الجريمة، خلال المدة الزمنية من وقت وقوع الجريمة، وحتى إكتشافها أو التحقيق فيها وهي فترة طويلة نسبيا، هذا يعطي للجاني أو لآخرين بتعديل، أو تغيير، أو إتلاف الآثار المادية للجريمة، مما يؤدي إلى الشك في الأدلة المستوفاة من المعاينة في الجريمة الإلكترونية.

- إمكانية التلاعب في البيانات عن بعد، أو محوها عن طريق التدخل، من خلال وحدة طرفية من

قبل المجرم المعلوماتي.⁴

¹ - للمزيد عن أهمية المعاينة أنظر فاروق عبد الرحمان مراد، المرجع السابق، ص 26 ما يليها.

² - عنيقي كامل عفيقي، المرجع السابق، ص 334.

³ - وهذا ما نص عليه المشرع الفرنسي في المادة 55 ق.ا.ج.ج والتي جاء نصها كما يلي :

Art 55. C. p.p.f dispose que : «dans les lieux ou à un crime a été commis il est interdit sous peine de l'amende prévue pour les contravention de le 4 classe à toute personne non habilitée, de modifier avant les premier opérations de l'enquête judiciaire l'Etat de lieux et d' y effectuer de prélèvement quelconque. »

⁴ - عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، المحلة الكبرى، ط1، 2001، ص 61.

الفقرة الثانية: الضوابط المتبعة في إجراء المعاينة

عند إجراء المعاينة في مسرح الجريمة الإلكترونية، لا بد من وجود ضوابط وشروط معينة لذلك التي تتمثل في:

أولا: كيفية إجراء المعاينة في العالم الافتراضي

تتم المعاينة في الجرائم الإلكترونية، كأى جريمة أخرى عن طريق الانتقال إلى مسرح الجريمة بإعتباره حجر الزاوية في التحقيق الجنائي، والشاهد الصامت على ما أرتكب من وقائع جنائية، ويحوي الأدلة التي تثبت وقوع الجريمة ونسبتها إلى مرتكبيها¹، إلا أن المعاينة في الجريمة الإلكترونية يمكن الجمع فيها بين مسرح الجريمة التقليدي والمسرح الافتراضي، وله أهمية كبيرة للتوصل إلى أدلة الإدانة، ففي كثير من الأحيان يترك المجرم المعلوماتي آثارا مادية في المسرح التقليدي أو المادي، تكون مكملة لما سوف يتوصل إليه من معاينة المسرح الافتراضي،² لذا يتكون مسرح الجريمة الإلكترونية من مسرحين هما:

1- مسرح تقليدي³

ويقصد به مسرح الجريمة الذي يقع خارج المنظومة المعلوماتية، وهي تتكون بشكل رئيسي من المكونات المادية للحاسب الآلي، ويقترب إلى مسرح الجريمة التقليدية، فالجرائم الواقعة على المكونات المادية للحاسب الآلي كالإعتداء على أشرطة الحاسب وكابلاته، وشاشة العرض، ومفاتيح التشغيل والأقراص الممغنطة، فالمعاينة التي تتم على هذا المسرح لا تثير أي صعوبة من قبل الشرطة القضائية أو قاضي التحقيق والتحفظ على الأشياء التي تعد أدلة مادية يستدل بها على إرتكاب الجريمة⁴، ونسبتها إلى شخص معين، فالمعاينة هناك لا تختلف عن المعاينة في مسرح الجريمة التقليدية.

¹ - سامي حارب المنذري، معاينة مسرح الجريمة والحصول على الأدلة المادية، موسوعة العلوم الجنائية تقنية الحصول على الأدلة المادية، الجزء الأول. شرطة الشارقة، مركز بحوث الشرطة، الشارقة، ط 1، 2007، ص 51.

² - دلال مولاي ملياني، المرجع السابق، ص 158.

³ - لم تقم التشريعات الجنائية بتعريف مسرح الجريمة وتمحورت معظم تعاريف الفقهاء لمسرح الجريمة أنه " المكان أو الأماكن التي شهدت مراحل ارتكاب الجريمة واحتوت على الآثار المختلفة عن إرتكابها، ويعتبر ملحقا لمسرح الجريمة، أماكن الدخول للمسرح والخروج منه وكل مكان شهد مرحلة الجريمة سواء كانت تمثل التخطيط والإعداد أو الإختفاء وإخفاء الأداة للإفلات من وجه العدالة، أنظر سامي حارب المنذري، المرجع السابق، ص 87.

⁴ - عفيفي كامل عفيفي، المرجع السابق، ص 336.

2 - مسرح إفتراضي

ويقصد به مسرح الجريمة الذي يقع داخل البيئة الإلكترونية، وتتكون من البيانات والمعلومات المتواجدة داخل الحاسب الآلي، والتي يكون الجاني قد وصلها عند ارتكاب الجريمة سواء باستخدام الجهاز بالوصول المباشر أو الوصول غير المباشر، عن طريق الشبكة بهدف الحصول على دليل إلكتروني،¹ ولإختلاف هذه البيئة عن المسرح المادي، قد يجد ضباط الشرطة القضائية صعوبة في إجراء عملية المعاينة، إلا أنه يمكن للجاني أن يترك آثارا للجريمة في العالم الافتراضي من خلال المواقع الإلكترونية التي تم الولوج إليها.

هذه المواقع التي تفتح سجلات تتضمن بعض المعلومات عن المجرم، كعنوان بريده الإلكتروني ومكان الإتصال ومن هذه المواقع موقع [www.Consumer. Net/ analys](http://www.Consumer.Net/analys) الذي يقدم كل المعلومات والبيانات الخاصة بالشخص الزائر، وكذلك في حالة إستعمال الجاني لأسماء مستعارة، أو إستخدام برامج إخفاء الهوية مثل ghost mail، فالجهة الوسيطة IPS التي تقدم الخدمة تحتفظ بسجل عن كافة تحركاته وقيامه بأعمال غير مشروعة، كرسائل التهديد، أو القنابل البريدية أو التصرفات، المخالفة للقوانين والتشريعات المعمول بها، وتفيد تلك المعلومات ضباط الشرطة القضائية في البحث والتحري عن أدلة الإدانة،² ومن أهم وسائط التخزين للمعلومات الذي يجب التركيز عليه أثناء المعاينة، القرص الصلب لإحتوائه على جميع ملفات الأدلة الرقمية، إحتوائه على المحفوظات التي تحكي تاريخ الإستخدام، نظام التشغيل، كما يحتوي على كل الأسرار المعلوماتية، وللمحافظة على هذا الفرص، لا بد من نسخه وحفظه³ للرجوع إليه وقت الحاجة إليه.

ثانيا: الخطوات المتبعة لإجراء المعاينة

ما تجدر الإشارة إليه إنه يجب تتبع خطوات معينة قبل التحرك والانتقال إلى مسرح الجريمة، وأخرى

¹ - سليمان مهج الغنزي، وسائل التحقيق في جرائم نظم المعلومات، رسالة لنيل شهادة الماجستير في العلوم الشرطية، كلية الدراسات العليا، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2003، ص 124.

² - سليمان منهج الغنزي، المرجع نفسه، ص 124

³ - سليمان غازي العتيبي، درجة توافر كفايات البحث والدليل الرقمي في الجرائم المعلوماتية لدى ضباط شرطة العاصمة المقدسة، رسالة لنيل شهادة ماجستير في العلوم الشرطية، كلية الدراسات العليا، قسم العلوم الشرطية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2010، ص 55

عند الوصول إلى مسرح الجريمة.

1 - الخطوات المتبعة قبل الانتقال إلى مسرح الجريمة

قبل الانتقال إلى مسرح الجريمة يجب مراعاة الخطوات التالية:

- توفير معلومات مسبقة عن مكان الجريمة، وعن نوع وعدد الأجهزة وشبكات الإتصال الخاصة بها، قصد تحديد إمكانية التعامل معها فنيا من حيث الضبط والتأمين وحفظ المعلومات.
- إعداد الفريق المتخصص الذي يتولى المعاينة، من الخبراء ورجال الضبط والأمن، مع تحديد البيانات والمهام والإختصاصات المطلوبة من كل عضو وذلك حتى لا تتداخل الاختصاصات.¹
- الحصول على الإحتياجات الضرورية من أجهزة وبرامج، للإستعانة في الفحص والتشغيل مثل برامج معالجة الملفات (xtree pro gold)، برامج النسخ (lap Link)، وبرنامج (encase) المنتج صور مطابقة للقرص الصلب الذي يستخدم في التحقيقات من طرف المباحث الفيدرالية الأمريكية المسماة "حقيبة الأدلة الرقمية".²
- تأمين التيار الكهربائي، بشكل لا يتم التلاعب أو التخريب عن طريق قطع التيار أو تعديل الطاقة الكهربائية.
- التأكد من خلو المحيط الخارجي لمسرح الجريمة الإلكترونية، من أية مجالات لقوى مغناطيسية، أو ممرات إتصالات، التي يمكن أن تتسبب في محو البيانات المسجلة، أو إتلاف الآثار الأخرى للجريمة.³

2 - الخطوات المتبعة أثناء المعاينة

عند معاينة مسرح الجريمة يرى الفقه الجنائي ضرورة وضع عدة ضوابط أو اتباع خطوات في معاينة مسرح الجريمة الإلكترونية وتتمثل في:

¹ - نبيلة هبة هروال، الجوانب الإجرائية لجرائم الأنترنت في مرحلة جمع الإستدلالات، المرجع السابق، ص 219.

² - عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي -دراسة مقارنة-، دار الجامعة الجديدة، الإسكندرية، د ط، 2009، ص 51.

³ - جمال إبراهيمي، المرجع السابق، ص 59.

- تحديد أجهزة الحاسب الآلي الموجودة في مكان المعاينة، مع تحديد مواقعها، وفي حالة وجود شبكة إتصالات يجب البحث عن الخادم للملف file server من أجل تعطيل الإتصالات، ولمنع تخريب الأدلة أو محوها، مع مراعاة تصوير الأجهزة الموجودة، خاصة تصوير الأجزاء الخلفية للحاسب الآلي، وتسجيل وقت وتاريخ ومكان التقاط كل صورة.¹
- ملاحظة الطريقة المعد بها النظام المعلوماتي، مع ملاحظة الآثار التي يمكن أن يخلفها، ومعرفة السجلات الإلكترونية التي تزود بها شبكات المعلومات، وذلك من أجل معرفة موقع الإتصال ونوع الجهاز المتصل عن طريق الدخول إلى النظام أو الموقع أو الدخول معه في حوار.²
- عدم التسرع في نقل أي مادة معلوماتية من مكان وقوع الجريمة، وذلك قبل إجراء إختبارات للتأكد من خلو المحيط الخارجي لمواقع الحاسب الآلي، من أية مجالات لقوى مغناطيسية يمكن أن تسبب في محو البيانات المسجلة.
- التحفظ على محتويات سلة المهملات، والقيام بفحص الأوراق والشرائط والأقراص الممغنطة المحطمة المتواجدة فيها، مع رفع البصمات التي قد تكون لها صلة بالجريمة المرتكبة.
- الإستعانة بأهل الخبرة عند الضرورة.³
- القيام بحفظ المستندات الخاصة بالإدخال وكذا مخرجات الحاسب الآلي الورقية، التي قد تكون ذات صلة بالجريمة وذلك من أجل رفع ومضاهاة البصمات التي قد تكون موجودة فيها.⁴
- ضبط وتحريز الدعائم الأصلية للبيانات وعدم الإكتفاء بضبط النسخ، كما يجب مراعاة ظروف تخزينها، كعدم وضعها على مقربة من محطة إرسال الأسلكي أو وضعها في أماكن تحتوي على الغبار بما يؤدي إلى إتلافها.⁵

¹ - خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 172.

² - عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، المرجع السابق، ص 63.

³ - نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت، المرجع السابق، ص 220.

⁴ - عفيفي كامل عفيفي، المرجع السابق، ص 337.

⁵ - خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 177.

ونخلص في الأخير، أن إجراء المعاينة لمسرح الجريمة الإلكترونية أنها غير فعالة للبحث عن الدليل الرقمي، لما تعثرها من صعوبات كبيرة، منها قدرة الجاني على محو وتدمير آثار الجريمة. ولهذا ولنجاحة إجراء المعاينة يجب على القائمين بالبحث والتحري ومعاينة مسرح الجريمة، أن يكونوا على درجة عالية من التأهيل والتدريب الفني لمواجهة هذه النوعية من الجرائم.

الفرع الثاني: الخبرة التقنية في الجريمة الإلكترونية

الخبرة هي الوسيلة لتحديد التفسير الفني للأدلة أو الدلائل بالاستعانة بالمعلومات العلمية، فهي في حقيقتها، ليست دليلا مستقلا عن الدليل القولي أو الدليل المادي، وإنما هي تقييم فني لهذا الدليل، والعنصر المميز للخبرة عن غيرها من إجراءات الإثبات كالمعاينة والشهادة، وهو الرأي الفني للخبير في كشف الدلائل أو تحديد ملامح شخصيته الإجرامية.¹

الفقرة الأولى: مفهوم الخبرة التقنية

تخضع الخبرة التقنية في أغلب التشريعات إلى نفس أحكام الخبرة القضائية، من حيث القواعد القانونية التي تحكم عمل الخبير وإجراءاته، ورغم هذا هناك بعض التشريعات ومنها التشريع البلجيكي الذي نظم الخبرة التقنية في مجال الجريمة الإلكترونية من خلال القانون الصادر بتاريخ 2000/11/23 بموجب المادة 88 منه²، وقد تناول المشرع الجزائري أحكام الخبرة في القسم التاسع من الباب الثالث في المواد من 143 إلى 155 من ق.إ.ج.ج.

أولا: تعريف الخبرة التقنية

يقصد بالخبرة بصفة عامة "إجراء تحقيقي يتم بموجبه الاستتارة برأي شخص مختص في مسألة فنية ذات أثر في حسم النزاع، أو كشف الحقيقة".³ وقد عرفت بأنها عبارة عن إستشارة فنية يستعين بها قاضي

¹ - سعيد سالم المزروعى، عبد الرحمان عزمان، إجراءات التحقيق في جرائم تقنية المعلومات وفقا للتشريع الإماراتي، مجلة العلوم الإقتصادية والإدارية والقانونية، المجلد 2، العدد 13، 2018، ص 122.

² - نصت المادة 88 على "يجوز لقاضي التحقيق وللشرطة القضائية أن تستعين بخبير ليقدم وبطريقة مفهومة المعلومات اللازمة عن كيفية تشغيل النظام وكيفية الدخول فيه أو الدخول للبيانات المخزونة أو المعالجة أو المنقولة بواسطته... " أنظر Meunier, la loi du 28 novembre 2000 relative à la criminalité informatique, revue de droit pénal criminel, 2002, p.p 680-683.

³ - غازي الذنيبات، الخبرة الفنية في إثبات التزوير، دار الثقافة، عمان، د ط 2010، ص 57.

التحقيق لنقد المسائل الفنية، التي تحتاج تقديرها إلى معرفة فنية أو دراية علمية، لا تتوافر لدى قاضي التحقيق بحكم تكوينه.¹ وعرفت أيضا على أنها "عملية بحث وتحرر يؤمر بها بطلب من الخصوم أو تلقائيا، كلما رأى القضاة أنهم بحاجة إلى مشاركة أهل الاختصاص لملاحظة أمور، أو تقدير واقع أو أسباب، أو مبررات غير واضحة".² فيما تعرف الخبرة التقنية بأنها "إبداء الرأي الفني من أحد المتخصصين في شأن واقعة ذات أهمية في دعوى متعلقة بإحدى الجرائم الإلكترونية،³ وبالتالي فإن الخبرة التقنية لا تختلف كثيرا عن الخبرة في مختلف المجالات الأخرى، إلا أنها متعلقة بالجرائم الإلكترونية.

و الواقع أن هذا النوع من الخبرة بدأ يتخذ حيزا في مجال إثبات جرائم العالم الافتراضي، حتى أصبح يعرف في الفقه المقارن بالمعلوماتية الشرعية، و تعرف هذه الأخيرة بأنها "إستخدام الطرق العلمية لجمع وتعريف وتحليل وتفسير الدليل الرقمي، المأخوذ من مصادر رقمية والإحتفاظ به وتوثيقه، على نحو يسهل بناء الأحداث التي تؤدي إلى إكتشاف الجريمة." أو جمع وحفظ وتحليل الدليل المتعلق بالحاسب الآلي.⁴

ثانيا: أنواع الخبرة

الخبرة في المجال التقني قد تكون خاصة، أو عن طريق الجهات والمؤسسات التعليمية، وقد تكون عن طريق جهات الضبط القضائي ويمكن بيانها كالاتي:

1 - الخبرة الخاصة

يقوم هذا النوع من الخبرة على شكيلين هما الخبرة الفردية الخاصة، والتي تشغل حيزا كبيرا وأثبتت مهارة عالية في الجانب التكنولوجي، سواء عن طريق التكوين أو الموهبة، وإن كانت هذه الأخيرة أكثر تحققا بالنظر للجرائم الإلكترونية، التي تحدث في الغالب ومن فئات لا علاقة لها بتكوين، أو الدراسة في هذا المجال، أما الشكل الثاني هو ما تقوم به الشركات الكبرى الناشطة في المجال التكنولوجي، من توظيف أو التعاقد مع أشخاص أثبتوا كفاءتهم في مجال الحاسوب والانترنت، فنجد بعض الشركات تعين العصاة للقانون الذين أثبتوا مهاراتهم في المجال التكنولوجي، وذلك من منطلق إقتصادي بحث.⁵

¹ - أحسن بوسقيعة، التحقيق القضائي في ضوء قانون 2006/12/2، دار هومة الجزائر، ط8، 2009، ص 107

² - محمود توفيق إسكندر، الخبرة القضائية، دار هومة، الجزائر، ط1، 2002، ص 55 .

³ - محمود محمد محمود جابر، الجرائم الناشئة عن إستخدام الهواتف النقالة لجرائم نظم الإتصالات والمعلومات، المكتب الجامعي الحديث، الإسكندرية، د ط، 2017، ص 257.

⁴ - محمد طارق عبد الرؤوف الخن، المرجع السابق، ص 331.

⁵ - محمد التوجي، الحماية الجنائية المرتكبة بواسطة الهاتف النقال، أطروحة لنيل شهادة دكتوراه (ل. م . د) في

2- الخبرة التعليمية

تعد الأنترنت أحد منتجات العلم في حركته التقنية، فإنه يعتبر من أقوى مظاهر الخبرة التي يمكن الإستعانة، بها لمواجهة الجريمة الإلكترونية، ويمكن أن تكون من خلال المؤسسات التعليمية، فهذه الأخيرة تعمل على تكوين خبراء في هذا المجال مدعمين بالنهج العلمي غير التجاري، وذلك من أجل رصد مثل هذا النوع من الجرائم.¹

3 -جهات الضبط القضائي

نظرا للطبيعة الخاصة للجريمة الإلكترونية، شرعت بعض الدول في إنشاء أجهزة متخصصة للخبرة في مجال الإجرام المعلوماتي، وعلى رأس هذه الدول الولايات الأمريكية، التي أسست المباحث الفيدرالية الأمريكية FBI أطلق عليه "المعمل الإقليمي الشرعي للحاسوب"، مهمته مكافحة الجريمة الإلكترونية وذلك بتحليل وتصنيف الدليل الرقمي، ويوجد بالمعمل المذكور ثلاثة فروع الأول هو Imaging والثاني analysis والثالث research and development، بحيث يكون تدريب الخبراء فيه بشكل دائرة متكاملة ويتم تدريبهم على الفروع الثلاثة.²

وهذا ما إتجه إليه المشرع الجزائري، وقيامه بإنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، حيث أسند لها مهمة إنجاز الخبرة التقنية في مجال الجريمة الإلكترونية وهذا ما نصت عليه المادة 14 / ب من القانون 09-04 "تتولى الهيئة المذكورة في المادة 13 أعلاه، خصوصا المهام التالية:"..... ب - مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيا الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية"، وكذلك نصت المادة 2/15 من المرسوم الرئاسي 20-183³ الذي يتضمن تنظيم الهيئة الوطنية "تكلف مديرية المراقبة الوقائية واليقظة الإلكترونية بما يلي..... بمساعدة

الحقوق، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية، أدرار، 2018، 2019، ص 186.

¹ - فتحي محمد أنور عزت، الحماية الجنائية الموضوعية والإجرائية الإعتداء على الصفقات والحق في الخصوصية والكمبيوتر والأنترنت في نطاق التشريعات الوطنية والتعاون الدولي، دار النهضة العربية، القاهرة، ط1، 2007، ص 308.

² - فتحي محمد أنور عزت، المرجع نفسه، ص 310.

³ -المرسوم الرئاسي رقم 20-183 المؤرخ في 2020/07/13، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، عدد40 الصادرة بتاريخ 2020/07/18.

السلطات القضائية بناء على طلبها، بما في ذلك في مجال الخبرات القضائية في إطار مكافحة الجريمة المتصلة بتكنولوجيا الإعلام والاتصال التي تتطلب اللجوء إلى أساليب التحري الخاصة للهيئة.

كما يلعب المعهد الوطني للأدلة الجنائية وعلم الإجرام، دورا كبيرا في مجال إنجاز الخبرات العملية أو الخبرات اللازمة في توجيه التحقيقات القضائية، بطلب من القضاة من أجل كشف الحقيقة بالأدلة العلمية لتحديد هوية مرتكب الجرائم.

ثانيا: الخبير التقني

الخبير بصفة عامة هو "شخص ذو دراية عالية، له إلمام بموضوع فني أو علمي أو عملي، يستعين به القضاء في أمور تدخل في إختصاصه، ولا يجوز للخبير أن يتجاوز المهمة المعهد له بها، ويشترط فيه أن يكون إنسانا إجتماعيا".¹ وعرف أيضا بأنه "كل شخص له دراية خاصة بمسألة من المسائل وله كفاءة فنية وعلمية خاصة".² أما في مجال الجرائم الإلكترونية يطلق عليه الخبير المعلوماتي، أو الخبير الرقمي، أو الخبير التقني و الذي يعرف بأنه "الشخص الذي تعمق في دراسة الأعمال الإلكترونية في أدائه لفترة زمنية طويلة، ما جعله يكسب الخبرة المعلوماتية متميزا بذلك عن الشخص العادي، وبالتالي قدرته على إبعاد الرأي الإلكتروني الرقمي في الأمور المتمثلة بهذا العمل".³ كما عرف أيضا بأنه "الخبير المتخصص والمدرّب على معالجة جميع أنواع الأدلة الرقمية وفحصها وتحليلها".

نظرا للدور الذي تلعبه الخبرة في الدعوى الجنائية، فقد أسند المشرع مهمة القيام بها لفئة من الأشخاص، الذين تتوفر فيهم الشروط القانونية والمؤهلات العلمية للتسجيل في جدول الخبراء، ومن أهم هذه الشروط أن يكون حاصلا على شهادة عملية في إختصاص معين، وأن يكون حسن السلوك والسمعة وجديرا بالثقة⁴، إلى جانب ذلك يتعين أن يكون خبيرا الحاسب الآلي المنتدبين أن تتوفر لديهم القدرة الفنية

¹ - عبد العزيز توفيق، شرح قانون المسطرة المدنية والتنظيم القضائي، دار النجاح الجديدة، الدار البيضاء، 1995، ص 183.

² - عبد الناصر محمد محمود فرغلي، محمد عبيد سيف المسماري، الاثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، دراسة تطبيقية مقارنة، ورقة علمية مقدمة للمؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الامنية، الرياض، المنعقد بين 12.14/11/2007، ص24.

³ - لينا محمد الأسدي، المرجع السابق، ص218.

⁴ - عبد الرزاق أحمد الشيبات، إجراءات الخبرة القضائية ودورها في الاثبات، مجلة كلية القانون للعلوم القانونية والسياسة، دعن د س ن، ص431.

والإمكانات العلمية في المسألة موضوع الخبرة، لا يكفي في ذلك حصول الخبير على شهادة علمية بل يجب مراعاة الخبرة العملية لأنها هي التي تحدد الكفاءة الفنية، ولذلك لا وجود لخبير لديه معرفة متعمقة في سائر أنواع الحاسبات وبرمجيتها وشبكاتها، أو لديه القدرة على التعامل مع كل أنواع الجرائم الإلكترونية¹، مما تستوجب طبيعة هذه الجرائم توافر شروط خاصة في الخبير المنتدب لبحث مسائل فنية وعلمية بالنسبة لها وهي:²

- الإلمام بتركيب الحاسب الآلي وصناعاته وطراره، ونظم تشغيله الرئيسية والفرعية والأجهزة الطرفية الملحقة به وكلمات المرور أو السر أو أكواد التشفير.-

- معرفة بيئة الحاسب الآلي أو الشبكة من حيث طبيعتها، تركيزها أو توزيعها، وكذا نمط ووسائل الإتصال.

- المكان المحتمل لأدلة الإثبات وشكلها وهيئتها.

- كيفية عزل النظام المعلوماتي والحفاظ على الأدلة دون تلف.

- الكيفية التي يتم بواسطتها نقل الأدلة إلى الأوعية دون إتلاف.

- كيفية تجسيد الأدلة في صورة مادية، وذلك بنقلها إن أمكن إلى أوعية ورقية تتيح للقاضي مطالعتها، وفهمها مع الإثبات أن المطبوع الورقي هو مطابق لما هو موجود على الدعامة الممغنطة.

وعليه فإن إختيار الخبير في مجال الجريمة الإلكترونية³، يتحدد بنوعية الجريمة المرتكبة، نظرا لأن

¹ - عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الإبتدائي في الجريمة المعلوماتية، المرجع السابق، ص99.

² - محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي، بحث مقدم لمؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، جامعة الإمارات، المنعقد بين 1-3/ 200/05، ص320.

³ - لقد حصر قانون الدليل الإلكتروني الخاص بولاية كاليفورنيا في الولايات المتحدة الأمريكية الخبراء الإلكترونيين الرقميين هم: المبرمج الذي قام بتحرير البرنامج إختياره، محلل النظم الذي صمم وحدد برنامج الحاسب الآلي الذي أنتج الدليل، المشغل الذي يقوم بتشغيل البرنامج، مهندس الصيانة الذي يقوم على صيانة الجهاز الأصلي والتأكد من عمله بصورة صحيحة، مبرمج صيانة النظام، طاقم عمليات البيانات الذي يعد البيانات بالصورة التي يستطيع الحاسب الرقمي قراءتها، أمناء مكتبة الشرطة الذين يتحملون مسؤولية توفير الشرطة والأسطوانات، التي تشتمل على البيانات المصدرة الصحيحة، المستخدم النهائي الذي يمد بالمعلومات المدخلة ويصرح بتنفيذ برامج الحاسب الرقمي ويستخدم نواتجها، أنظر سليمان مهج الغنزي، المرجع السابق، ص75.

الحاسبات الآلية وشبكات الأنترنت ذات نماذج متعددة.

الفقرة الثانية: الضوابط القانونية والفنية للخبرة التقنية

نظرا للدور البارز التي تؤديه الخبرة التقنية في مجال الإثبات الجنائي، حرصت معظم الدول على تنظيمها وإحاطتها بمجموعة من الضوابط حتى يكون لنتائجها حجية أمام القضاء وتتمثل هذه في الضوابط القانونية إضافة إلى أخرى فنية.

أولا: الضوابط القانونية

وتتمثل هذه الضوابط المتعلقة بالخبير، وأخرى خاصة بالخبرة.

1 . الضوابط الخاصة بالخبير

أ- اختيار الخبير من جدول الخبراء

الأصل أن يختار الخبراء حسب التخصص من الجداول التي تعدها المجالس القضائية بعد استطلاع رئيس النيابة العامة، كما تحدد الأوضاع التي يجري فيها قيد الخبراء أو شطبهم بقرار من وزير العدل، ولكن إستثناء في حالة عدم توفر الخبرة المطلوبة في جداول الخبراء يجوز لجهات التحقيق أن تختار خبراء بقرار مسبب ليسوا مقيدين في أي من هذه الجداول،¹ كما أن عملية إختيار الخبير أمرا متروكا لجهات التحقيق، فبمفهوم المادة 147 من قانون الإجراءات الجزائية الجزائري، للقاضي أن ينتدب خبيرا واحدا أو خبراء متعددين حسب الحاجة، ولا تهم طبيعة الخبير سواء كان شخصا طبيعيا أو شخصا معنويا كمؤسسة متخصصة في مجال الخبرة التقنية و إن الواقع العملي أن يستعين بالشخص الطبيعي.²

لكن في مجال الجريمة الإلكترونية يتعين الإستعانة، بشركات ومنظمات أو مؤسسات متخصصة، بما تملكه من موارد مادية وبرامج وأجهزة حديثة، وموارد بشرية من مهندسين متخصصين في الحاسب الآلي و الأنترنت، ومن أمثلة هذه الشركات مخبر الخبرة والبحث عن البصمات (الآثار) المعلوماتية في فرنسا.³ Lerti

¹ - المادة 144 من قانون الإجراءات الجزائية الجزائري.

² - رشيدة بوكري، المرجع السابق، ص426.

³ - laboratoire d'expertise et de recherche de traces informatiques, le laboratoire a été créé en 2004 par cinq experts judiciaires en informatique et un ancien gendarme appréter le sèment légale le 29 janvier près du tribunal de Grenoble et inscrit dans la liste des experts plus des renseignements voir sur le site [www. Lerti .Fr](http://www.Lerti.Fr)

ب- أداء اليمين القانونية

من أجل حمل الخبير على الصدق والأمانة في أداء عمله وبث الطمأنينة في آرائه، التي يقدمها سواء بالنسبة لتقدير القاضي أو لثقة أطراف الدعوى،¹ فقد حرصت أغلب التشريعات على ضرورة أداء الخبير لليمين قبل قيامه بعمله وإلا كان له عمله باطلا.

لقد أوجب المشرع الجزائري بموجب المادة 145 من ق.إ.ج.ج.²، أن يحلف الخبير اليمين القانونية قبل أدائه مهامه، غير أنه إذا كان الخبير المعين مقيدا في الجدول، فلا يلزم أن يجدد حلفه لليمين مرة أخرى، مادام قد أدى اليمين عند تعيينه بالجدول لأول مرة.

2 - الضوابط الخاصة بالخبرة

لا يكتفي التشريع بالضوابط التي تحكم الخبير، بل هناك ضوابط أخرى متعلقة بالخبرة نفسها، وتتمثل فيما يلي:

أ- خضوع الخبرة للرقابة القضائية

على أن يتولى الخبير مهامه تحت رقابة القاضي الذي أمر بإجراء الخبرة، ولا يستلزم حضوره فعلا أثناء أداء أعماله، بل يكفي أن يبقى على إتصال مستمر مع إحاطته علما بكل المستجدات التي تطرأ بعمله، على إعتبار الخبير ليس سوى مساعد فني للقاضي.³

ب -إنجاز الخبير لأعمال الخبرة بنفسه

لا بد على الخبير أن يقوم بأعمال الخبرة بنفسه، وفي حدود ما نص عليه أمر أو حكم النذب، وأن يستجيب للطلبات التي يقدمها أطراف الخصومة مثل سماع أي شخص قادر على إعطاء معلومات فنية.⁴

¹ - حسن بشيت خوين، ضمانات المتهم في الدعوى الجزائية خلال مرحلتي التحقيق الابتدائي والمحاكمة، دراسة مقارنة، دار الثقافة، عمان، 1998، ص 115.

² - تنص المادة 145 ق.إ.ج.ج. على "يحلف الخبير لأول مرة في الجدول الخاص بالمجلس القضائي يمينا أمام ذلك المجلس بالصيغة الآتية : أقسم بالله العظيم أن أؤدي مهمتي كخبير على خير وجه وبكل إخلاص وأبدي رأي بكل نزاهة وإستقلال " ولا يجدد هذا القسم ما دام الخبير مقيدا بالجدول ".

³ - Myriam quémener , Yves charpenel , op, cit, p 183

⁴ - تنص المادة 152 من ق.إ.ج.ج. على أنه "يجوز لأطراف الخصومة أثناء إجراء أعمال الخبرة أن يطلبوا إلى الجهة القضائية التي أمرت بها أن تكلف الخبراء بإجراء أبحاث معينة أو سماع أي شخص معين باسمه قد يكون قادرا على مدهم بالمعلومات ذات الطابع الفني".

ج -إبداع الخبرة التقنية

بعد انتهاء الخبير من أبحاثه وفحوصاته، يعد تقريراً يضمنه خلاصة ما توصل إليه من نتائج، بعد تطبيق الأسس العلمية والفنية على المسائل محل البحث، على الخبير إبداع تقرير خبرته لدى كتابة الجهة القضائية التي أمرت بالخبرة، خلال الآجال المحددة في أمر التعيين، ولا يجوز إستبداله بغيره مالم يطلب الخبير تمديد هذه الآجال.

ثانيا: الضوابط الفنية للخبرة التقنية

تعتبر عملية تجميع الأدلة من أصعب الأمور التي تواجه الخبير التقني، كان لزاما عليه أن يتبع عدة خطوات واعتماد تقنيات ومهارات علمية مهمة والاستعانة بوسائل تكنولوجية متطورة.

1 - أساليب عمل الخبير التقني

للخبير التقني في سبيل تحري الحقيقة، فله كامل الصلاحيات في أن يستخدم الوسائل والأساليب العلمية للوصول إلى الحقيقة، وهناك أسلوبان لعمل الخبيرهما:

الأول: يتمثل في تجميع وتحصيل لمجموعة من المواقع التي تشكل جريمة في ذاتها، كما هو الشأن في جرائم النصب والتهديد والسب، أو في بث صور فاضحة بقصد الدعاية للتحريض، ثم القيام بعملية تحليل رقمي لها لمعرفة كيفية إعدادها، برمجيا ونسبتها إلى مسارها الذي أعدت فيه، وتحديد عناصر حركتها، و من تم التوصل في النهاية إلى معرفة بروتوكول الأنترنت IP الذي ينسب إلى جهاز الحاسب الذي صدر عنه هذا الموقع.¹

الثاني: أما الأسلوب الثاني، يتمثل في القيام بتجميع وتحصيل لمجموعة المواقع التي لا يشكل موضوعها جريمة في ذاته، وإنما تؤدي في حال تتبع موضوعها إلى قيام الأفراد بإرتكاب جرائم، كما هو الحال في المواقع التي تساعد الغير على التعرف على جرعات المخدرات والمؤثرات العقلية، ذلك حسب وزن الإنسان بإدعائه أنه إذا تم تتبع التعليمات الواردة فيها فلن يطالب الشخص بحالة إدمان، وأيضا كيفية زراعة المخدرات بعيدا عن أعين الغير، وأيضا كيفية إعداد القنابل وتخزينها ...، ويتم في إطار تصنيف

¹ - خالد ممدوح إبراهيم، فن التحقيق الجنائي، المرجع السابق، ص301.

المواقع المذكورة إستخدام برمجيات متطورة مهمتها الكشف عن هذه المواقع بإستمرار، ومعرفة الجديد فيها.¹

2- وسائل الخبير لإنجاز الخبرة التقنية

يستخدم الخبير التقني العديد من الوسائل العلمية والبرمجيات التي تمكنه من إستخلاص الدليل الإلكتروني وتساعده في الوصول إلى المجرم المعلوماتي، منها الوسائل المادية وأخرى إجرائية والتي تتمثل فيما يلي:

أ- الوسائل المادية: وهي الأدوات الفنية التي غالبا ما يستخدم الخبير في الفضاء الرقمي وهي:

بروتوكول الأنترنت (IP)

ويسمى بعنوان الأنترنت هو نظام يشبه عنوان البريد العادي، يعمل على ترسل حزم البيانات عبر شبكة الأنترنت وتوجيهها إلى أهدافها، فهو موجود في كل جهاز إلكتروني مرتبط بشبكة الأنترنت، ويتكون من أربعة أجزاء كل جزء يتكون من أربعة خانات، ويشير الجزء الأول من اليسار إلى المنطقة الجغرافية، والجزء الثاني لمزود الخدمة والجزء الثالث لمجموعة الأجهزة الإلكترونية المرتبطة، والجزء الرابع يحدد الجهاز الذي تم الإتصال به²، وفي حالة وقوع جريمة إلكترونية فيمكن للخبير إتباع المسار التراسلي للبروتوكول (IP) للبحث عن رقم الجهاز المستعمل في إرتكاب الجريمة، ومن ثم تحديد موقعه، ومنه معرفة الجاني.

- نظام البروكسي (proxy)

كلمة إنجليزية وتعني الوكيل، يعمل هذا النظام كوسيط بين المشتركين لدى إحدى شركات تقديم خدمة الأنترنت، وبين المواقع الموجودة على الشبكة العالمية، بحيث يضمن مقدم الخدمة توفير الذاكرة الجاهزة، ويقوم هذا النظام على تلقي مزود البروكسي طلبا من المستخدم للبحث عن صفحة ما ضمن الذاكرة الجاهزة، فيتحقق البروكسي فيما إذا كانت هذه الصفحة قد تم تنزيلها من قبل، فيقوم بإرسالها إلى المستخدم دون الحاجة إلى إرسال الطلب إلى الشبكة العالمية مرة أخرى، وهنا يستخدم البروكسي أحد عناوين (IP) ومن أهم مزايا هذا النظام، أن الذاكرة المتوفرة لديه تحتفظ وتخزن كل عمليات التنزيل التي

¹ - عمر أبو بكر بن يونس، الجرائم الناشئة عن إستخدام الأنترنت، المرجع السابق، ص، ص 1043-1044.

² - سليمان بن مهج الغنزي، المرجع السابق، ص98.

تمت عليه¹، والتي يمكن أن تساعد الخبير على اقتناء الأدلة.

- برامج التتبع المعلوماتية

تقوم هذه البرامج بالتعرف على محاولات الإختراق، التي تتم مع تقديم بيان بها إلى المستخدم الذي تم إختراق جهازه، ويحتوي هذا البيان على إسم الحدث وتاريخ حدوثه، وعنوان IP الذي تمت من خلال عملية الإختراق، وإسم الشركة المزودة لخدمة الأنترنت المستضيفة للمخترق، وأرقام مداخلها ومخارجها على شبكة الأنترنت ومعلومات أخرى.²

-نظام كشف الإختراق

و يرمز إليه اختصارا بالأحرف IDS، وهذه الفئة من البرامج تتولى مراقبة بعض العمليات التي يجري حدوثها على أجهزة الحاسوب أو الشبكة³، ويتم ذلك من خلال تحليل رزم البيانات أثناء إنتقالها عبر الشبكة من بعض ملفات التشغيل الخاصة بتسجيل الأحداث، فور وقوعها في جهاز الحاسب الآلي أو الشبكة، ومقارنة نتائج التحليل بمجموعة من الصفات المشتركة للإعتداءات على الأنظمة الحاسوبية، والتي يطلق عليها أهل الإختصاص مصطلح التوقيع، وفي حالة إكتشاف النظام لوجود أحد هذه التوقيعات يقوم بإصدار مدير النظام بشكل فوري، ويسجل البيانات الخاصة بهذا الإعتداء في سجلات الكمبيوتر الخاصة.⁴

ب- الوسائل الإجرائية: ويقصد بها الإجراءات التي تهدف إلى البحث عن الدليل، ومن ثم يمكن للمحقق وبمساعدة من الخبير تحديد شخصية مرتكب الجريمة⁵ ومن بين هذه الإجراءات:

-الذكاء الصناعي

يقصد بالذكاء الصناعي تقنيات وبرامج الحاسب الآلي، التي يستعين بها الخبير التقني لحصر

¹ - ممدوح عب الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والأنترنت، دار الكتب القانونية، المحلة الكبرى، د ط، 2006، ص 83.

² - حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الأنترنت، المرجع السابق، ص 513.

³ - علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة الإلكترونية -دراسة مقارنة- دار الكتاب الجامعي الحديث، الإسكندرية، ص 72.

⁴ - محمد بن نصير السرحاني، المرجع السابق، ص 84.

⁵ - خال ممدوح إبراهيم، فن التحقيق في الجرائم الإلكترونية، المرجع السابق، ص 307.

الأسباب والفرضيات المتعلقة بالجريمة، وجمع الأدلة الجنائية وتحليلها، واستخلاص الحقائق منها، عن طريق عمليات حسابية يتم حلها بواسطة برنامج الحاسوب صممت خصيصا لهذا الغرض، كبرنامج (X tree pro gold)، الذي يستخدم للعثور على الملفات المبحوث عنها في أي مكان على الشبكة، أو الأقراص الصلبة أو الأقراص المرنة المضغوطة، وقراءة محتوياتها في صورتها الأصلية من أجل التحليل والتقويم.¹

-اقتفاء الأثر

يمكن تقصي أثر المجرم ارتكابه لجريمة إلكترونية، في حالة إذا لم يتم بمسح آثار جريمته، ويمكن تقصي الأثر بعدة طرق، سواء عن طريق بريد إلكتروني ثم إستقباله، أو عن طريق تتبع أثر الجهاز الذي تم إستخدامه للقيام بعملية الإختراق.

- الإطلاع على عمليات التنظيم المعلوماتي وأسلوب حمايته

ينبغي على المحقق وهو بصدد التحقيق في إحدى الجرائم الإلكترونية، أن يطلع على النظام المعلوماتي وشبكاته والإطلاع على عمليات النظام المعلوماتي كقاعدة البيانات وإدارتها، و خطة تأمينها ومعرفة مواد النظام والمستفيدين والملفات، وإلى غير ذلك من الإجراءات، التي تهدف إلى إحاطة كاملة بالنظام المعلوماتي للتعرف على الجريمة الإلكترونية.²

و في الأخير يمكن القول أن الإستعانة بخبير من أجل إثبات الجريمة الإلكترونية، أضحي شيء حتمي وضروري تفرضه الطبيعة الخاصة والتميز لهذه الجريمة، ونظرا للتكوين القانوني البحث للسلطات القضائية المختصة في مكافحة الجريمة من جهة، ونقص خبرتهم وكفاءتهم الفنية من جهة أخرى وعجزها عن جمع الدليل الإلكتروني، تفرض وجود خبير في مجال المعلوماتية، مما يعكس أهمية الخبرة التقنية لمواجهة الجريمة الإلكترونية.

المطلب الثالث: الشهادة في الجريمة الإلكترونية

تعد الشهادة من أقدم وأبرز وسائل الإثبات للحصول على الأدلة، فالشهادة في مجال الإجراءات الجزائية لها أهمية كبيرة وبالغة، لأن الجريمة ليست تصرفا قانونيا ولكنها عمل غير مشروع يجتهد الجاني

¹ - جمال إبراهيمي، المرجع السابق، ص 81.

² - خالد ممدوح إبراهيمي، المرجع السابق، ص 308.

في التحكم عند قيامه به، ويحرص على إخفاءه عن أعين الناس، وذلك فعندما يتم العثور على شاهد فإن ذلك يعتبر مكسبا للعدالة¹، لذلك قال بنثام (Bentham) إن الشهود هم عيون القضاء وآذانها²، والشهادة هي إجراء من إجراءات التحقيق، وهي المعلومات التي تتعلق بالجريمة التي يدلي بها الشاهد أمام سلطة التحقيق، وهي الطريق العادي للإثبات الجنائي، كما لا تقل الشهادة أهمية مثل باقي الإجراءات لإستخلاص الدليل الإلكتروني، لهذا سوف نتطرق إلى مفهوم كل من الشهادة و الشاهد في الجريمة الإلكترونية في (الفرع الأول) والتزامات الشاهد المعلوماتي في (الفرع الثاني).

الفرع الأول: مفهوم الشهادة والشاهد المعلوماتي في الجريمة الإلكترونية

نتطرق في هذا الفرع إلى تعريف الشهادة (الفقرة الأولى) ثم نتبعه بتعريف الشاهد المعلوماتي وأهم

تصنيفاته

أولاً: تعريف الشهادة

اختلف الفقه في إعطاء تعريف للشهادة، فمنهم من عرفها على أنها "أقوال التي يدلي بها غير الخصوم أمام سلطة التحقيق، أو القضاء بشأن جريمة وقعت، سواء كانت تتعلق بثبوت الجريمة وظروف ارتكابها، وإسنادها إلى المتهم أو براءته منها".³، كما تعرف أيضا بأنها "واقعة معينة من خلال ما يقوله أحد الأشخاص، عما شاهده أو سمعه أو أدركه بحواسه عن هذه الواقعة بطريقة مباشرة".⁴

أما في مجال الجريمة الإلكترونية، ظهر نوع مستحدث من الشهادة يسمى بالشهادة الإلكترونية، حيث لم يتضمن أي من التشريع القائم تعريفا للشهادة الإلكترونية، غير أنه إعمالا للإجتهادات الفقهية في تعريف الشهادة التقليدية يمكن تعريف الشهادة الإلكترونية على أنها " تقرير الشخص لما يكون قد رآه أو سمعه أو أدركه على وجه العموم بحواسه، على أن يتم هذا التقرير عبر نظم المعلوماتية أو الوسائط الإلكترونية".⁵، ومصطلح الشهادة الإلكترونية يطلق على نوع من الشهادة لا يكون فيها الشاهد حاضرا

¹ - سليمان غازي العتيبي، المرجع السابق، ص76.

² - عائشة بن قارة مصطفى، المرجع السابق، ص77.

³ - عائشة بن قارة مصطفى، المرجع نفسه، ص77.

⁴ - أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، 1985، ص177.

⁵ - عادل بوزيدة، دور الشهادة الإلكترونية في الإثبات الجزائي على ضوء قانون الإجراءات الجزائية الجزائري، مجلة النبراس للدراسات القانونية، المجلد الأول، العدد الأول، سبتمبر 2016، ص 137.

لجلسة التحقيق بذاته المادية أي جسديا، و إنما تتم عبر وسائل إلكترونية أو رقمية.¹

لقد نظم المشرع الجزائري هذا النوع من الشهادة بموجب القانون رقم 15-03 المؤرخ في 2015/02/1² يتعلق بعصرنة العدالة، الذي سمح من خلاله إستخدام و لأول مرة إستعمال الطرق التكنولوجية في قطاع العدالة، خاصة إستعمال المحادثة المرئية عن بعد *vidéo conférence* أثناء الإجراءات القضائية، والتي يلجأ إليه أساسا في حالات بعد المسافة أو إذا تطلب حسن سير العدالة ذلك، كما أجاز إستخدامها بموجب الأمر 15-02³ المعدل والمتمم لقانون الإجراءات الجزائية في مجال حماية الشهود والخبراء والضحايا، حيث تجيز المادة 65 مكر 27 لجهة الحكم سماع الشاهد مخفي الهوية عبر المحادثة المرئية عن بعد، ويتمثل هذا الإجراء بحماية الشهود الذين بسبب خوفهم من إلحاق الأذى بشخصيتهم أو بدويهم يحجمون عن الإدلاء بشهادتهم، فجاء المشرع لفرض ضمانات لحماية الشاهد وعائلته في جرائم حددت بموجب المادة 65 مكرر 19 من ق.إ.ج.ج، وهي الجرائم الخاصة منها الجريمة المنظمة والإرهاب وجرائم الفساد، وقد استثنى منها باقي الجرائم ومنها الجرائم الإلكترونية التي تعتبر فيها الشهادة من أبرز طرق الإثبات الأكثر فعالية.

وهذه الآلية أصبحت مفعلة على أرض الواقع في الجزائر، حيث قدمت أول محاكمة و إستخدمت فيها هذه التقنية، القضية التي أستجوب فيها المتهم المحبوس بمؤسسة إعادة التربية والتأهيل بمدينة القليعة عن طريق الشاشة الإلكترونية، بعد إقراره بالوقائع المنسوبة إليه، فأصدرت المحكمة حكما بإدانة المتهم⁴، كذلك أستخدمت هذه التقنية لسماع شاهد من فرنسا على مستوى مجلس قضاء المسيلة يوم 11 جويلية 2016 في قضية تتعلق بمجموعة إغتالت شرطيا في فرنسا إستطاع أحدهم الهروب إلى الجزائر،

¹ - خالد ممدوح إبراهيم، المرجع السابق، ص 260.

² - القانون رقم 15-03 المؤرخ في 2015/02/01، المتعلق بعصرنة العدالة، الجريدة الرسمية للجمهورية الجزائرية، عدد6 الصادر بتاريخ 2015/02/10.

³ - الأمر 15-02 المؤرخ في 2015/07/23 المعدل والمتمم للأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية، عدد40 الصادرة بتاريخ 2015/07/23.

⁴ - حكم عن محكمة القليعة قسم الجench، قضية رقم 17982 بتاريخ 07 أكتوبر 2015، مشار إليه لدى خضرة شنتير، الآليات القانونية لمكافحة الجريمة الإلكترونية، -دراسة مقارنة- أطروحة لنيل شهادة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية، أدرار، 2020 - 2021، ص 242.

وقد قررت محاكمته في الجزائر بدل تسليمه لفرنسا بإعتباره أنه جزائري الجنسية.¹

كما تتخذ الشهادة الإلكترونية إحدى صورتين: الأولى الشهادة المسجلة وتعني الأقوال المدلى بها والمسجلة سلفا في تاريخ سابقا لجلسة المحاكمة، أما الثانية فهي الشهادة الإلكترونية الفورية وهي الشهادة التي يتم الإدلاء بها مباشرة في مواجهة الخصوم، عن طريق وسيط رقمي على النحو الذي يتبع لجهات التحقيق والخصوم مناقشتها شفاهة والرد بشأنها فورا.²

ثانيا: المقصود بالشاهد المعلوماتي

الشاهد بصفة عامة يعرف بأنه " كل شخص حلف اليمين القانونية وتوافرت فيه قدرة الإدراك والتمييز على الإدلاء أمام المحقق أو مجلس القضاء، بما شاهده من عمل الغير أو سمعه أو أدركه بإحدى حواسه بغية إثبات الجريمة أو نفيها عن المتهم".³، أما فيما يخص الجريمة الإلكترونية يعرف بأنه " الفني صاحب الخبرة والتخصص في تقنية وعلوم الحاسبة الإلكترونية والذي لديه معلومات جوهرية أو مهمة لازمة للولوج في نظام المعالجة الآلية للبيانات، إذا كانت مصلحة التحقيق تقتضي التتقيب عن أدلة الجريمة داخله".⁴، لذلك يطلق على هذا الشخص إسم الشاهد المعلوماتي تمييزا له عن الشاهد التقليدي وعليه يتميز الشاهد المعلوماتي عن الشاهد التقليدي، بكونه لا يكتف فقط بسرد ما شاهده أو سمعه أو رآه فقد، وإنما يتطلب أن يتمتع بقدر من الخبرة في مجال الأنظمة المعلوماتية وشبكات الإتصال.

وقد يحدث أن تتداخل صفة الشاهد مع صفة الخبير في مجال نظم المعلوماتية، ويمكن أن نتصور ذلك، في الحالة التي يكون فيها شخص الشاهد يملك أيضا وبحكم وظيفته في ميدان من ميادين المعالجة الآلية للبيانات، معرفة وقدرات تؤهله للتحكم في النظم المعلوماتية، ففي هذه الحالة لن يكتفي بما سمعه أو رآه، بل أن شهادته ستتضمن تصريحات يظهر من خلالها معرفته بالنظم المعلوماتية.

¹ - مريم لوكال، الآليات القانونية المستحدثة لحماية الشهود والخبراء والضحايا بموجب الأمر 15-02 المعدل والمتمم لقانون الإجراءات الجزائية . دراسة مقارنة . مجلة حوليات جامعة الجزائر 1، العدد 1، الجزء الثاني، ص 112.

² - عادل بوزيدة، المرجع السابق، ص 138.

³ - سلطان الشاوي، أصول التحقيق الإجرامي، مطبعة جامعة بغداد، 1982، ص 99.

⁴ - رضا هميسي، أحكام الشاهد في الجريمة المعلوماتية، ورقة علمية مقدمة في إطار الملتقى الوطني الجريمة المعلوماتية بين الوقاية والمكافحة، مخبر الحقوق والحريات في الأنظمة المقارنة، كلية الحقوق، جامعة بسكرة، المنعقد بين 16-17/2015، ص 2.

لكن يمكن أن نفرق بين الشاهد المعلوماتي والخبير، حيث أن هذا الأخير يقوم بتقديم تقارير وآراء ونتائج توصل إليها من خلال تطبيق معايير علمية وأصول فنية دقيقة، أما الشاهد فيقدم معلومات تحصل عليها بالملاحظة الحسية.

و هي تشمل عدة طوائف أهمها:

1- مشغلو الحاسب الآلي

هو ذلك الشخص المسؤول عن تشغيل جهاز الحاسب الآلي، والمعدات المتصلة به، لذلك يجب أن يكون لديه خبرة كبيرة في استخدام جهاز الحاسب الآلي ومكوناته، مثل وضع القرص في وحدة الأقراص واستخدام لوحة المفاتيح في إدخال البيانات، كما تكون لديه معلومات عن قواعد كتابة البرامج.¹

2- المحللون

المحلل (Analyst) وهو الشخص الذي يحلل الخطوات، ويقوم بتجميع بيانات نظام معين، ودراسة هذه البيانات ثم تحليل النظام، أي تقسيمه إلى وحدات منفصلة وإنتاج العلاقات الوظيفية من هذه الوحدات، كما يقوم بتتبع البيانات داخل النظام عن طريق ما يسمى بمخطط تدفق البيانات، وإنتاج الأماكن التي يمكن ميكنتها بواسطة الحاسب الآلي.²

3- خبراء البرمجة

مخطوطو البرامج (Programmers) وهم الأشخاص المتخصصون في كتابة أوامر البرامج ويمكن تقسيمهم إلى فئتين:

الفئة الأولى: هم مخطوطو برامج التطبيقات، حيث يقومون بالحصول على خصائص ومواصفات النظام المطلوب من محلل النظم، ثم يقومون بتحويلها إلى برامج دقيقة وموثوقة لتحقيق هذه المواصفات، أما الفئة الثانية: هم مخطوطو النظم ويقومون باختبار وتعديل وتصحيح برامج نظام الحاسب الآلي الداخلية آية تعديلات أو إضافات لها.³

¹ - أشرف عبد القادر قنديل، الإثبات في الجريمة الإلكترونية، دار الجامعة الجديدة، الإسكندرية، د ط، 2015، 161.

² - عبد الله حسين علي محمود، المرجع السابق، ص 388.

³ - عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجزائية في جرائم الكمبيوتر والأنترنت دار الكتب القانونية، المحلة الكبرى، 2007، ص 158.

4 - مهندسو الصيانة والإتصالات

وهم المسؤولون عن أعمال الصيانة بتقنيات الحاسب الآلي بمكوناته وشبكات الاتصال المتعلقة به.

5 - مديرو النظم

وهم الذين يوكل لهم أعمال الإدارة في النظم المعلوماتي.¹

بالإضافة إلى هذه الفئات، هناك من يعتبرون بمثابة شاهد معلوماتي في الجريمة الإلكترونية، ويلعبون دورا كبيرا في توصيل الأشخاص إلى شبكة الأنترنت منهم مقدمو الخدمات، أيضا متعهد الوصول، ومتعهد الإيواء، وناقل المعلومات ومسؤولو متعدد الخدمات.

بالرجوع إلى المشرع الجزائري نجده ألزم مقدمو الخدمات بموجب المادة 10 من القانون 09-04 بالتزامات منها مساعدة السلطات القضائية المكلفة بالتحريات لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات أو المعطيات المتعلقة بحركة السير.²

الفرع الثاني: إلتزامات الشاهد المعلوماتي

هناك إختلاف واضح بين الشاهد العادي والشاهد المعلوماتي، ففي الجرائم العادية كل شخص تنطبق عليه شروط أداء الشهادة هو أهل لها، في حين أن الشاهد في الجرائم المعلوماتية، لا بد أن يكون منتميا إلى فئات معينة ليعتد بالشهادة³، ففي حالة وقوع جريمة إلكترونية، وتم إستدعاء الشاهد المعلوماتي بالإدلاء بشهادته فعليه أن يستجيب لذلك، لكن وفقا للقواعد العامة الواردة في قانون إجراءات جزائية⁴ لهذا نجد أن الشاهد ملزم بالإدلاء بما سمعه أو رآه، غير أن الطبيعة الخاصة للجريمة الإلكترونية تضع الشاهد أمام إلتزام آخر وهو الإلتزام بالإعلام.

فمن خلال هذا الفرع نتناول الأساس الفقهي لإلتزام الشاهد (أولاً) ثم التطرق لمضمون الإلتزام (ثانياً).

¹ - خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 264.

² - المادتان 10-11 من قانون رقم 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها .

³ - دلال مولاي ملياني، شهادة الشهود في جرائم تكنولوجيا الإعلام والاتصال، مجلة البحوث القانونية والسياسية، عدد 06، جوان 2016، ص 297.

4 - تناول المشرع الجزائري التزامات الشاهد أثناء الإدلاء بشهادته من خلال نص المادة 89 من ق.إ.ج.ج، حيث يتحمل الشاهد ثلاث التزامات هي: الالتزام بالحضور ، حلف اليمين ، الادلاء بشهادته.

أولاً: الأساس الفقهي للإلتزام الشاهد

اختلف الفقه حول جواز إجبار الشاهد في الجريمة الإلكترونية على تقديم المعلومات، وانقسم الفقه بين مؤيد ومعارض لهذا الإلتزام.

1- الاتجاه الأول

ويرى أنصار هذا الإتجاه أنه ليس من واجب الشاهد وفقاً للإلتزامات التقليدية للشهادة، أن يقوم بطبع ملف البيانات أو الإفصاح عن كلمات المرور، أو الشفرات الخاصة بالبرامج المختلفة، ويميل إلى هذا الإتجاه الفقه الألماني حيث يرى إلى عدم إلتزام الشاهد بطباعة البيانات المخزنة في ذاكرة الحاسوب على أساس أن الإلتزام بأداء الشهادة لا يتضمن هذا الواجب، كذلك في تركيا فلا يجوز إكراه الشاهد لحمله على الإفصاح عن كلمات المرور السرية، أو كشف ثغرات تشغيل البرامج المختلفة.¹

2- الإتجاه الثاني

على عكس الإتجاه الأول يرى أنصار هذا الإتجاه، أن من بين الإلتزامات التي يتحملها الشاهد القيام بطباعة البيانات أو الإفصاح عن كلمات المرور، أو الشفرات الخاصة بالبرامج المختلفة، ومن التشريعات التي تفرض واجب تعاون الشاهد في الجريمة الإلكترونية القانون الإنجليزي الصادر عام 1984 في شأن البوليس والأدلة الجنائية، حيث يسمح للمحققين أن يطلبوا من الغير لتمكينهم الدخول إلى المعلومات المخزنة في الحاسب الآلي للإطلاع عليها أو قراءتها.²

كما يتيح مشروع قانون الحاسب الآلي في هولندا، سلطات التحري والتحقيق بأن يصدرُوا أمراً إلى القائم بتشغيل النظام لتقديم المعلومات اللازمة لإختراقه والولوج إلى داخله للإفصاح عن كلمة المرور السرية، والشفرات الخاصة بتشغيل البرامج المختلفة، كما يلزمون القائم على تشغيل النظام المعلوماتي بحل رموز هذه البيانات.³

¹ Mohrenschlager(Manfred) : « computer crimes and othors crimes against information - technology in R.I.D.P.1993,p351 Germany » مشار إليه لدى عبد الله حسين علي محمود، المرجع السابق، ص 390.

² - رضا هميسي، المرجع السابق، ص 6.

³ - نزيهة مكاري، وسائل الإثبات في جرائم الإعتداء على حق المؤلف عبر الأنترنت، مجلة المناهج القانونية، العدد 13-14، ص 77.

وقد تبني الفقه الفرنسي هذا الإتجاه، حيث يرى بعض الفقهاء أن المشرع لم ينظم هذه المسألة فإنه لا مناص من تطبيق القواعد العامة في الشهادة، وعليه يلتزم الشهود بكشف كلمات المرور وشفرات تشغيل البرامج، ما عدا حالات المحافظة على سر المهنة فإنهم يكونون في حل من هذا الإلتزام.¹

كما نصت الفقرة الرابعة من المادة 18 من الإتفاقية الأوروبية للجريمة الإلكترونية وجاء فيها "يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية، من أجل تخويل سلطاته المختصة سلطة إصدار الأمر، لأي شخص لديه معلومات عن تشغيل النظام أو الإجراءات المطبقة من أجل حماية البيانات المعلوماتية، التي تتضمن تقديم كل المعلومات الضرورية على نحو معقول يسمح بتطبيق الإجراءات المشار إليها في الفقرتين 1 و2."، يتبين من نص المادة أنها تتعلق بالإلزام مقدمو خدمات الأنترنت بالتعاون مع سلطات التحري والتحقيق بعمليات التفتيش والضبط، لجمع الدليل الإلكتروني، أما المعلومات التي يمكن إلزام مقدمي الخدمات تقديمها هي المعلومات الضرورية التي تسمح بتطبيق إجراءات التفتيش والضبط أو أي طريقة تهدف إلى الوصول إلى الدليل الإلكتروني.

أما بالنسبة لموقف المشرع الجزائري تناول هذه المسألة، بموجب المادة 10 من قانون 04-09، والتي نصت من خلالها على إلتزامات تقع على عاتقهم ومنها الإلتزام بالمساعدة والتعاون مع سلطات التحري والتفتيش من أجل تزويدهم بكافة المعطيات المتعلقة بمحتوى الإتصالات، وفي حالة الإخلال بهذا الإلتزام تقوم في حقهم عقوبات جزائية تتمثل في جريمة عرقلة حسن سير التحريات القضائية، وبالتالي أصبح الإلتزام بالإعلام بعد صدور القانون 04-09 مقننا.²

ثانيا: مضمون الإلتزام بالإعلام في الجريمة الإلكترونية

إن الإعلام في الجرائم الإلكترونية جوهرها، متى كان الشاهد المعلوماتي حائزا لمعلومات جوهرية لازمة لإختراق نظام المعالجة الآلية للمعطيات، بحثا عن أدلة داخلية تتطلبها مصلحة التحقيق، فإنه يكون مطالبا بأن يعلم سلطات التحقيق والتحري على سبيل الإلزام، وإلا تعرض للعقوبات المقررة للامتناع عن

¹ - jacque francillon , les cimes informatiques et d'autres crimes dans le domaine de la technologie informatique en France, rev. Int. Pen, 1990 vol 64, p 309.

مشار إليه : عبد العال الديربي، محمد صادق إسماعيل، المرجع السابق، ص 316.

² - دلال مولاي ملياني، إشكالية الإثبات في جرائم الإثبات في التشريع الجزائري، المرجع السابق، ص 145.

الشهادة وذلك في غير الأحوال التي يجيز له القانون فيها ذلك.¹

1- السمات الجوهرية لإلتزام الشاهد

يتضمن إلتزام الشاهد المعلوماتي مجموعة من السمات الجوهرية نذكرها فيما يلي:

أ- إلتزام الشاهد بالإعلام إلتزاما قانونيا

بمعنى لا بد من وجود نص قانوني صريح يلزم الشاهد بإعلام سلطات التحقيق بالمعلومات والبيانات الجوهرية، التي تساعد في الوصول إلى أدلة الجريمة الإلكترونية وتحديد الفاعل فيها.

ب - إستقلالية الإلتزام بالإعلام

الإلتزام بالإعلام عن الجريمة الإلكترونية هو إلتزام مستقل وله ذاتية خاصة به، أي أن إلتزام الشاهد المعلوماتي هو إلتزام مستقل عن بقية إلتزامات الشاهد التقليدية، وهو واجبا جديدا يشترط أن يفرضه القانون على بعض الفنين والمبرمجين والمحليين ومستخدمي أجهزة الحاسوب، ومضمون هذا الواجب هو تقديم المعلومات الجوهرية والهامة التي لها علاقة بمحل البحث والتحقيق.²

ج - الإلتزام بالإعلام إلتزام وقائي

يعتبر الإلتزام بالإعلام في الجريمة الإلكترونية إلتزاما وقائيا في بيئة تكنولوجيا المعلومات، ويترتب على مراعاة هذا الإلتزام والأخذ به تجنب ضبط شبكات الحاسب الآلي، وبالأخص الشبكات الكبيرة أو الممتدة، فمن الملاحظ أن الشكوى تنثر في الحالات التي تكون فيها البيانات مخزنة في وحدة معالجة مركزية في حاسب ضمن شبكة معلوماتية ممتدة، ففي هذه الحالة يمكن المحقق ضبط هذا النظام الشبكي بأكمله وعزله عن البيئة المحيطة به، وبؤدي إلى المساس بحقوق الغير في النظام محل الضبط³، لذلك فإنه ينبغي عدم التحفظ على الشبكة بأكملها وإنما على نوع محدد من البيانات محل الشك، وبالتالي فإن الإلتزام عن الإعلام في الجرائم الإلكترونية يلعب دورا وقائيا في بيئة تكنولوجيا المعلومات.⁴

¹ - عبد الله أحمد هلال، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، دار النهضة العربية، القاهرة، ط2، 2008، ص 25.

² - رضا هميسي، المرجع السابق، ص 9.

³ - يحيى الشديدي، الشهادة في الجريمة الإلكترونية، مجلة جامعة البعث، المجلد 38، العدد 50، 2016، ص 54.

⁴ - رضا هميسي، المرجع السابق، ص 8.

2- شروط الالتزام بالإعلام في الجريمة الإلكترونية

إن إلزام الشاهد بالإعلام في الجريمة الإلكترونية له شروط لا بد من تحققها، بغير هذه الشروط لا يكون الشاهد المعلوماتي ملزما بالإعلام عن الجريمة، وتتلخص هذه الشروط بالآتي:

أ - أن نكون بصدد جريمة إلكترونية

حتى يلتزم الشاهد المعلوماتي بالإعلام في الجريمة الإلكترونية، فلا بد أن تكون هذه الجريمة قد وقعت بالفعل حتى يتحقق إلزام الشاهد المعلوماتي، لا يمكن أن يتحقق حسب القواعد العامة لضبط جريمة مستقبلية، حتى ولو كان هناك تحقيقات جدية تؤكد أن الجريمة سوف تقع بالفعل.

وقوع الجريمة بشكل فعلي لا يحقق هذا الإلتزام، بل أن تكون الجريمة الواقعة تحمل وصف جنائية أو

جناية.¹

ب - علم الشاهد ومعرفته بالمعلومات المتعلقة بالجريمة

إن معرفة الشاهد بمضمون المعلومات الجوهرية المتصلة بالنظام المعلوماتي محل الواقعة، تمثل شرطا هاما لنشأة الإلتزام بالإعلام في الجرائم الإلكترونية، ومضمون هذه المعلومات الجوهرية في ثلاث عناصر هي: طبع الملفات الخاصة بالبيانات والإفصاح عن كلمات السر والكشف عن مفاتيح الشفرات.²

ج - أن تقتضي مصلحة التحقيق الحصول على هذه المعلومات

حتى يقوم الجاني بأداء إلتزامه بالإعلام في الجريمة الإلكترونية، لا بد أن تتطلب مصلحة التحقيق الحصول على المعلومات الجوهرية، خاصة إذا كان الأمر يتطلب إختراق النظام المعلوماتي لأجل البحث عن أدلة الجريمة الكائنة بداخل هذا النظام.³

يعد التشريع الفرنسي سباقا في هذا المجال، إذ تلزم الشاهد المعلوماتي بالإعلام الإفصاح عن كلمات السر التي يعلمها، طبقا للقواعد العامة بموجب المواد 62 - 198 - 109 من قانون الإجراءات الجزائية

¹ - يحيى الشديدي، المرجع السابق، ص 59

² - عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، المرجع السابق، ص 623.

³ - عبد الفتاح بيومي حجازي، المرجع نفسه، ص 623.

فرنسي، ويعاقب جنائيا في حالة رفضه إعطاء هذه المعلومات في مرحلة التحقيق الابتدائي والمحاكمة.¹ وفي الأخير يمكن القول أن الشهادة في الجريمة الإلكترونية لها مكانة هامة في إثبات السلوكات الإجرامية المرتكبة من المجرم المعلوماتي، فالشاهد المعلوماتي يلعب دورا كبيرا لما يدلي به من معلومات تساعد الأجهزة القضائية في الوصول إلى الحقيقة، فدور الشاهد في الجريمة الإلكترونية يختلف تماما عن دور الشاهد في الجريمة التقليدية، فالإلتزامات المفروضة على الشاهد المعلوماتي تفرض تمتعه بالخبرة وأن يكون من الأشخاص الذين لهم دراية بالأنظمة المعلوماتية، مما يجعل شهادته لها أثر كبير في تقديم مفاتيح الحقيقة لحل لغز الجريمة الإلكترونية، من خلال الإلتزامه بإعلام سلطات التحقيق بما يفيد في كشف الجريمة، كما يجب معالجة موضوع إلتزام الشاهد المعلوماتي بسن نصوص تشريعية صريحة تسد الفراغ التشريعي في مجال الشهادة في الجريمة الإلكترونية.

المطلب الرابع: الإختصاص القضائي للجهات القضائية في الجريمة الإلكترونية

تعد مكافحة الجريمة الإلكترونية من أهم التحديات التي تواجه السلطات القضائية، وبالنظر للطبيعة الخاصة لها، وتميزها بمحل غير مادي، أي تتم في البيئة الافتراضية، مما يجعل الملاحقة القضائية للمجرم أمرا في غاية الصعوبة، خاصة وأن السلوك الإجرامي في هذه الجرائم يتجاوز حدود الدولة الواحدة² الذي ينجم عنه تنازع أكثر من جهة قضائية سواء وطنية أو دولية للنظر في الجرائم الإلكترونية، ولضمان الفعالية والسرعة، في معالجة هذه الجرائم قام المشرع بتعديلات لأحكام قانون الإجراءات الجزائية، بإدراج قواعد إجرائية توسع من دائرة إختصاص السلطات القضائية.

الفرع الأول: توسيع الإختصاص المحلي للجهات القضائية

يقصد بالإختصاص السلطة التي يقررها المشرع للقضاء، لأن ينظر في دعاوى معينة حددها القانون،³ فالإختصاص في المسائل الجزائية هو ولاية القاضي في نظر دعاوى جزائية معينة⁴، وتعتبر الجرائم الإلكترونية من أكثر الجرائم التي تثير بعض الإشكالات في مواجهتها خاصة مشكلة الإختصاص، فتطبيق القواعد التقليدية التي تحدد معايير الإختصاص لا تتلاءم مع طبيعة هذه الجرائم، وتماشيا مع

¹ - سليمان غازي العتيبي، المرجع السابق، ص 79.

² - أمينة علالي، المرجع السابق، ص 154.

³ - محمود نجيب حسيني، شرح قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، ط 2، 1988، ص 139.

⁴ - محمد طارق عبد الرؤوف الخن، المرجع السابق، ص 197.

التطور الحاصل في هذا المجال، قام المشرع الجزائري بتوسيع إختصاص كل من وكيل الجمهورية، قاضي التحقيق، وضباط الشرطة القضائية.

أولا: الإختصاص المحلي لوكيل الجمهورية

يعرف الإختصاص المحلي، بأنه "تلك الدائرة القضائية التي يستطيع فيها وكيل الجمهورية، مباشرة وظيفته بصفة مباشرة طبقا لقانون الإجراءات الجزائية".¹

ويعد وكيل الجمهورية ممثل النيابة العامة على مستوى المحكمة وهو العصب الحساس فيها، يتحدد إختصاصه المحلي بإحدى الحالات الثلاث بمكان وقوع الجريمة أو بمحل المشتبه فيهم أو المكان الذي تم القبض فيه أحد المشتبه فيهم وهذا ما نصت عليه المادة 37/1 من ق.ا.ج.ج " يتحدد الإختصاص المحلي لوكيل الجمهورية بمكان وقوع الجريمة، وبمكان إقامة أحد الأشخاص المشتبه في مساهمتهم فيها أو في المكان الذي تم في دائرته القبض على هؤلاء الأشخاص حتى ولو حصل هذا القبض لسبب آخر وعليه يمكن القول يتحدد إختصاص وكيل الجمهورية بتوافر هذه الأمكنة الآتية:

- أن تكون الجريمة قد أقيمت في دائرة إختصاص وكيل الجمهورية المكاني.
 - أن تكون إقامة أحد المشتبه في إرتكاب الجريمة بنفس دائرة إختصاص.
 - أن يكون قد أُلقي القبض على أي من المشتبه فيهم في تلك الدائرة ولو تم القبض لسبب آخر.
- ونظرا لظهور جرائم مستحدثة خطيرة ومنها الجريمة الإلكترونية بإعتبارها جرائم عابرة للحدود أضاف المشرع الجزائري الفقرة الثانية من المادة 37 من قانون الإجراءات الجزائية التي نصت على تمديد الإختصاص المحلي لوكيل الجمهورية، ليشمل إختصاص محاكم أخرى على أن يكون ذلك عن طريق التنظيم، في جرائم المخدرات، والجريمة المنظمة عبر الحدود الوطنية، والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف.²

ثانيا: توسيع الإختصاص المحلي لقاضي التحقيق

طبقا لنص المادة 40/1 ق.ا.ج.ج فإن الإختصاص المحلي يتحدد لقاضي التحقيق وفقا ل:

¹ - بغدادي مولاي ملياني، الإجراءات الجزائية في التشريع الجزائري، المؤسسة الوطنية للكتاب، الجزائر، د ط، 1992، ص 139.

² - المادة 37 من القانون رقم 04-14 المؤرخ في 10/11/2004 بالمعدل والمتهم لقانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية، عدد 71، الصادرة بتاريخ 10/11/2004.

-مكان وقوع الجريمة.

-أو محل إقامة أحد الأشخاص المشتبه في مساهمتهم في إقترافها.

-أو محل القبض على هؤلاء الأشخاص حتى ولو كان هذا القبض قد حصل لسبب آخر، إلا أنه تم توسيع الإختصاص الإقليمي لقاضي التحقيق ليشمل كافة الإقليم الوطني وذلك من خلال المادة 2/40 من قانون الإجراءات الجزائية والتي تنص على ".... يجوز تمديد الإختصاص المحلي لقاضي التحقيق إلى دائرة إختصاصه محاكم أخرى، عن طريق التنظيم في جرائم المخدرات ،والجريمة المنظمة عبر الحدود الوطنية، والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والارهاب والجرائم المتعلقة بالتشريع الخاص بالصرف".¹

ومن الملاحظ أيضا أن المادة 329 من ق.ا.ج.ج نصت على تمديد الإختصاص المحلي لقاضي التحقيق للمحكمة إلى دائرة إختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات أو الجريمة المنظمة عبر الحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب وكذا الجرائم والمتعلقة بالتشريع الخاص بالصرف. " ويدعم هذا التمديد ما جاءت به المادة 5 من القانون 04-09 التي شملت بتمديد الإختصاص إذا تعلق الأمر بمسرح الجريمة الافتراضي، إذ حاول المشرع الجمع بين المسرح العادي والمسرح الافتراضي² حيث نصت المادة 05 على "..... إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى، وأن هذه المعطيات يمكن الدخول إليها إطلاقا من المنظومة الأولى، يجوز تمديد التفتيش إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك."

ثالثا: توسيع الإختصاص المحلي لضباط الشرطة القضائية

أناط القانون الجزائري مهمة البحث والتحري للضبطية القضائية، عن الجرائم المحددة في قانون العقوبات، ويطلق على من يخول إليهم هذه المهمة بضباط الشرطة القضائية، وتوضع الشرطة القضائية بدائرة إختصاص كل مجلس قضائي تحت إشراف النائب العام، ويتولى وكيل الجمهورية إدارتها على كل مستوى كل محكمة وذلك تحت رقابة غرفة الإتهام.

¹ - المادة 2/40 معدلة بموجب القانون رقم 04-14 المعدل والمتمم لقانون العقوبات.

² - دلال مولاي ملياني، المرجع السابق، ص252.

كقاعدة عامة يمارس ضباط الشرطة القضائية إختصاصهم المحلي في حدود الدائرة التي يباشرون فيها وظائفهم المعتادة وهذا ما جاءت به المادة 1/16 من قانون الاجراءات الجزائية¹، إلا أنه ورد إستثناء على هذه القاعدة جاءت به الفقرة الثانية من المادة 16 ق.ا.ج.ج وهو تمديد إختصاص ضباط الشرطة القضائية إلى دائرة إختصاص المجلس القضائي الملحقين به إذا بررت حالة الإستعجال ذلك.

كما وسع المشرع الجزائري من الإختصاص المحلي لضباط الشرطة القضائية في مجال مكافحة الجريمة الإلكترونية فأجازت المادة 7/16 من ق.ا.ج.ج تمديد غختصاصات ضباط الشرطة القضائية في حالة البحث والمعاينة إلى كافة الإقليم الوطني والتي تنص على "غير أنه فيما تتعلق ببحث ومعاينة جرائم المخدرات، والجريمة المنظمة عبر الوطنية، والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف، يمتد إختصاص ضباط الشرطة القضائية إلى كافة الإقليم الوطني، ويعمل هؤلاء تحت إشراف النائب العام لدى المجلس القضائي المختص إقليميا ويعلم وكيل الجمهورية المختص إقليميا بذلك في جميع الحالات".

إن التعديلات الواردة في قانون الإجراءات الجزائية والمتعلقة بتوسيع إختصاص جهات المتابعة والتحقيق وبالتالي الحكم عما يتعلق الأمر بالجرائم الإلكترونية كان يهدف من وراءها وضع إطار إجرائي متماسك بإمكانه التحري والفصل في هذا النوع من القضايا بكل مهنية لإنجاز هذا الغرض يفترض أن تكون هذه الجهات معززة بقضاة متخصصين في كل المجالات.²

الفرع الثاني: القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

إن الإنتشار الواسع لمستعملي وسائل التكنولوجيا الحديثة زاد من تفشي الجرائم الإلكترونية في المجتمع الجزائري، مما أدى بالإضرار بمصالح الأفراد والجماعة ككل هذا من جهة، ومن جهة أخرى ومن أجل إزالة العقبات والعراقيل التي تواجهها المحاكم التقليدية في التصدي لها³، فإجراءات المتابعة والتحقيق

¹ - تنص المادة 1/16 على أنه " يمارس ضباط الشرطة القضائية إختصاصهم المحلي في حدود الدائرة التي يباشرون فيها وظائفهم المعتادة."

² - بن عيسى بن كثير، الإجراءات الخاصة المطبقة على الإجرام الخطير، نشرة القضاة، العدد 63 وزارة العدل، الديوان الوطني للاستغلال التربوية، الجزائر، 2008، ص 83.

³ - جمال الدين بوقرة، جمال الدين عنان، القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 07، العدد 01، 2022، ص 1674.

التقليدية قاصرة على مكافحتها، مما يلزم ضرورة تدخل المشرع الجزائري فبادر بإصدار الأمر 21-11 المؤرخ في 25 غشت 2021¹ المعدل لقانون الإجراءات الجزائية، أين إستحدث قطب جزائي وطني متخصص لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال²، وذلك تكريسا لفكرة التخصص القضائي من أجل مواجهة الجرائم الخطيرة.

أولا: نشأة القطب الجزائي

كعائته المشرع الجزائري لم يضع تعريفا للقطب الجزائي، إلا أنه تم تعريفه من البعض أن الأقطاب الجزائية بصفة عامة هي " جهات قضائية متخصصة للنظر في بعض الجرائم التي حددها القانون، وليست جهات قضائية خاصة تنشط بإجراءات قانونية خاصة تخرج عن النظام القضائي ساري المفعول."³، كانت البداية الحقيقية لظهور الأقطاب القضائية المتخصصة، كانت في صورة إختصاص إقليمي موسع في المادة الجزائية، ظهرت رسميا سنة 2004، مع صدور القانون رقم 04-14 المؤرخ في 10/11/2004 المتضمن تعديل قانون الإجراءات الجزائية، عندما تناول في المواد 37، 40، 329 إمكانية تمديد الإختصاص الإقليمي لكل من وكيل الجمهورية، قاضي التحقيق وقاضي الحكم عندما يتعلق الأمر بالبحث والتحري في جرائم خاصة وعلى سبيل الحصر وهي جرائم المخدرات، والجريمة المنظمة عبر الوطنية، والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وجريمة تبييض الأموال والإرهاب والجرائم التشريع الخاص بالصرف.

كما تم إدراج الأقطاب القضائية بموجب القانون العضوي 05-11 المؤرخ في 17/07/2005 المتضمن التنظيم القضائي، فقد نصت المادة 24 منه على أنه " يمكن إنشاء أقطاب قضائية متخصصة ذات إختصاص إقليمي موسع لدى المحاكم.

¹ - الأمر رقم 21-11 المؤرخ في 25 غشت 2021 يعدل ويتمم الأمر 66-156 المؤرخ في 8 يونيو 1966 والمتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية، عدد 65، الصادرة بتاريخ 26 غشت 2021.

² - عرفت المادة 211 مكرر 22 فقرة الثالثة من القانون 21-11 الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بأنه " يقصد بمفهوم هذا القانون، بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال، أي جريمة ترتكب أو يسهل ارتكابها استعمال منظومة معلوماتية أو نظام للاتصالات الإلكترونية أو أي وسيلة لأخرى أو آلية ذات صلة بتكنولوجيا الإعلام والاتصال." جاء هذا التعريف ليقوم بحذف عبارة "جرائم المساس بأنظمة المعالجة الآلية" عن نص المادة 2 من القانون 09-04 وذلك من أجل تجنب التكرار الواردة في المادة 2 من ق 09-04 أنظمة معلوماتية نفس المصطلح لمنظومة معلوماتية.

³ - جمال الدين بوقرة، جمال الدين عنان، المرجع السابق، ص 1676.

يتحدد الاختصاص النوعي لهذه الأقطاب حسب الحالة في قانون الإجراءات المدنية أو قانون الإجراءات الجزائية".، لكن هذه المادة فصل بعدم دستوريته بموجب الرأي رقم 01/ر ق ع/م د/05 المؤرخ في 17/06/2005 المتعلق بمراقبة القانون العضوي المتعلق بالتنظيم القضائي، وبعد الجدل الذي صادف ظروف نشأتها، وعليه أصبحت مجسدة على أرض الواقع منذ سنة 2008، وحددت هذه المحاكم ووزعت إلى القطب الجزائي المتخصص بمحكمة سيدي أحمد، قسنطينة، وهران، والقطب المتخصص لمحكمة ورقلة.

و نظرا لتطور وسائل الإتصال واستخدامها في كافة مجالات الحياة، وأثرها السلبي وما خلفته من سلوكيات غير مشروعة وخطورتها على إستقرار المجتمع وخاصة المساس بالحياة الخاصة للأفراد والإقتصاد، بالإضافة إلى غياب هيئات قضائية متخصصة قادرة على مواجهة هذه الجرائم، فقد أدت الضرورة الحتمية في إيجاد آليات هدفها الأساسي مواجهة الجريمة الإلكترونية، وما كان على المشرع الجزائري إلا قيامه بتعديل قانون الإجراءات الجزائية وإصدار الأمر 21-11 المؤرخ في 25/08/2021 الذي تم من خلاله إنشاء قطب جزائي مختص يعنى بمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وذلك بإستحداث الباب السادس ومن خلال المادة 211 مكرر 22 من ق.إ.ج.ج التي نصت على "ينشأ على مستوى محكمة مقر مجلس قضاء الجزائر، قطب جزائي وطني متخصص في المتابعة والتحقيق في الجرائم المتصلة بتكنولوجيا الإعلام والاتصال والجرائم المرتبطة بها، كما يختص بالحكم في الجرائم المنصوص عليها في هذا الباب إذا كانت تشكل جنحا."

ثانيا: قواعد إختصاص القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام

والإتصال

نص القانون 21-11 المعدل لقانون الإجراءات الجزائية على وجود جهة قضائية مختصة في النظر في الجرائم المرتكبة عن طريق تكنولوجيا الإعلام والاتصال، وخصها بقواعد إختصاص وإجراءات متابعة تختلف عن باقي الجرائم الأخرى.

1- الإختصاص النوعي للقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام

والاتصال

يقصد بالإختصاص النوعي هي أن تكون الجهة القضائية مختصة بالنسبة لنوع محدد من الجرائم،

التي يحددها القانون وذلك من حيث طبيعتها أو جسامتها (جناية أو جنحة أو مخالفة)¹، منح المشرع القطب الجزائي الوطني إختصاصا حصريا للنظر في الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وكذا الجرائم المرتبطة بها ولا يجوز لجهة قضائية أخرى أن تشترك في ذلك، حيث نصت المادة 211 مكرر 2/22 على "...في الجرائم المنصوص عليها في هذا الباب إذا كانت تشكل جنحا". أما المادة 211 مكرر 24 من ق.إ.ج.ج حددت على سبيل الحصر الجرائم التي يختص بها القطب الجزائي الوطني وهي جاءت كما يلي: "مع مراعاة أحكام الفقرة 2 من المادة 211 مكرر 22 أعلاه يختص وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وقاضي التحقيق ورئيس ذات القطب حصريا بالمتابعة والتحقيق والحكم في الجرائم المتصلة بتكنولوجيا الإعلام والاتصال المذكورة أدناه وكذا الجرائم المرتبطة به:

-الجرائم التي تمس بأمن الدولة أو الدفاع الوطنيين.

- جرائم نشر وترويج أخبار مغرضة كاذبة بين الجمهور من شأنها المساس بالأمن أو السكينة العامة أو إستقرار المجتمع،

-جرائم نشر وترويج أنباء مغرضة تمس بالنظام والأمن العموميين ذات الطابع المنظم أو العبر للحدود الوطنية،

-جرائم المساس بأنظمة المعالجة الآلية للمعطيات المتعلقة بالإدارات والمؤسسات العمومية،

-جرائم الإتجار بالأشخاص أو بالأعضاء البشرية أو تهريب المهاجرين،

-جرائم التمييز وخطاب الكراهية."

فمن خلال المادة السابقة الذكر نلاحظ أن هناك شروط أساسية لهذا الإختصاص الحصري هي:

-أن يتعلق الإختصاص على سبيل الحصر في الجرائم المذكورة في المادة 24/211 من قانون إجراءات جزائية.

-أن تأخذ هذ الجرائم وصف الجرح، حيث لا يمكن أن ينعقد لها الإختصاص في حالة الجنائيات.

¹ - أمينة بن عميور، إلهام بوحلايس، القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، مجلة البحوث في العقود وقانون الأعمال، المجلد 7، عدد 01، 2022، ص 67.

-أن تكون الجرائم المرتكبة لها صلة ومرتبطة بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

كما أضاف جرائم أخرى ضمن الإختصاص الحصري للقطب الجزائري الوطني للنظر دون سواء في الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، والتي أسماها بالجرائم أكثر تعقيدا والجرائم المرتبطة بها، وقد عرفت هذه الأخيرة بموجب المادة 211مكرر 25 من ق.إ.ج.ج على أنه "مع مراعاة أحكام ويقصد بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال الأكثر تعقيدا بمفهوم هذا القانون، الجريمة التي بالنظر إلى تعدد الفاعلين أو الشركاء أو المتضررين أو بسبب إتساع الرقعة الجغرافية لمكان إرتكاب الجريمة، أو جسامة آثارها أو الآثار المترتبة عليها أو لطابعها أو العابر للحدود الوطنية أو لمساسها بالنظام والأمن العموميين، تتطلب إستعمال وسائل تحري خاصة وخبرة فنية متخصصة للجوء إلى تعاون قضائي دولي."

2-الإختصاص المحلي للقطب الجزائري الوطني

حدد المشرع الجزائري نطاق الإختصاص المحلي للقطب الجزائري الوطني المتخصص في الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، أنه يمارس إختصاصا وطنيا في جميع الجرائم المخولة له قانونا وهي التي تضمنتها كل من المواد 211مكرر 24 و 211مكرر 25 من ق.إ.ج.ج، وهذا حسب ما جاء في المادة 211مكرر 23 من ق.إ.ج.ج بقولها أنه " يمارس وكيل الجمهورية لدى القطب الجزائري الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وكذا قاضي التحقيق، ورئيس ذات القطب صلاحياتهم في كامل التراب الوطني."

وفي ذلك نجد المشرع قد سبق وأن تطرق إلى توسيع قواعد الإختصاص للجهات القضائية، في الجرائم المتصلة بتكنولوجيا الإعلام والاتصال المرتكبة خارج الإقليم الوطني، عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني، وهذا ما تناولته المادة 15 من القانون 04-09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، مما يجعل من القطب الجزائري الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال له إختصاص النظر في هذه الجرائم.

كما أجاز القانون تمديد الإختصاص الوطني للقطب الجزائري الوطني، على جرائم التمييز وخطاب الكراهية التي تقع خارج الإقليم الوطني، إذا كان المجني عليه جزائريا الجنسية، وهذا تطبيقا لمبدأ

الشخصية في شقه الإيجابي، إذ يمكن للدولة بسط ولايتها القضائية في حالة أن ترتكب الجريمة على أحد رعاياها في الخارج.¹

بالإضافة للاختصاص الحصري للقطب الجزائي، يمارس كل من وكيل الجمهورية لدى القطب الجزائي الوطني، وكذا قاضي التحقيق ورئيس ذات القطب اختصاصا مشتركا مع الاختصاص الناتج عن تطبيق المواد 37 و40 و329 من هذا القانون بالنسبة للجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وهذا أشارت إليه المادة 211 مكرر 27 من قانون الإجراءات الجزائية، أي أنه يمارس اختصاصا مشتركا مع اختصاص الأقطاب الجزائية ذات الاختصاص الموسع، إذا ما تعلق الأمر بالجرائم الواردة في النصوص القانونية السابقة الذكر خاصة الجريمة المنظمة العابرة للحدود الوطنية إذا كانت ذات وصف جنحة، وكذا جرائم المخدرات والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، أما جرائم تبييض الأموال، وجرائم الفساد، جرائم الصرف وجرائم التهريب فيؤول الاختصاص للقطب الجزائي الإقتصادي والمالي بالاشتراك مع الأقطاب الجزائية ذات الاختصاص الموسع، كما يستثنى من هذا الاختصاص المشترك إذا كانت تحمل وصف جرائم إرهابية، فتكون من اختصاص محكمة مقر مجلس قضاء الجزائر خاصة المنصوص عليها في الفقرات 6 و9 و10 و12 و13 من المادة 87 مكرر من قانون العقوبات.²

ثالثا: الإجراءات المتبعة أمام القطب الجزائي الوطني

لم يتضمن القانون 11-21 المعدل لقانون الإجراءات الجزائية قواعد إجرائية خاصة، تتعلق بالقطب الجزائي الوطني، وإنما أخضعها للإجراءات التي تتبع على مستوى الأقطاب ذات الاختصاص الموسع، وكذلك الإجراءات المتبعة أمام محكمة مقر مجلس قضاء الجزائر.

1- التحقيق أمام وكيل الجمهورية

في إطار الاختصاص المشترك لوكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال المنصوص عليه حسب المادة 211 مكرر 27 من ق.إ.ج.ج، ومن

¹ شريفة سوماتي، القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال كآلية جديدة ضمن الجهاز القضائي المتخصص، مجلة الدراسات القانونية، المجلد 08، عدد 02، 2022، ص 500.

² - شريفة سوماتي، المرجع نفسه، ص، ص، 497-489.

الصلاحيات المخولة له، فبموجب المادة 211 مكرر¹6 من قانون الإجراءات الجزائية، يتولى وكلاء الجمهورية لدى الجهات القضائية المختصة إقليميا على سبيل السرعة وبكل الطرق إرسال نسخ التقارير الإخبارية وإجراءات التحقيق المنجزة من قبل الشرطة القضائية في إطار إحدى الجرائم المنصوص عليها في المواد 211 مكرر 24 و 211 مكرر 25 من ق.إ.ج.ج، إلى وكيل الجمهورية لدى القطب الجزائي الوطني، يمكن لوكيل الجمهورية لدى القطب الجزائي الوطني أن يطالب بملف القضية إذا رأى أن الجريمة تدخل ضمن إختصاصه، وهذا بعد أخذ رأي النائب العام لدى مجلس قضاء الجزائر وهذا طبقا لما جاء في نص المادة 211 مكرر 7 من ق.إ.ج.ج.

يمكن لوكيل الجمهورية لدى القطب الجزائي الوطني، أن يطالب بملف الإجراءات خلال كل مراحل الدعوى سواء على مستوى التحريات الأولية أو المتابعة أو التحقيق، وهذا ما خولته المادة 211 مكرر 8 من ق.إ.ج.ج، لكن يمكن خلال مرحلتي التحريات الأولية والمتابعة لوكيل الجمهورية المختص إقليميا، أن يصدر مقرر التخلي لصالح وكيل الجمهورية المختص لدى القطب الجزائي الوطني عند المطالبة بملف القضية وهذا احتوته المادة 211 مكرر 9 من ق.إ.ج.ج.

يؤول الإختصاص وجوبا لوكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، عندما يتزامن الإختصاص مع القطب الجزائي الاقتصادي والمالي.

2-التحقيق أمام قاضي التحقيق

في حالة فتح تحقيق قضائي تحال إلتماسات وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال،المتضمنة المطالبة بملف الإجراءات من قبل وكيل الجمهورية لدى القطب الجزائي الوطني، وعليه يصدر قاضي التحقيق أمرا بالتخلي لصالح قاضي التحقيق لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وهذا طبقا للمادة 211 مكرر 10 من ق.إ.ج.ج.

¹ - المادة 6/211 من القانون رقم 04-14 المعدل لقانون الإجراءات الجزائية.

في الأخير نقول لقد وفق المشرع الجزائري ونشمن جهوده في إستحداث هيئة قضائية مختصة في المتابعة والتحقيق في الجرائم الإلكترونية، وأسماها بالقطب الجزائري الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، إثر التعديل الذي مس قانون الإجراءات الجزائية بالأمر 11-21 المعدل والمتم، إذ تعتبر آلية فعالة لمواجهة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال والمرتبطة بها، وكذا الجرائم الأكثر تعقيدا، مما خول لها إختصاص حصري نظرا لخطورتها، وكذا تمتعها بإختصاص مشترك مع الجهات القضائية الأخرى كالأقطاب القضائية ذات الإختصاص الموسع، لكن ما يمكن ملاحظته أن هذا الأمر لم يتطرق إلى تشكيلة هذا القطب لا من حيث التعيين ولا من حيث التكوين، ولم يذكر الجهات التي يتم إستئناف الأحكام الصادرة عن القطب الجزائري، مما ندعو المشرع الجزائري إلى الإسراع في تنصيب هذا القطب لاستفحال ظاهرة الإجرام المعلوماتي في الجزائر.

المبحث الثاني: الإجراءات المستحدثة لمكافحة الجريمة الإلكترونية

بعد أن رأينا عدم فعالية وقصور الإجراءات التقليدية في مواجهة الجريمة الإلكترونية، دفع بالتشريعات الدولية إلى إعادة النظر في نصوصها الإجرائية بشكل يتناسب مع خصوصيات البحث والتحري في هذا النوع من الجرائم وتبني قواعد إجرائية تتلاءم وطبيعتها الخاصة و الخطيرة ، وهو نفس الإتجاه الذي سار عليه المشرع الجزائري، حيث أدخل جملة من التعديلات القانونية في هذا الإطار، من خلال سنه لإجراءات جديدة تتماشى والظاهرة الإجرامية الخطيرة والمستحدثة، وهذا بموجب الفصل الرابع من الباب الثاني من الكتاب بعنوان "في إعتراض المراسلات وتسجيل الأصوات والنقاط الصور" بموجب المواد من 65 مكرر 5 إلى 65 مكرر 10¹ من القانون رقم 22/06 المؤرخ في 20/12/2006 المعدل والمتمم لقانون الإجراءات الجزائية، وكذا إجراء التسرب من خلال المواد من 65 مكرر 11 الى 65 مكرر 18 من ق.ا.ج.ج سنتطرق إلى هذه الإجراءات كما يلي:

¹ - تطلق على هذه الأخيرة عند الفقه بأساليب التحري الخاصة، وتعرف بكونها تلك العمليات والإجراءات أو التقنيات التي تستخدمها الشرطة القضائية تحت مراقبة وإشراف السلطة القضائية، بغية البحث والتحري عن الجرائم الخطيرة المقررة في قانون العقوبات وجمع الأدلة عنها والكشف عن مرتكبيها، وذلك دون علم ورضا الأشخاص المعنيين، وقد انقسم الفقه بين معارض ومؤيد لاستعمال هذه الأساليب وللمزيد من الإطلاع أنظر: عبد الرحمان خلفي، الإجراءات الجزائية في التشريع الجزائري والمقارن، د.د، ط3، 2017، ص135.

المطلب الاول: إعتراض المراسلات وتسجيل الأصوات

استحدثت المشرع الجزائري وسائل تحري وتحقيق حديثة تتلاءم مع طبيعة هذه الجرائم، وذلك بموجب القانون رقم 22/06 المؤرخ في 2006/12/20 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون الإجراءات الجزائية، تتمثل في الإعتراض والتسجيل والإلتقاط والتسرب، هي عدة تسميات يمكن إختزالها في مصطلح واحد وهو "المراقبة" التي لا تخرج عن كونها رقابة مشروعة لشخص أو مكان أو أحاديث أو مراسلات مكتوبة أو مسموعة أو مرئية، نتيجة الإشتباه في تصرفات غير قانونية وذلك بصورة لا يحس معها الغير بمباشرتها لطابع السرية التي يكتنفها.¹

سوف نتناول من خلال هذا المطلب مفهوم إعتراض المراسلات وتسجيل الأصوات في (فرع أول) وشروطها في (فرع ثاني).

الفرع الأول: مفهوم إعتراض المراسلات وتسجيل الاصوات

نص المشرع الجزائري على هذا الإجراء بموجب المادة 65 مكرر 5 من ق.إ.ج.ج لهذا سوف نتطرق إلى تعريف إعتراض المراسلات في (الفقرة الأولى) ثم إلى تسجيل الأصوات في (الفقرة الثانية).

الفقرة الأولى: تعريف إعتراض المراسلات

لم يعرف المشرع الجزائري أسلوب إعتراض المراسلات السلوكية واللاسلكية شأنه في ذلك شأن التشريعات، ولكنه اكتفى بتنظيم هذا الإجراء من خلال نص المادة 65 مكرر 05 من ق.إ.ج.ج، فعرفه بأنه "إجراء تحقيقي يباشر خلصة وينتهك سرية الأحاديث الخاصة، تأمر به السلطة القضائية في الشكل المحدد قانونا بهدف الحصول على دليل غيرمادي للجريمة ويتضمن من ناحية أخرى إستراق السمع إلى الأحاديث"²، كما عرفت لجنة الخبراء الأوروبي بستراسبورغ المؤرخ في 2006/10/06 عملية إعتراض المراسلات بأنها "عملية مراقبة المراسلات السلوكية واللاسلكية وذلك في إطار البحث والتحري عن الجريمة

¹ - فوزي عمارة، إعتراض المراسلات وتسجيل الأصوات والنقاط الصور والتسرب كإجراءات تحقيق قضائي في المواد الجزائية، مجلة العلوم الإنسانية، عدد 33، 2010، ص 236.

² - أحمد غلاب، زهيرة كيسي، إجراءات إعتراض المكالمات السلوكية واللاسلكية كألية لمتابعة جرائم المخدرات، مجلة تحولات، المجلد 02، العدد 01، جانفي 2019، ص 266.

وجمع الأدلة والمعلومات حول الأشخاص المشتبه في ارتكاب أو مشاركتهم في ارتكاب جريمة¹، عرفه الاتحاد الدولي للاتصالات على أنها "تخص الحياة، المشاهدة، الالتقاط النسخ لمحتوى كل جزء من محتوى مراسلة وكذا للمعطيات المتعلقة بالمحتوى، معطيات الإعلام الآلي، معطيات متعلقة بالحركة و/أو الإصدارات الإلكترونية لهذه المعطيات التي تتم بوسائل سلكية واللاسلكية، رقمية، بصرية، شفوية، أو وسائل أخرى، أثناء نقلها باستعمال نظام إلكتروني آلي بصري، نظام للذبذبات، الإلكتروميكانيكي، أو أي نوع آخر من الأنظمة.²

والملاحظ أن المشرع حدد نوع المراسلات التي تصلح أن تكون محلا للإعتراض وهي التي تتم بواسطة وسائل الإتصال السلكية واللاسلكية، دون أن يشير إلى طبيعة هذه المراسلات، مما يفتح المجال لمختلف الرسائل المكتوبة، بغض النظر عن شكلها (كتابة، رموز، أشكال، صور) أو الدعامة التي تنصب عليها (ورقية أو غير ورقية) أو الوسيلة المستعملة لإرسالها سلكية كانت (فاكس، تليفون) أو لاسلكية (البريد الإلكتروني، الهاتف النقال).³

وهذا ما أكدته المادة 10 من القانون 18-04⁴ المتعلق بالقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية والتي عرفت الإتصالات الإلكترونية بأنها " كل إرسال أو تراسل أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو بيانات أو معلومات مهما كانت طبيعتها عبر الأسلاك أو الألياف البصرية أو بطريقة كهرومغناطيسية" وهو نفس التعريف الوارد في المادة 2 فقرة " و" من القانون 04/09 المتعلقة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، وقد استثنى المشرع الرسائل والخطابات والطرود لدى مكاتب البريد، كما أنه لم يولى إهتمامه لأداة الاعتراض فقد تكون

¹ - الدوايدي مجراب، الأساليب الخاصة للبحث والتحري في الجريمة المنظمة، أطروحة لنيل شهادة دكتوراه علوم، كلية الحقوق، جامعة الجزائر 01، الجزائر، 2016، ص209.

² - « l'interception désigne l'acquisition, la visualisation, la capture ou la copie du contenu ou d'une partie du contenu d'une données relatives au trafic, et/ ou les émissions électroniques de ces données, par des moyens avec transmission grâce à l'utilisation d'un dispositif électronique, mécanique, optique, à ondes électromécanique, ou un autre de dispositif » voir Philippe Guillot et Daniel ventre, capacités d'interception et surveillance, projet utic, université paris 8, Vincennes saint Denis, paris, France, 2017, p12.

³ - جمال إبراهيمي، المرجع السابق، ص89.

⁴ - القانون رقم 18-04 المؤرخ في 10 ماي 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، الجريدة الرسمية للجمهورية الجزائرية عدد 27، الصادرة بتاريخ 13 ماي 2018.

تقليدية أو بأحدث الوسائل التكنولوجية المتوفرة.¹

و الملاحظ كذلك أن المراسلات التي تصلح أن تكون محلا لإجراء الاعتراض يجب أن تتسم بالخصوصية والسرية، فهي مكفولة بالحماية دستوريا وفي قوانين تشريعية²، إلا أن هذه الحماية غير مطلقة، فإذا إقتضت ضرورة البحث والتحري والتحقيق في الجرائم الإلكترونية، فيجوز إعتراض هذه المراسلات وكشف سريتها بواسطة ترتيبات تقنية يتم وضعها مسبقا دون موافقة المعنيين من أجل البحث عن دليل لإدانة المتهم، ويعتبر المبرر الشرعي لإباحة هذا الإجراء بسبب أنه يتضمن اعتداء ومساس بحرمة الحياة الخاصة للأفراد وسرية الاتصالات.³

ومن جهة أخرى اعتبر جانب من الفقه أن إعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية يقصد بها أساس التنصت التليفوني،⁴ والملاحظ وبالرجوع للمادة 65 مكرر 5 أن المشرع الجزائري لم يعط تعريفا محددا لإعتراض المراسلات وقد أحسن في ذلك، وترك المجال مفتوحا لإحتواء أي تطور تكنولوجي في مجال وسائل الإتصال.

و تساهم وسائل الإتصال الحديثة في تسهيل إرتكاب العديد من الجرائم الخطيرة سواء عن طريق المكالمات الهاتفية أو المراسلات الإلكترونية المتبادلة عن طريق الشبكات الإلكترونية، حيث أجازت المادة 03 من إتفاقية بودابست الاعتراض الشرعي لكافة أشكال النقل الإلكتروني للبيانات سواء تم عبر التليفون أو الفاكس أو البريد الإلكتروني، وتشمل الاتصالات محل الاعتراض المحتوى غير المشروع أو الدليل على الأفعال الإجرامية الخطيرة المنصوص عليها في القانون الداخلي لكل دولة طرف في الاتفاقية، مما يستوجب ضرورة اعتراض المراسلات الإلكترونية المتبادلة عبر الحاسب الآلي لدرء خطر الجريمة

¹ - فوزي عمارة، المرجع السابق، ص 237.

² - تنص المادة 46 من التعديل الدستوري المؤرخ في 2016/03/06 على " لا يجوز انتهاك حرمة حياة المواطن الخاصة وحرمة شرفه ويحميها القانون، سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة، لا يجوز باي شكل المساس بهذه الحقوق دون امر معال من السلطة القضائية ويعاقب القانون على انتهاك هذا الحكم .." كذلك المادة 164 من قانون 04/18 المتعلق بالقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، كذلك نص المادتين 42-43 من القانون 15-04 المؤرخ في 2015/02/01 المتعلق بالقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، كذلك المادتين 303 و303 مكرر من قانون العقوبات الجزائري.

³ - نعيم سعيداني، المرجع السابق، ص 179.

⁴ - أحسن بوسقيعة، التحقيق القضائي، دار هومة، الجزائر، د ط، 2008، ص 113.

وملاحقة الجناة، وهذا ربما ما قصده المشرع الجزائري من خلال أحكام إعتراض المراسلات السلكية واللاسلكية، وهذا ما إتجه إليه كذلك المشرع من خلال أحكام القانون 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها¹، حيث نصت المادة 03 من القانون 04/09 على "....وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام أيضا بإجراءات التفتيش والحجز داخل منظومة معلوماتية.²

الفقرة الثانية: تسجيل الأصوات

ثاني إجراء من الإجراءات الخاصة التي سنها المشرع، إجراء التسجيل الصوتي الذي يتم اللجوء إليه للبحث والتحري عن الجرائم المحددة حصرا.

ويقصد بتسجيل الأصوات، تسجيل أحاديث المتهم وشركائه عن واقعة معينة من الوقائع المنصوص عليها في المادة 65 مكرر من ق.ا.ج.ج. خلسة³، كما يقصد بها " المحادثات الشفوية التي يتحدث بها الأشخاص بصفة سرية أو خاصة في مكان خاص أو عام ويتم ذلك عن طريق حفظ الحديث على جهاز معد لذلك، للاستماع إليه مرة أخرى."⁴، ولم ينص المشرع الجزائري في قانون الإجراءات الجزائية على تعريف التسجيل الصوتي، وإنما أشار لها في نص المادة 65 مكرر 5 فقرة 2 بقوله "وضع الترتيبات التقنية دون موافقة المعنيين من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة، أو سرية من طرف شخص أو عدة أشخاص، في أماكن خاصة أو عمومية."

إذا فالتسجيل الصوتي لا يقتصر على تسجيل الكلام المتفوه به فحسب، وإنما يشمل كذلك الإلتقاط وتثبيت وبث الكلام، فتسجيل الكلام أو الحديث فهو حفظه على جهاز أو أي وسيلة أخرى معدة لذلك، قصد الاستماع إليه فيما بعد ذلك⁵، أما الإلتقاط هو " الإستماع للحديث خلسة أو سرا بأي وسيلة كانت

¹ - جميلة محلق، إعتراض المراسلات، تسجيل الاصوات والتقاط الصور في قانون الإجراءات الجزائية الجزائري، مجلة التواصل في الإقتصاد والإدارة والقانون، عدد 42، جوان 2015، ص178.

² - أنظر المواد من 05 الى 09 من القانون 04/09 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها.

³ - فوزي عمارة، المرجع السابق، ص237.

⁴ - جميلة محلق، المرجع السابق، ص178.

⁵ - عبد الرحمان خلفي، الحق في الحياة الخاصة في التشريع العقابي الجزائري، المرجع السابق، ص172.

بشرط أن يتسم بطابع السرية والخصوصية"، وهذا ما يدل أن المشرع أخذ بالمعيار الموضوعي فأجاز التسجيل الصوتي للأحاديث بصفة خاصة أو سرية في أماكن خاصة أو عامة، حيث تعد طبيعة الحديث أساس الحماية الجنائية.¹

فبفضل التطور التكنولوجي لوسائل الاتصالات، لم يعد التسجيل الصوتي عملا صعبا، فقد يتم على مسافات بعيدة دون الحاجة إلى البقاء قريبا من المكان المراد التسجيل منه، ومثال ذلك تقنية التجسس على الهاتف النقال التي يطلق عليها تسمية السن الأزرق² (Blue Tooth) حيث تسمح بالنقاط التسجيلات والمحادثات المارة من وإلى الهاتف النقال التابع للغير داخل مسافة معينة.³

و يمكن القول أن للتسجيلات الصوتية حجية كبيرة في الإثبات، ومنه قناعة القاضي بها كدليل في الإثبات، مع ملاحظة أن الصوت عند تسجيله إلكترونيا فإنه لا يحتمل الخطأ، ويستعصي على إمكانية التلاعب فيه، ويمكن للخبراء أن يكتشفوا أي تلاعب أو خداع بوسائل تقنية عالية الكفاءة، ومن ثم يمكن القول أن التسجيل الصوتي الممغنط يمكن أن تكون له قيمة دامغة في الإثبات.⁴

الفرع الثاني: شروط وضوابط تنفيذ إجراء اعتراض المراسلات وتسجيل الأصوات

حدد قانون الإجراءات الجزائية الضوابط التي ترد على الجهات المخول لها إجراء اعتراض المراسلات وتسجيل الأصوات، من خلال تضمنه عدة شروط يجب توافرها، لذا سوف نتعرض للشروط المطلوبة لشرعية إجراء تلك الإجراءات التي تمس الحياة الخاصة للأشخاص وبدون موافقتهم وتتمثل في:

¹ - جميلة مخلوق، المرجع السابق، ص 179.

² - بعد انتشار الهاتف النقال سنة 1990، كان الاعتقاد السائد أنه لا يمكن مراقبة هذا الأخير بالتتصت عليه، حيث قامت شركة المالية تدعى international Mobile scbscr فطورت نظاما أعطت له اسما Schwarz identité فمن خلاله يمكن إصطياد جميع الإشارات الصادرة من هاته الهواتف وقلبها إلى كلمات مسموعة، كما قامت الشركة بمعرفة مكان المتحدثين، كما طورت جهاز إلكتروني عن طريق استخدام الميكروفون الموجود في الهاتف النقال لكي ينقل جميع الأصوات، انظر خضرة شنتير، الآليات القانونية لمكافحة الجريمة الإلكترونية، أطروحة لنيل شهادة الدكتوراه الطور الثالث (ل.م.د)، كلية الحقوق والعلوم السياسية، جامعة احمد دراية، ادرار، الجزائر، 2021، ص 129.

³ - خضرة شنتير، المرجع نفسه، ص 129.

⁴ عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، ص 781.

الفقرة الأولى: الشروط الموضوعية

لتنفيذ إجراء اعتراض المراسلات السلكية واللاسلكية وتسجيل الأصوات، لابد من احترام الضوابط الموضوعية والتي تتمثل فيما يلي:

أولا: السلطة المختصة بإجراء هذه العملية

حدد المشرع الجزائري السلطات المختصة بإصدار الإذن باعتراض المراسلات السلكية واللاسلكية وتسجيل الأصوات، لقاضي التحقيق في حالة فتح تحقيق قضائي وتحت رقابته المباشرة وهذا بموجب المادة 65 مكرر 5 فقرة 6 و7 من ق.ا.ج.ج، وبناء على ذلك يحظر على ضابط الشرطة القضائية اعتراض المراسلات السلكية واللاسلكية وتسجيل الأصوات إلا بعد انتدابه لمباشرة هذا الإجراء من قبل قاضي التحقيق أو وكيل الجمهورية¹ بحسب الأحوال، فإذا قام ضابط الشرطة القضائية بالتنصت على المحادثات الهاتفية أو تسجيلها دون إذن بذلك فإن الدليل المستمد من المراقبة يعد باطلا.

ثانيا: طبيعة الجريمة

حصر المشرع الجزائري إجراءات اعتراض المراسلات وتسجيل الأصوات في حالة التلبس أو بمناسبة التحقيق الابتدائي في جرائم حددها على سبيل الحصر، وهي جرائم المخدرات، والجريمة المنظمة العابرة للحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وجرائم تبييض الأموال وجرائم الإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد، وفي حالة إكتشاف جرائم أخرى أثناء القيام بإجراءات التحري الخاصة فإن ذلك لا يكون سببا في بطلان الإجراءات العارضة²، وإنما يخطر بها وكيل الجمهورية ليتخذ ما يراه مناسبا بشأنها، إن تحديد المشرع لجرائم معينة يحد من حرية السلطة القضائية في اللجوء إلى أساليب التحري الخاصة بسبب صعوبة وصف الجريمة وتكييفها قبل إكمال إجراءات التحقيق، مما يؤدي إلى إفلات الكثير من العقاب في جرائم تكون خطيرة، بعكس المشرع الفرنسي فكرس هذه الضمانة في المادة 100 من ق.ا.ج.ج ف فأجاز اعتراض المراسلات وتسجيل المكالمات الهاتفية في

¹ - غير إنه إستثناء لهذه القاعدة عندما يتعلق الأمر بالوقاية من الأفعال الإرهابية أو التخريب أو الجرائم الماسة بأمن الدولة، يكون النائب العام لدى مجلس قضاء الجزائر هو المختص بمنح الإذن لإجراء المراقبة أنظر المادة 4 فقرة 6 و7 من ق.ا.ج.ج المؤرخ في 05 أوت 2009.

² - تنص المادة 65 مكرر 6 من ق.ا.ج.ج على " إذا إكتشفت جرائم أخرى غير تلك التي ورد ذكرها في إذن القاضي، فإن ذلك لا يكون سببا في بطلان الإجراءات العارضة."

الجنايات أو الجناح المعاقب عليها بعقوبة تساوي أو تزيد على الحبس لمدة سنتين، ووضع معيارا يحدد جسامه الجريمة وأساس العقوبة المقرر لها.¹

ثالثا: فائدة الإعتراض في إظهار الحقيقة

تقرر التشريعات المعاصرة أن ضابط فائدة المراقبة في ظهور الحقيقة، يعتبر السند الشرعي المبرر للاعتراض، ذلك بسبب أن هذا الإجراء يتضمن أعتداءا جسيما على حرمة الحياة الخاصة وسرية الإتصالات، فيباح إستثناء، وفي حدود ضيقة وذلك للفائدة المنتظرة منه والتي تتعلق بإظهار الحقيقة بكشف غموض الجريمة وضبط الحياة.²

رابعا: ميقات ومكان إجراء هذه العمليات

لم يضع قانون الإجراءات الجزائية قيودا زمنية ولا مكانية لإجراء عملية اعتراض المراسلات وتسجيل الأصوات، حيث أجاز إجرائها في كل ساعة من ساعات الليل والنهار وفي مكان عام أو خاص، ولكن إشتراط المشرع صراحة أن تنفذ عملية الإعتراض في سرية تامة، ودون علم أو رضا المشتبه فيه أو صاحب الأماكن، مع مراعاة عدم المساس بالسري المهني³ المقرر بنص المادة 45 من ق.ا.ج.ج.

الفقرة الثانية: الشروط الشكلية لإجراءات إعتراض المراسلات وتسجيل الأصوات

إلى جانب الشروط الموضوعية، هناك شروط شكلية يجب الإلتزام بها لإجراء هذه العملية وتتمثل فيما يلي:

أولا: الإذن

قبل الحصول على الإذن للجوء لمباشرة هذه الاجراءات، لابد أن يكون مصدره مختصا نوعيا وإقليميا في البحث والتحري في الجرائم الإلكترونية، وفقا ما يحدده الإختصاص النوعي أي نوع الجريمة والإختصاص الإقليمي والمتعلق بالضوابط الثلاث أي محل وقوع الجريمة أو القبض على المتهم أو محل إقامته.

¹ - Art 100.C.P.P.F. « .en matière criminelle ou correctionnelle, si la peine encourue est égale ou supérieure à deux ans d'emprisonnement , le juge d'instruction peut , lorsque les nécessités et la transcription de correspondances émises par la voie des télécommunications.. ».

² - محمد أبو العلا عقيدة، مراقبة المحادثات التلفونية -دراسة مقارنة-، دار النهضة العربية، القاهرة، ط2، 2008، ص192.

³ - فوزي عمارة، المرجع السابق، ص299.

يلزم المشرع الجزائري بموجب المادة 65 مكرر 5 من ق.ا.ج.ج، ضرورة الحصول على إذن قضائي من وكيل الجمهورية أو قاضي التحقيق في حالة فتح تحقيق قضائي، فلا يمكن لضباط الشرطة القضائية اللجوء إلى هذا الإجراء إلا بعد حصولهم على هذا الإذن ويجب أن يتضمن البيانات التالية:

- أن يتضمن كل العناصر التي تسمح بالتعرف على الأماكن المطلوب التقاط الصور فيها، أو تسجيل الأحاديث السكنية أو غيرها.

- ذكر طبيعة الجريمة التي تبرر إجراء الاعتراض .

- تحديد المدة الزمنية في الإذن والتي لا يمكن أن تتجاوز 4 أشهر قابلة للتجديد حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية وهذا طبق المادة 65 مكرر 7 من ق.ا.ج.ج.¹

- وأن يكون مكتوبا تحت طائلة البطلان، ذلك أن الأصل في العمل الإجرائي الكتابة .

وما يمكن ملاحظته أن المادة 65 مكرر 7 من ق.ا.ج.ج أنها لم تحدد عدد مرات قابلية الإذن إلى التجديد، كما لم ينص كذلك صراحة ما إن كان يجوز للسلطة المختصة المانحة للإذن للقيام بهذا الإجراء، توقيفها قبل الموعد المحدد في الإذن²، كما لم يول المشرع أهمية لشرط التسبب كما فعله بالنسبة لإجراء التسرب، فعلى المشرع تدارك ذلك بالنص عليه صراحة وذلك بذكر الأسباب الدافعة إلى اتخاذ مثل هذه العمليات، فذكر نوع الجريمة لا يعد تسببا، كما لم يتطرق المشرع إلى مسألة ضرورة إيداع نسخة من الإذن في ملف الإجراءات.³

ثانيا: كيفية إجراء عملية الاعتراض

يقوم أعوان مصالح الاتصالات السلكية واللاسلكية سواء العمومية أو الخاصة، بالجانب التقني للعملية وهذا بتسخير من السلطة القضائية المختصة، وذلك طبقا للمادة 65 مكرر 8 من ق.ا.ج.ج، مع إلزام ضباط الشرطة القضائية المأذون له أو المناب من طرف قاضي التحقيق المختص بتحرير محضر

¹ - تنص المادة 65 مكرر 2/7 من ق.ا.ج.ج على "...يسلم الاذن مكتوبا لمدة أربعة (4) أشهر قابلة للتجديد حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية."

² - فوزي عمار، المرجع السابق، ص 241.

³ - سامية آيت مولود، الضمانات المقررة المشروعية إعتراض المراسلات وتسجيل الأصوات والتقاط الصور في الجرائم الإقتصادية، المجلة النقدية، المجلد 10، العدد 2، 2015، ص 351.

عن كل عملية اعتراض وتسجيل المراسلات، وكذلك عن عمليات وضع الترتيبات التقنية وعمليات الالتقاط، وأن يحدد في المحضر تاريخ وساعة وبداية هذه العمليات وتاريخ الإنتهاء منها، كما يمكن ترجمة المراسلات التي تتم باللغات الأجنبية، ويودع هذا المحضر بالملف وفقا لما نصت عليه المادتين 95 مكرر 9 و65 مكرر 10 من ق.ا.ج.ج.¹

كما ينبغي الإشارة إليه أن المشرع الجزائري لم يشير صراحة إلى كيفية وضع الأدلة المحصل عليها من عملية الاعتراض سواء كانت تسجيلات سمعية بصرية، البيانات الرقمية في إحرار مختومة، وهذا ما يطرح التساؤل حول مدى إعتبارها من قبيل الأشياء المضبوطة والتي يجب أن تخضع لأحكام المادة 84 من ق.ا.ج.ج. والمادة 45 من نفس القانون.²

علما أن هذه التسجيلات والبيانات تعتبر أدلة إثبات رقمية، مما يقتضي وضعها في أحرار مختومة تضمن عدم التلاعب والعبث بها بالحذف أو الإضافة، وضمها إلى ملف الإجراءات مع المحاضر التي تصف أو تنسخ محتواها للكشف عن الحقيقة.

المطلب الثاني: إلتقاط الصور

لم يكتف المشرع بالسماح بتسجيل الأصوات فحسب، بل أجاز إمكانية إلتقاط الصور لشخص أو عدة أشخاص في مكان خاص، بإعتباره أحد وسائل البحث والتحري الحديثة، وهي إستثناء عن المبدأ العام الذي يمنع إلتقاط الصور خلسة دون رضا صاحبها بإعتباره تدخل في مجال الحياة الخاصة فلا يجوز السماح بإلتقاط الصور أو نشرها إلا بعد موافقة صاحبها. سنتناول مفهوم إلتقاط الصور في (الفرع الأول) ثم نبين إجراءاته في (الفرع الثاني).

¹ - تنص المادة 65 مكرر 9 من ق.ا.ج.ج. على "يحدد ضابط الشرطة القضائية المأذون له أو المناب من طرف القاضي المختص محضرا عن كل عملية اعتراض تسجيل المراسلات وكذا عن عمليات وضع الترتيبات التقنية وعمليات الإلتقاط والتنثبت والتسجيل الصوتي أو السمعي البصري.

يذكر بالمحضر تاريخ وساعة بداية هذه العمليات والانتهاؤها منها."

أما المادة 65 مكرر 10 من ق.ا.ج.ج. تنص على أنه " يصف أو ينسخ ضابط الشرطة القضائية المأذون لو أو المناب المراسلات أو الصور أو المحادثات المسجلة المفيدة في إظهار الحقيقة محضر يودع بالملف.

تنسخ وترجم المكالمات التي تتم باللغات الأجنبية عند الاقتضاء، بمساعدة مترجم يسخر لهذا الغرض.

² - تنص المادة 5/45 من ق.ا.ج.ج. على " تغلق الأشياء والمستندات المحجوزة ويختتم عليها إذا امكن ذلك فإذا تعذرت الكتابة عليها فانها توضع في وعاء أو كيس يضع عليه ضابط الشرطة القضائية شريطا من الورق ويختتم عليه بختمه ."

أما المادة 84 من ق.ا.ج.ج. تنص على "...ويجب على الفور إحصاء الأشياء والوثائق المضبوطة ووضعها في إحرار مختومة ..."

الفرع الأول: مفهوم التقاط الصور

وهو أسلوب جديد للبحث والتحري استحدثه المشرع الجزائري بموجب أحكام المادة 65 مكرر 5 من ق.ا.ج.ج، ويقصد به وضع أجهزة التصوير المختلفة في أمكنة خاصة ودون موافقة المعنيين، من أجل التقاط صور لشخص أو عدة أشخاص تفيد في إجلاء الحقيقة وتسجيلها¹، لم يتطرق المشرع إلى تعريف هذا الإجراء، وإنما نص على مجال تطبيقه وتوضيح إجراءات القيام به، وبالرجوع إلى نص المادة 65 مكرر 5 من ق.ا.ج.ج التي نصت على "...وضع الترتيبات التقنية، دون موافقة المعنيين من أجل التقاط وتثبيت وبت وتسجيل الكلام المنقوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية أو النقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص..." إذا فالصور المعنية بهذا النص هي تلك الملتقطة في المكان الخاص، والتي أقر حمايتها بموجب المادة 303 من ق.ع.ج.

كما أن عبارة وضع الترتيبات التقنية تفيد استخدام كل أنواع أجهزة التصوير، ووسائل المراقبة المختلفة المرتبطة بالتطور التقني كالفديو، والآلات التصوير المتطورة وتسجيل الأصوات والهواتف النقالة الذكية، وإرسالها إلى جهات محددة على مسافات بعيدة، إلى جانب الآلات الدقيقة التي يتم تثبيتها في الأماكن الخاصة والنقاط الصورة بدقة متناهية لكل ما هو موجود بها، بتقنية إشارات إلكترونية من الخارج، والكاميرات المزودة بعدسات صغيرة الحجم التي يمكن وضعها في الملابس أو في أماكن ثابتة أو متحركة يصعب إكتشافها بالعين المجردة، وبفضل إستغلال هذه الآلات الرقمية الحديثة والمتطورة للتصوير أصبحت التحقيقات التي تقوم بها الشرطة القضائية تبرز وقائع الجريمة بصفة فعلية وحقيقية، يمكن من خلالها التعرف على الفاعلين الحقيقيين دون شك في صحتها، بشرط أن لا يستغل هذا الأسلوب في الإطار غير الشرعي الذي لا يسمح به القانون.²

ولابد من الإشارة كذلك أن المشرع الجزائري، لم ينص على شروط خاصة تتعلق بعملية التقاط الصور، وهذا يفسر إرتباط عملية التقاط الصور بالأحكام الخاصة بإعتراض المراسلات وتسجيل الأصوات، ويستشف ذلك من خلال النص الذي أورده المشرع الجزائري في الفصل الرابع بعنوان إعتراض

¹ - نجية شيخ، أساليب البحث والتحري المستحدثة في القانون رقم 22/06 المعدل والمتمم لقانون الإجراءات الجزائية الجزائرية، المجلة النقدية، المجلد 8، العدد 01، ص 294.

² - دوادي مجراب، المرجع السابق، ص 216.

المراسلات وتسجيل الأصوات والتقاط الصور .

الفرع الثاني: إجراءات التقاط الصور

تتمثل هذه الشروط فيما يلي:

أولاً: أن تطبق على الجرائم المحددة حصر

إن عملية التقاط الصور يمكن تطبيقها على الجرائم الواردة في المادة 65 مكرر 05 من قانون إجراءات جزائية والتي تتمثل في جرائم المخدرات، الجريمة المنظمة العابرة للحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، جرائم تبيض الأموال، جرائم الإرهاب، الجرائم بالتشريع الخاص بالصرف، جرائم الفساد.

ثانياً: الجهة القضائية المختصة بمنح الإذن بعملية التقاط الصور

-وكيل الجمهورية في الجرائم المتلبس بها أو التحقيق الابتدائي المادة 65 مكرر 5.

-قاضي التحقيق في حالة فتح تحقيق قضائي، وتتم العمليات تحت رقابته المباشرة المادة 65 مكرر

05 فقرة الأخيرة.

ثالثاً: الحصول على الإذن بعملية التقاط الصور

لا يشرع بعملية التقاط الصور إلا بالحصول على إذن مكتوب من وكيل الجمهورية أو قاضي التحقيق، حيث يتضمن هذا الإذن على كل العناصر التي تسمح بالتعرف على أشخاص المراد التقاط الصور لهم وكذا الجريمة التي تبرر اللجوء إلى هذه التدابير ومدتها، حيث تنص المادة 65 مكرر 7 على "...يسلم الإذن مكتوباً بالمدة أقصاها أربعة (4) أشهر قابلة للتجديد حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية"، كما تتم أماكن التقاط الصور في الأماكن الخاصة بعكس إجراء تسجيل الأصوات الذي يتم في أماكن عمومية وخاصة، غير أن المشرع الجزائري سمح بهذا التدبير في بعض القوانين الخاصة كالترصد الإلكتروني والإختراق بموجب المادة 56¹ من القانون 06-01 المتعلق

¹ - تنص المادة 56 من قانون رقم 06-01 على أنه " من أجل تسهيل جمع الأدلة المتعلقة بالجرائم المنصوص عليها في هذا القانون، يمكن اللجوء إلى التسليم المراقب أو اتباع أساليب تحري خاصة كالترصد الإلكتروني والاختراق، على النحو المناسب وبإذن من السلطة القضائية المختصة."

بالوقاية من الفساد ومكافحته.¹

رابعاً: أن تنفذ من عون مؤهل لذلك

خول القانون لضابط الشرطة القضائية بإنجاز العمليات، ويجوز لقاضي التحقيق أو لضابط الشرطة القضائية الذي ينييه، أن يسخر كل عون مؤهل للتكفل بالجوانب التقنية للعملية، سواء كان العون المؤهل يعمل لدى هيئة عمومية أو خاصة، وذلك طبقاً للمادة 65 مكرر 8 من قانون إجراءات جزائية، وبمجرد إنتهاء ضابط الشرطة القضائية من العملية المكلف بها يحضر محضراً عنها، يتضمن محتوى مجريات العملية التي قام بها من البداية إلى النهاية، ويرسله إلى قاضي التحقيق وهذا بموجب المادتين 9 و10 مكرر من ق.ا.ج.ج.²

بعد دراسة عملية الاعتراض وتسجيل الأصوات والنقاط الصور وإعتبارها، من الأساليب الخاصة التي أثبتت نجاعتها في مكافحة الجريمة الإلكترونية، إلا أن هناك إشكالات قانونية وأخرى عملية والتي تتمثل في:³

1-الإشكالات القانونية

إن النصوص القانونية لم تبين الوسائل القانونية التي يمكن إستعمالها الوسائل التقنية والتكنولوجية للقيام بهذه العملية، كذلك لا يوجد نصوص تحدد نوع المؤسسات المسخرة وكذلك المصاريف والأتعاب.

2-الإشكالات العملية

مدى توافر وسائل اعتراض المراسلات وتثبيتها وهي عادة ما تكون وسائل تقنية ذات تكلفة عالية عدم تحديد الجهة التي تتكفل بالمصاريف.

وإن المراسلات أو الأصوات المثبتة على دعامات إلكترونية أو مغناطيسية معرضة لإمكانات التلاعب بها دون ترك أثر وهي كذلك سهلة الإتلاف لا بد من إيجاد احتياطات خاصة لتخزينها.

¹ - القانون رقم 01/06 المؤرخ في 20/02/2006 المتعلق بالوقاية من الفساد ومكافحته، الجريدة الرسمية عدد 14، الصادرة بتاريخ 08/03/2006.

² - نجبة شيخ، المرجع السابق، ص 297.

³ - عبد المجيد جباري، المرجع السابق، ص، ص 67- 68.

المطلب الثالث: التسرب الإلكتروني

من بين الأساليب التي أرساها المشرع ضمن خطته لمكافحة الجرائم الخطيرة ومنها الجريمة الإلكترونية، استحدثت نصوص قانونية جديدة تتضمن إجراءات خاصة ضمنها القانون رقم 22/06 المؤرخ في 2006/12/20 المتعلق بقانون الإجراءات الجزائية المعدل والمتمم، حيث نص في الفصل الخامس منه تحت عنوان "في التسرب" والذي يعتبر أسلوبا جديدا وخصوصا للبحث والتحري، وقد تم تنظيم هذا الإجراء ضمن المواد من 65 مكرر 11 إلى 65 مكرر 18 سنحاول التطرق إلى مفهوم التسرب (الفرع الأول) وشروطه (الفرع الثاني) وآثاره (الفرع الثالث).

الفرع الأول: مفهوم التسرب

يقصد بالتسرب حسب نص المادة 65 مكرر 12 من ق.ا.ج.ج "قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك أو خاف".¹، ويعرف عمليا بأنه "التسلل عن طريق التوغل داخل مكان أو هدف أو تنظيم يصعب الدخول إليه فيما يسمى بالمكان المغلق لكشف نوايا الجماعات الإجرامية".²

و يلاحظ من خلال التعريفين السابقين، أن عملية التسرب تقتضي التواجد في الوسط الإجرامي موضوع عملية التحقيق والإحتكاك المباشر مع المشتبه فيهم عن طريق التكر والخداع، وكسب ثقة المشتبه فيهم من أجل الحصول على المعلومات، وتحديد نقاط قوة وضعف هذه الجماعة وإكتشاف أعضائها ووسائل التواصل بينهم،³ وأن يرتكب عند الضرورة أفعالا غير مشروعة للوصول إلى الغاية أو الهدف المرجو من عملية التسرب.

وقد حصر المشرع الجزائري اللجوء إلى عملية التسرب في جرائم محددة تتميز بخطورتها وتأثيرها

¹ - وهذا التعريف جاء مطابقا للتعريف الفرنسي المنصوص عليه في المادة 81/706-2 من ق.ا.ج.ف والتي جاء نصها: Art 706/81 du c.p.p.f <l'infiltration consiste, pour un officier ou un agent de police judiciaire habilité dans des conditions fixées par décret et agissant sous la responsabilité d'un officier de judiciaire chargé de coordonner l'opération à surveiller des personnes suspectées de commettre un crime, ou un délit en se faisant passer auprès de ces personnes comme un de leurs coauteurs, complices ou receleurs.>

² - يوسف شويرف، التسرب كأسلوب للتحري والتحقيق الإثبات، مجلة المستقبل، مدرسة الشرطة سيدي بلعباس، عدد 1، جويلية 2007، ص 20.

³ - خضرة شنتير، المرجع السابق، ص 133 .

السلبى على الإستقرار الأمني والإقتصادي، إضافة إلى أن التحقيق في مثل هذه الجرائم بإستعمال الأساليب التقليدية صعب جدا، خاصة وأن أغلب هذه الجرائم ترتكب في إطار شبكات إجرامية، إضافة للطابع الخفي والتقني المتغير لهذه الجرائم.¹

ويمكن تجسيد عملية التسرب في الجريمة الإلكترونية، من خلال إشتراك ضابط الشرطة القضائية في محادثات غرف الدردشة أو حلقات النقاش حول دعاة الأطفال، أو كلام يدور حول قيام أحدهم بإختراق شبكات أو بث فيروسات، ويستعمل المتسرب أسماء وصفات مستعارة ووهمية ظاهرا فيها بمظهر طبيعي بإعتباره فاعلا مثلهم حتى يتمكن من التعرف عليهم وضبطهم متلبسين.²

الفرع الثاني: الأحكام الضابطة لعملية التسرب

أحاط المشرع الجزائري عملية التسرب بجملة من الضوابط والشروط يجب مراعاتها ضمانا لمشروعية الدليل المتحصل عليه من خلالها، ويتجلى ذلك من خلال المادة 65 مكرر 11 من ق.ا.ج.ج أن يكون اللجوء إلى عملية التسرب عندما تقتضي ضرورات التحري أو التحقيق في إحدى الجرائم المذكورة اللجوء إليها، وعلى إعتبار الجريمة الإلكترونية، إحدى هذه الجرائم التي جاءت في نص المادة السالفة الذكر، ويمكن إيجازها في نوعين من الشروط هي:

الفقرة الأولى الشروط الشكلية

وضع المشرع الجزائري مجموعة من الشروط الشكلية يجب أن تتوافر في عملية التسرب وتتمثل فيما يلي:

أولا: تحرير تقرير مسبق من طرف ضباط الشرطة القضائية

يقوم ضابط الشرطة القضائية قبل مباشرة عملية التسرب، بكتابة تقرير مفصل عن عملية التسرب، وإرساله إلى وكيل الجمهورية كإجراء أولي قبل مباشرة هذه العملية.³

¹ - أمينة معزیز، التسرب في قانون الإجراءات الجزائية الجزائري، مجلة القانون والمجتمع، المجلد 3، العدد 1، ص 251.

² - عائشة بن قارة مصطفى، المرجع السابق، ص 40.

³ - تنص المادة 65 مكرر 13 ا.ج.ج على " يحرر ضابط الشرطة القضائية المكلف بتنسيق عملية التسرب تقريرا يتضمن العناصر الضرورية لمعاينة الجرائم غير تلك التي تعرض للخطر أمن الضابط او العون المتسرب، وكذا الأشخاص المسخرين طبقا للمادة 65 مكرر 14 أدناه."

وعليه يجب على الضابط المنسق أن يجمع أكبر قدر ممكن من المعلومات حول القضية محل التحري، وكذا جدوى إجراء عملية التسرب، حتى يتسنى لوكيل الجمهورية أو قاضي التحقيق أن يأمر بإجرائها آخذا بعين الاعتبار العناصر الضرورية لمعينة الجرائم، وما إذا كانت تشكل خطرا على أمن الضابط أو العون المتسرب أو الأشخاص المسخرين.¹

ثانيا: صدور الإذن القضائي بمباشرة العملية

نصت المادة 65 مكرر 11 من ق.ا.ج.ج أنه " عندما تقتضي ضرورة التحري والتحقيق في إحدى الجرائم المذكورة في المادة 65 مكرر 5 أعلاه يجوز لوكيل الجمهورية، أو قاضي التحقيق، بعد إخطار وكيل الجمهورية، أن يأذن تحت رقابته ... " يفهم من نص المادة أن القانون خصص جهات معينة لها الحق في إصدار إذن عملية التسرب وذلك حماية للحقوق الأساسية المكرسة دستوريا، وعليه لا يمكن بأي حال من الأحوال أن يقوم ضابط الشرطة القضائية بالعملية بمفرده دون المرور على الجهاز القضائي²، كما يجب أن يتضمن الإذن بإجراء التسرب تحت طائلة جزاء البطلان الشروط والأوضاع القانونية وعليه يجب أن يكون هذا الإذن مكتوبا تطبيقا للفقرة الأولى من المادة 65 مكرر 15 والتي نصت على " يجب أن يكون الإذن المسلم طبقا للمادة 65 مكرر 11 علاه مكتوبا ..."، إلى جانب ذلك أن يكون مسببا وهذا ما جاء في نص المادة 65 مكرر 15 من ق.ا.ج.ج " يجب أن يكون الإذن ... ومسببا وذلك تحت طائلة البطلان أي من الضروري أن يشمل الإذن على الأسباب والدواعي لخطورة هذا الإجراء وإلا أدى إلى بطلان هذا الإجراء."³

بالإضافة أن يذكر في الإذن الجريمة التي تبرر اللجوء إلى هذا الأسلوب وهي الجرائم المحددة على سبيل الحصر في المادة 65 مكرر 5 من ق.ا.ج.ج، مع ذكر إسم الضابط المشرف على العملية وهويته الكاملة أو العون المكلف.

ثالثا: تحديد المدة المطلوبة لعملية التسرب

حدد قانون الإجراءات الجزائية في المادة 65 مكرر 15 مدة عملية التسرب بأربعة (04) أشهر قابلة

¹ - عبد المجيد جباري، المرجع السابق، ص 58 .

² - رشيدة بوكر، المرجع السابق، 435.

³ - نجية شيخ، إجراء التسرب في القانون الجزائري وسيلة لمكافحة الجرائم المستحدثة، مجلة المعارف، العدد 22، ديسمبر 2018، ص6.

للتجديد ضمن نفس الشروط، أي بناء على إذن مكتوب من وكيل الجمهورية، أو قاضي التحقيق بعد إخطار وكيل الجمهورية، كما أجاز في نفس الوقت للقاضي الذي أصدر هذا الإجراء أن يأمر في أي وقت بوقفه قبل إنقضاء المدة المحددة، طبقا للفقرة 4 من المادة 65 مكرر 15، وفي حالة عدم تمديدتها يمكن للعون المتسرب مواصلة نشاطاته للوقت الضروري لتوقيف العملية في ظروف تضمن أمنه دون أن يكون مسؤولا جزائيا، على ألا يتجاوز ذلك مدة أربع أشهر مع وجوب إخطار القاضي المصدر للرخصة الذي اصدر الإذن في اقرب الآجال، وإذا انقضت مهلة الأربعة أشهر دون أن يتمكن العون المتسرب من توقيف نشاطه في ظروف تضمن أمنه وسلامته يجوز للقاضي الذي اصدر الرخصة أن يمدد هذه المهلة أربعة أشهر أخرى على الأكثر.¹ وللحفاظ على سرية ونجاح عملية التسرب يشترط القانون إبقاء الإذن خارج ملف الإجراءات لغاية الإنتهاء من العملية.

الفقرة الثانية: الشروط الموضوعية

إضافة إلى الشروط الشكلية السابقة الذكر يتطلب اللجوء إلى عملية التسرب مجموعة من الشروط الموضوعية ويمكن إجمالها فيما يلي:

أولا: دوافع اللجوء لعملية التسرب

نظرا لخطورة عملية التسرب فإنه لا يتم اللجوء إلى هذا الإجراء، إلا إذا إقتضت ضرورات التحقيق والتحري ذلك وهذا ما نصت عليه المادة 65 مكرر 11 من قانون الإجراءات الجزائية، والتي إعتبرت التسرب إجراء جديد للتحري أوجدته ضرورات قضائية في التشريع، وقد قصر المشرع اللجوء إلى هذا الإجراء إلا عندما تقتضي ضرورات التحري أو التحقيق في أحد الجرائم المذكورة سابقا ومنها الجرائم الإلكترونية، بمعنى آخر أن اللجوء إلى هذا الإجراء يكون مرتبطا بالضرورة الملحة التي يقتضيها التحري أو التحقيق وذلك بغرض جمع البيانات والإستدلالات الجنائية، فالدافع أولا هو ضرورة التحري، وثانيا طبيعة الجرائم.²

¹ - المادة 65 مكرر 17 من قانون الإجراءات الجزائية الجزائري.

² - فوزي لواتي، التسرب كآلية للتحقيق في جرائم الإتجار بالمخدرات في الجزائر المتطلبات القانونية والإشكالات العملية، مجلة آفاق للعلوم، المجلد 1، العدد 2، مارس 2016، ص 216.

ثانيا: الجرائم المقصودة بعملية التسرب

إن الجرائم المستهدفة بإجراء التسرب، هي تلك الجرائم التي عرفت إنتشارا كبيرا في يومنا هذا والتي تتسم بالتخطيط بالسرعة والفعالية وكلها تشكل تهديدا على إستقرار الدولة في جميع المجالات إقتصادية كانت أو سياسية أو إجتماعية ... إلخ¹، والمحددة حصرا في المادة 65 مكرر 5 من ق.إ.ج.ج في سبعة أنواع هي: جرائم المخدرات، الجريمة المنظمة العابرة للحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، جرائم تبييض الأموال، الإرهاب، الجرائم المتعلقة الخاص بالصرف، جرائم الفساد.

الفرع الثالث: آثار التسرب

يترتب القيام بعملية التسرب عدة آثار تتمثل في:

أولا: تسخير الوسائل المادية والقانونية

نصت المادة 65 مكرر 14 من ق.إ.ج.ج " يمكن لضباط وأعوان الشرطة القضائية المرخص لهم بإجراء عملية التسرب، وكذلك الأشخاص الذين يسخرون لهذا الغرض، دون أن يكون مسئولين جزائيا القيام بما يلي:

- إقتناء أو حيازة أو نقل أو تسليم أو إعطاء مواد وأموال أو منتجات أو وثائق أو معلومات متحصل عليها من ارتكاب الجرائم أو مستعملة في ارتكابها.
- إستعمال أو وضع تحت تصرف مرتكبي هذه الجرائم، الوسائل ذات الطابع القانوني أو المالي وكذا وسائل النقل أو التخزين أو الإيواء أو الحفظ أو الإتصال."

أحيانا لا يكفي أن يقوم المتسرب بالتسرب داخل الجماعة الإجرامية، بل لابد له من القيام ببعض الأفعال حتى يطمئنون إليه، ومن أجل تمكينه من أداء مهامه على أكمل وجه أجاز قانون الإجراءات الجزائية لضباط وأعوان الشرطة القضائية، وكذا الأشخاص المسخرين لعملية التسرب، ارتكاب بعض الأفعال غير المشروعة محددة في القانون، والتي تكفل له النجاح في مهمته دون أن يشكل ذلك تحريضا على ارتكاب الجريمة²، والملاحظ أن المشرع قد قام بتسخير جميع الوسائل المادية والقانونية الممكن

¹ -نجية شيخ، المرجع السابق، ص 11.

² - أمينة معزيز، المرجع السابق، ص 262.

إستعمالها من طرف الشخص المتسرب في إرتكاب الجرائم أو وضعها تحت تصرف مرتكبي هذه الجرائم¹، فالوسائل المادية تتمثل في النقل، التسلم، حيازة، إيواء ...أما الوسائل القانونية فالمقصود بها توفير الوثائق الرسمية إن كان هناك ضرورة لذلك كإستخراج بطاقة التعريف أو رخصة سياقة وبالتالي يحتاج إلى جهاز خاص لتزوير الوثائق الرسمية دون المرور على الإدارة المختصة لإبقاء أعماله ضمن السرية المطلوبة.²

ثانيا: إحاطة العملية بالسرية

حرص المشرع على سرية عملية التسرب بحيث أحاطها بالسرية الكاملة، وحصر مجال العلم بها في جهات المانحة الإذن وكيل الجمهورية وقاضي التحقيق، وما يؤكد سرية العملية نص المادة 65 مكرر³ من ق.ا.ج.ج التي نصت على جزاءات صارمة في حالة الكشف عن الهوية لضابط أو أعوان الشرطة القضائية، بل وسع المشرع من نطاق الحماية لتشمل أفراد عائلة المتسرب وشدد هذه الجزاءات وتتراوح هذه العقوبات من سنتين إلى عشرين سنة حبس وغرامة مالية من خمسين ألف إلى مليون دينار حسب الحالات المذكورة بالمادة السالفة الذكر.

وقد ذهب المشرع أبعد من ذلك بشأن سرية هوية الضابط أو عون الشرطة القضائية القائم بهذه المهمة وذلك بجزمه بعدم السماح بإيداع رخصة الإذن في ملف الإجراءات وهذا ما جاء في نص المادة 65 مكرر 15 من ق.ا.ج.ج، ولم يتوقف المشرع عن هذا الحد بل أضاف بموجب المادة 65 مكرر 18

¹ - زكريا لدغم شيكوش، النظام القانوني للتسرب في القانون الجزائري، مذكرة لنيل شهادة الماجستير في العلوم القانونية والادارية، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، 2013، ص 105.

² - رشيدة بوكري، المرجع السابق، ص، ص 437 - 438.

³ - تنص المادة 65 مكرر 16 من ق.ا.ج.ج على " لا يجوز إظهار الهوية الحقيقية لضابط أو أعوان الشرطة القضائية الذين باشرُوا عملية التسرب تحت هوية مستعارة في أي مرحلة من مراحل الإجراءات. يعاقب كل من يكشف هوية ضابط وأعوان الشرطة القضائية بالحبس من سنتين إلى خمس سنوات وغرامة من 50000 دج إلى 200000 دج .

وإذا تسبب الكشف عن الهوية في أعمال عنف أو ضرب وجرح على أحد هؤلاء الأشخاص أو أزواجهم أو بنائهم أو أصولهم المباشرين فتكون العقوبة الحبس من خمس إلى عشر سنوات والغرامة من 200000 دج إلى 500000 دج . وإذا تسبب هذا الكشف في وفاة أحد هؤلاء الأشخاص فتكون العقوبة الحبس من عشر (10) إلى عشرين (20) سنة وغرامة من 500.000 إلى 1.000.000 دج دون الإخلال عند الاقتضاء بتطبيق أحكام الفصل الأول من الباب الثاني من قانون العقوبات.

من ق.ا.ج.ج أنه "يجوز سماع ضابط الشرطة القضائية الذي تجري عملية التسرب تحت مسؤوليته، دون سواه بوصفه شاهدا عن العملية" ولذلك إذا أراد القاضي سماع شهادة المتسرب فإنه لا يمكن كشف هويته، فلا يتم سماع أقواله أثناء الشهادة، ويحل ضابط الشرطة القضائية بعملية التسرب محله بصفة شاهدا على العملية، وتبعا لذلك فإن شرط السرية المنصوص عليه قانونا، يدل على حرص المشرع على حماية العون المتسرب والعمل على ضمان سلامته وأمنه وسلامة كل عائلته وهي ضمان حقيقية له.¹

ثالثا: الإعفاء من المسؤولية الجزائية

أقر المشرع الجزائري بموجب المادة 65 مكرر 14² من ق.ا.ج.ج بعدم المسؤولية الجزائية لضابط أو أعوان الشرطة القضائية المأذون لهم بتنفيذ عملية التسرب عن كل الأفعال المرتبطة بهذه العملية، وجعل هذه الأفعال من الأفعال المبررة والمباحة، وأخرجها من دائرة التجريم إلى دائرة الأفعال الغير معاقب عليه³ عملا بنص المادة 39 من ق.ع.ج التي تنص على " لا جريمة إذا كان الفعل قد أمر أو أذن به القانون..." كما مدد نطاق هذا الإعفاء لظروف أمنية للمتسرب حتى بعد انقضاء المهلة المحددة في رخصة التسرب أو في حالة تقرر وقف عملية التسرب وفق لما نصت عليه المادة 65 مكرر 17 من ق.ا.ج.ج.⁴

بعد تناولنا كل الأحكام المتعلقة بعملة التسرب ورغم أهميته في مكافحة الجريمة المستحدثة لكن يمكن أن يحاط هذا الإجراء ببعض المشاكل القانونية منها:

1-عدم التحديد الدقيق للأشخاص المساعدين في عملية التسرب حيث نصت المادة 65 مكرر 14 من ق.ا.ج.ج أنه "يمكن ضابط أو أعوان الشرطة القضائية المرخص لهم بإجراء عملية التسرب والأشخاص الذين يسخرونهم لهذا الغرض.." فالمشرع لم يحدد صفة هؤلاء الأشخاص المسخرين للقيام

¹ - نجية شيخ، المرجع السابق، ص 11.

² - تنص المادة 65 مكرر 14 من ق.ا.ج.ج على " يمكن لضابط وأعوان الشرطة القضائية المرخص لهم بإجراء عملية التسرب والأشخاص الذين يسخرونهم لهذا الغرض، دون ان يكونوا مسؤولين جزائيا..."

³ - عز الدين وداعي، التسرب كأسلوب من أساليب البحث والتحري الخاصة على ضوء قانون الإجراءات الجزائية الجزائري والمقارن، المجلة الأكاديمية للبحث القانوني، المجلد 16، عدد 02، 2017، ص 213 .

⁴ - تنص المادة 65 مكرر 17 من ق.ا.ج.ج على أنه " إذا تقرر وقف عملية التسرب، وفي حالة عدم تمديدها، يمكن العون المتسرب مواصلة النشاطات المذكورة في المادة 65 مكرر 14 اعلاه للوقت الضروري الكافي لتوقيف عمليات المراقبة في ظروف تضمن أمنه دون يكون مسؤولا جزائيا، على ألا يتجاوز ذلك مدة أربعة أشهر..."

بعملية التسرب ولا إلى صفتهم، والفئة التي ينتمون إليها، هل هم من عامة الناس أم أشخاص متخصصين في الميدان¹، لذلك يجب على المشرع تدارك هذا الفراغ وذلك لتسهيل مهام الضبطية القضائية في تعيين هؤلاء المسخرين.

-عدم السماح لسماع المتسرب رغم ما يقدمه من معلومات تفيد التحقيق، عكس المشرع الفرنسي الذي يسمح للعون أو الضابط المتسرب الإدلاء بشهادته في حالة نفي الوقائع من طرف أعضاء الشبكة ويمكنه كذلك بناء على طلبه الكشف عن هويته.²

-ما حكم ضابط الشرطة القضائية الذي قام بعملية التسرب والذي ألقى القبض عليه في الجريمة المتسرب فيها خارج الحدود الوطنية، في غياب نصوص قانونية وإتفاقيات قضائية ثنائية أو متعددة الأطراف تنظم هذا الإجراء مع هذه الدول، فهل يعاقب من طرف هذه الدولة أم هناك إجراءات أخرى لإطلاق سراحه عن طريق وجود اتفاقيات تحكم هذه العملية.³

-إشكالية تتعلق بشخص الذي يقوم بعملية التسرب هل يجبر أم يخير للقيام بهذه العملية، وهل يخضع لتدريبات قبل تسريبه كما فعل المشرع الفرنسي.⁴

المطلب الرابع: صعوبات الحصول على الدليل الإلكتروني بالوسائل التقليدية

يعد الدليل الجنائي جوهر الإثبات ووسيلة لإسناد الواقعة الإجرامية إلى المتهم أو نفيها عنه، لذا فهو يكتسي أهمية في جميع مراحل الدعوى، وبه تعرف الحقيقة، ويعرف بأنه "كل وسيلة مرخص أو مسموح بها قانونا لإثبات وجود أو عدم وجود الواقعة المرتكبة، أو صحة أو كذب وقوعها".⁵، وعلى إثر التطور التكنولوجي ظهر إلى الوجود ما يعرف بالدليل الإلكتروني، الذي يرتبط ببروز نوع جديد من الجرائم تسمى بالجرائم الإلكترونية، تتميز بطابعها الخاص والمعقد، بالإضافة إلى صعوبة اكتشافها، وإثباتها يكون بواسطة هذا النوع المستحدث من الأدلة لقصور الوسائل التقليدية في إثباتها والتعرف على مرتكبيها، وهذا

¹ - نجية شيخ، المرجع السابق، ص 14 .

² - عبد المجيد جباري، المرجع السابق، ص 66.

³ - دوادي مجراب، المرجع السابق، ص 362.

⁴ - دوادي مجراب، المرجع نفسه، ص 363.

⁵ - محمد بن فردية، الدليل الجنائي الرقمي وحجتيه أمام القضاء الجزائي -دراسة مقارنة- المجلة الأكاديمية للباحث القانوني، المجلد 5، العدد 2، 2014، ص 277.

ما أدى إلى خلق مشاكل وصعوبات عدة، حول مدى قبوله أو رفضه أو إيمانه كدليل للإثبات أمام القضاء الجنائي.

وسوف نتطرق من خلال هذا المطلب إلى مفهومه (الفرع الأول) وصعوبات إثبات الدليل الإلكتروني في (الفرع الثاني) وحججه في (الفرع الثالث).

الفرع الأول: مفهوم الدليل الإلكتروني

الدليل الإلكتروني ثمرة من ثمرات التكنولوجيا الحديثة، وهو من الناحية العملية وسيلة لا تكاد تخطئ في إثبات وقوع الجريمة الإلكترونية، كما يمكن القول أن الدليل الرقمي قرينة قاطعة في وقوع الجريمة الإلكترونية، لا سيما عند تكرار التجارب ودقتها ومهارة خبراءها، إلا أنه يبقى في الكثير من الأحيان قاصرا على نسبتها لشخص معين¹، لذا سوف نقوم بتعريف هذا النوع المستحدث من الأدلة (أولا) وبيان خصائصه (ثانيا).

أولا: تعريف الدليل² الرقمي

تعددت التعريفات التي قيلت بشأن الدليل الإلكتروني وتباينت بين موسع ومضيق لهذا التعريف، ويرجع ذلك لموضع العلم الذي ينتمي إليه هذا الدليل شأنه شأن الجريمة الإلكترونية لأنها محل هذا الدليل، فاختلقت التعريفات في ذلك، فيعرفه البعض بأنه "الدليل الذي يجد له أساسا في العالم الافتراضي ويقود إلى الجريمة" كما يعرفه جانب من الفقه "ذلك الجزء المؤسس على الاستعانة بتقنية المعالجة التقنية للمعلومات والذي يؤدي إلى إقناع قاضي الموضوع بثبوت ارتكاب شخص ما لجريمة عبر الانترنت"³،

¹ - عبد القادر عمير، آليات إثبات الجريمة المعلوماتية في التشريع الجزائري-دراسة مقارنة-أطروحة لنيل شهادة دكتوراه، كلية الحقوق، جامعة الجزائر، 2019-2020، ص126.

² - الدليل لغة هو ما يستدل به، والدليل هو الدال أيضا، والدليل في اللغة العربية هو المرشد وما به الإرشاد، وما يستدل به، والدليل الدال والجمع أدلة ودلالات.

والدليل إصطلاحا هو ما يلزم من العلم به علم شيء آخر، وغايته أن يتوصل العقل الى التصديق اليقيني فيما يشك في صحته، أي التوصل به إلى معرفة الحقيقة، ويعرف الدليل بأنه أي شيء يفيد في إثباتا نفي مسألة معينة في القضية، أو ما كل ما يتصل اتصالا مباشرا بإدانة متهم أو تبرئته، استنادا إلى المنطق. أنظر في ذلك محمد الأمين البشري، التحقيق في الجرائم المستحدثة، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الامنية، الرياض، ط1، 2004، ص، ص 229-230.

³ - ضياء علي أحمد نعمان، الغش المعلوماتي الظاهر والتطبيقات، سلسلة الدراسات القانونية في المجال المعلوماتي، المطبعة والوراقة الوطنية، مراكش، ط1، 2011، ص282.

ويعرف أيضا بأنه " معلومات يقبلها المنطق والعقل ويعتمدها العلم، يتم الحصول عليها بإجراءات قانونية وعلمية، بترجمة البيانات الحاسوبية المخزنة في أجهزة الحاسب الآلي وملحقاتها وشبكات الإتصال، ويمكن إستخدامها في أية مرحلة من مراحل التحقيق أو المحاكمة، لإثبات حقيقة فعل أو شيء له علاقة بجريمة أو جان أو مجني عليه"¹، ومن جانب آخر يعرف بأنه "الدليل المأخوذ من أجهزة الكمبيوتر ويكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية، ممكن تجميعها وتحليلها بإستخدام برامج وتطبيقات وتكنولوجيا خاصة، وهو مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور والأصوات والأشكال والرسوم، وذلك من أجل الربط بين الجريمة والمجرم والمجني عليه وبشكل قانوني يمكن الأخذ به أمام أجهزة إنفاذ وتطبيق القانون."²

وعليه يمكن القول أن الدليل الإلكتروني هو ذلك الدليل الذي ينشأ في العالم الرقمي، والذي يكون على شكل مستخرج مادي يتم قبوله أمام القضاء.

لم تعرف التشريعات المقارنة الدليل الإلكتروني ومن بينها المشرع الجزائري الذي ترك مهمة ذلك للفقهاء إلا أننا نجد المشرع المصري قام بتعريف الدليل الإلكتروني في المادة 1 من الفقرة العشرين (20) من قانون تقنية المعلومات بقوله " الدليل الرقمي: أي معلومات إلكترونية لها قوة أو قيمة ثبوتية مخزنة أو منقولة أو مستخرجة أو مأخوذة من أجهزة الحاسب أو الشبكات المعلوماتية وما في حكمها، ويمكن تجميعها وتحليلها بإستخدام أجهزة أو برامج أو تطبيقات تكنولوجية خاصة."³

ثانيا: خصائص الدليل الإلكتروني

نظرا للطبيعة الخاصة للجرائم الإلكترونية فإن دليل إثباتها يتميز عن الدليل التقليدي، بعدة خصائص

هي:

¹ - نضال ياسين الحاج حمو، دور الدليل الإلكتروني في الإثبات الجنائي -دراسة تحليلية - مجلة جامعة تكريت للعلوم القانونية والسياسية، المجلد 1، العدد 19، 2013، ص181. منشور على الموقع www.iasj.net.iasj article أطلع عليه يوم 2020/07/25 على الساعة 15:30.

² - ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والانترنت، دار الكتب القانونية المجلة الكبرى، د ط، 2006، ص88.

³ - قانون رقم 175 -2018 بشأن مكافحة جرائم تقنية المعلومات المصري، الجريدة الرسمية للجمهورية العربية المصرية، عدد 32 مكرر (ج)، الصادرة بتاريخ 2018/07/14.

1-الدليل الإلكتروني دليل علمي وتقني

الدليل الإلكتروني بإعتباره دليل يحتاج إلى بيئته التقنية التي يتكون فيها لكونه من طبيعة تقنية المعلومات، لأجل ذلك فإن ما ينطبق على الدليل العلمي ينطبق على الدليل الإلكتروني، فإذا كان الدليل العلمي له منطقته الذي يجب ألا يخرج عليه من حيث أنه يجب عدم تعارضه مع القاعدة العلمية السليمة، فإن الدليل الإلكتروني له ذات الطبيعة، فلا يجب أن يخرج الدليل العلمي عما توصل إليه العلم الرقمي وإلا فقد معناه¹، ونظر لبيئة التقنية وكذا بإعتبار الدليل الإلكتروني عبارة عن نبضات إلكترونية ذات طبيعة ديناميكية، تتميز بالسرعة الفائقة المتعدية لحدود الزمان والمكان كل هذا يجعل الدليل الإلكتروني دليل يعتمد على التقنيات بالدرجة الأولى.²

2-الدليل الإلكتروني متنوع ومتطور

لما كانت البيئة التي يعيش فيها الدليل الإلكتروني بيئة متطورة بطبيعتها، وأن تطورها الذي يكاد يكون تلقائيا مما يتسع لشمول مظاهر إلكترونية جديدة، لا سيما وأن المبدأ في العالم الافتراضي أنه لا يزال في بداياته ولم يصل بعد إلى منتهاه، فالعالم الرقمي لا ينتهي ولن يكون من السهولة إحتوائه فهو عالم متسع ولهذا فإن الدليل الإلكتروني هو الآخر دليل متطور.³

3-صعوبة التخلص من الدليل الإلكتروني

تعتبر إحدى أهم خصائص الدليل الإلكتروني، وميزة يتمتع بها هذا الدليل عن غيره من الأدلة الأخرى، إن التخلص من الدليل الإلكتروني بإستخدام وسائل التخلص من الملفات في الحاسب الآلي، أو الأنترنت كخاصية `delete, remove, ecrase`... إلخ لا تعد من العوائق التي تحيل دون إسترجاع الملفات المذكورة إذ تتوفر برمجيات من ذات الطبيعة الرقمية، يمكن بمقتضاها إسترداد كافة الملفات التي تم إلغائها أو إزالتها من الحاسب الآلي.⁴

1 - خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص، ص، 179 - 180.

² - عيدة بلعابد، الدليل الرقمي بين حتمية الاثبات الجنائي والحق في الخصوصية المعلوماتية، مجلة آفاق علمية، المجلد 11، العدد 01، 2019، ص 138.

³ - عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن إستخدام الأنترنت، المرجع السابق، ص 980.

⁴ - خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص 185.

4-الدليل الإلكتروني ذو طبيعة معنوية

يعتبر الدليل الإلكتروني دليلا غير ملموس أي كونه دليل ذو طبيعة معنوية، يكون في شكل موجات مغناطسية أو كهربائية، حيث أن ترجمة الدليل الإلكتروني وإخراجه في شكل مادي ملموس لا يعني أن هذا التجمع يعتبر هو الدليل، بل إنما هذه العملية تعتبر عملية نقل تلك المجالات من طبيعتها الإلكترونية إلى الشكل الذي يمكن الاستبدال بها على معلومة معينة.¹

5-الدليل الإلكتروني قابل للنسخ

يتميز الدليل الإلكتروني بخاصية المقدرة على نسخه، حيث يمكن نسخ الدليل الإلكتروني بنسخه مطابقة للأصل تماما، ويمكن إجراء الفحص المعلوماتي على هذه النسخة، لتفادي خطر إتلاف النسخة الأصلية وهذه الميزة لا تتوافر في الأدلة المادية.²

ثالثا: أشكال الدليل الإلكتروني

للتعريف بالدليل الإلكتروني يجب علينا تحديد أنواعه وأشكاله، حتى يتسنى فهم الهيئة التي يتخذها الحكم على قيمته القانونية فيما بعد، بحيث يمكن تقسيم الدليل الإلكتروني إلى التقسيم التقليدي والتقسيم الحديث.

1-التقسيم التقليدي

قسم الدليل الإلكتروني إلى قسمين الأول اعتبر ليكون وسيلة إثبات والثاني لم يعد كوسيلة إثبات

أ- أدلة أعدت لتكون وسيلة إثبات

و تضم السجلات التي تم إنشاؤها تلقائيا بواسطة الأجهزة التكنولوجية، وتعتبر هذه السجلات من مخرجات الحاسب الآلي التي لم يساهم الأفراد في إنشائها، مثل سجلات الهاتف وفواتير البطاقة البنكية، بالإضافة إلى ذلك، هناك سجلات تحتوي على بيانات تم إدخالها إلى الجهاز وتم إجراء المعالجة عليها

¹ خالد عياد الحلبي، المرجع السابق، ص232.

² - هارون بحرية، دور الدليل الرقمي في إثبات الجريمة المعلوماتية في التشريع الجزائري، ورقة علمية مقدمة في إطار الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، مخبر الحقوق والحريات في الأنظمة المقارنة، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، الفترة بين 16، 17 نوفمبر 2015، ص3.

من خلال برنامج خاص، كما في إجراء العمليات الحسابية على البيانات التي يحتويها السجل.¹

ب- أدلة لم تعد لتكون وسيلة إثبات

وهذا النوع من الدليل الإلكتروني نشأ دون إرادة الفرد، أي أنها أثر يتركه الجاني دون أن يكون راغبا في وجوده، ويسمى بالبصمة الإلكترونية أو الآثار المعلوماتية الإلكترونية، وعادة ما تترك هذه الآثار من قبل الجاني عند تسجيل الرسائل المرسلة، أو تلك التي يستقبلها وكافة الإتصالات التي تمت من الحاسب الآلي أو شبكة الأنترنت.²

حيث أن هذا النوع من الأدلة لم يعد أساسا للحفظ من قبل من صدر عنه، غير أن الوسائل الفنية الخاصة تمكن من ضبط هذه الأدلة ولو بعد فترة زمنية من إنشائها، فالإتصالات التي تجري عبر الأنترنت والمراسلات الصادرة عن الشخص أو التي يتلقاها، كلها يمكن ضبطها بواسطة تقنية خاصة بذلك³، كتقنية التتبع والإسترداد، ومن ضمن هذه التقنيات ما يعرف ببرتوكول (IP) والذي يتمكن من ضبط تحركات مستخدم شبكة الأنترنت، وإستخراج الدليل الإلكتروني بإستخدام بروتوكولات⁴(IP/TCP) فبواسطة هذه البرتوكولات يمكن معرفة مصادر العناوين والمعلومات والتي يحتويها هذا البرتوكول بإعتباره وسيلة إتصال بين الشبكات، وعن طريقهما يمكن تحديد المنظومة المعلوماتية المستخدمة في الجرائم الإلكترونية، وبواسطتها يمكن تتبع المراسلات واستعادة البيانات.⁵

وتبدو أهمية التمييز بين هذين النوعين من الأدلة الإلكترونية، حيث أن النوع الأول أعد أصلا ليكون وسيلة إثبات لبعض الوقائع، وعادة ما يعتمد إلى حفظه للاحتجاج به لاحقا، وهو ما يقلل من إمكانية فقده، ويجعل من السهل الحصول عليه، عكس النوع الثاني فهو لم يعد أصلا ليكون أثرا لمن صدر عنه، فيعتبر هذا الأخير ذا أهمية من النوع الأول لأنه غالبا ما يتضمن معلومات ذات مصداقية تفيد في

¹ - لينا محمد الأسدي، المرجع السابق، ص260.

² - خالد عياد الحلبي، المرجع السابق، ص234.

³ - خالد عياد الحلبي، المرجع نفسه، ص235.

⁴ - بروتوكول (IP) هو المسؤول على إرسال رزم على عنوان وجهة المعطيات، أما بروتوكول (tcp) transport control

Protocol وهو المسؤول عن تدقيق صحة نقل المعلومات من الحاسب الآلي إلى الحاسب الخادم. أنظر في ذلك دلال

مولاي ملياني، المرجع السابق، ص109.

⁵ - دلال مولاي ملياني، المرجع نفسه، ص109.

الكشف عن الجريمة، ويمكن الحصول عليه بإتباع تقنيات خاصة قد تكون صعبة ومعقدة، وهو على العكس من الأول لم يعد ليحفظ مما يجعله عرضة للفقان.¹

2-التقسيم الحديث

تقسم الأدلة الإلكترونية الخاصة بأجهزة الكمبيوتر وشبكاتها، الأدلة الإلكترونية الخاصة بالإنترنت، كذلك الأدلة الخاصة ببرتوكولات تبادل المعلومات بين أجهزة الشبكة العالمية للمعلومات، وأخيرا الأدلة الإلكترونية بالشبكة العالمية للمعلومات.²

كما يوجد الدليل الإلكتروني في صورة مخرجات وهو على ثلاثة أشكال تتمثل في:³

-المخرجات الورقية

من خلال هذه المخرجات الورقية يمكن تسجيل المعلومات على الورق ويستخدم في ذلك الطابعات والراسم في طباعة الرسومات بدرجات وضوح مختلفة على الورق.

-المخرجات ذات الطبيعة الرقمية

وتسمى كذلك بالمخرجات اللاورقية، وهي المعلومات المخزنة على الأوعية المغنطة كالأشرطة المغناطيسية والأقراص المرنة، والقرص الصلب وغيرها من الأوعية الأخرى كالفلش ديسك الذي يحتوي على مساحة تخزين واسعة.

المخرجات المرئية

ويتمثل في عرض البيانات المعالجة آليا بواسطة الحاسب الآلي على الشاشة الخاصة به، أو الهواتف الذكية.

أما بالنسبة للمشرع الجزائري فقد تطرق في نص المادة 06 من القانون رقم 09-04 على شكل الدليل الإلكتروني بحيث يتم نسخ المعطيات محل البحث، وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية قابلة للحجز، بهذا حافظ المشرع على البيئة التي يتواجد فيها الدليل الإلكتروني، تم وسع من

¹ - جمال إبراهيمي، المرجع السابق، ص 173.

² - ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص 88.

³ - عبد القادر عمير، المرجع السابق، ص 143.

أشكال الدليل حينما قرر إمكانية استعمال الوسائل التقنية لتشكيل وإعادة تشكيل المعطيات، قصد جعلها قابلة للاستغلال لأغراض التحقيق وفي هذه الحالة أعطى المشرع لسلطة التحقيق حرية تشكيل الدليل شريطة عدم المساس بمحتوى المعطيات.¹

وما يمكن استخلاصه أن الدليل الإلكتروني يتميز بالتنوع وله أشكال متعددة حيث تعددت وسائل الحصول عليه، إلا أن مجرد وجود هذا الدليل غير كاف لإصدار الحكم ضد المجني عليه، إذ لا بد أن يكون لهذا الدليل القيمة القانونية التي يمكن من خلالها الاستناد على هذا الدليل لإصدار حكم الإدانة على المتهم، ولهذا فإن للدليل الإلكتروني مجموعة من الشروط لكي يقبل أمام القضاء.

رابعا: شروط قبول الدليل الإلكتروني

حرصت أغلبية التشريعات والقوانين على إحاطة بعض الإجراءات بشروط وضمانات أساسية، ومنها قبول الأدلة الإلكترونية، ولا يمكن الإعتداد بالدليل الإلكتروني كأداة إثبات في الجريمة الإلكترونية، إلا إذا توافر على شروط معينة هي:

1- يجب أن تكون هذه الأدلة يقينية

يشترط في الأدلة المستخرجة من الحاسب الآلي أن تكون غير قابلة للشك، حتى يمكن الحكم بالإدانة، ذلك أنه لا مجال للدحض قرينة البراءة وإفترض عكسها إلا عندما يصل إقتناع القاضي إلى حد الجزم واليقين²، ويترتب على ذلك أن كافة مخرجات الوسائل الإلكترونية من مخرجات ورقية أو إلكترونية أو أقراص مغناطسية تخضع لتقدير القاضي الجنائي، ويجب أن يستنتج منها الحقيقة بما يتفق مع اليقين وبيتعد عن الشك والاحتمال³، ولهذا يستطيع القاضي أن يصل إلى يقينية الدليل الإلكتروني عن طريق نوعين من المعرفة أولهما المعرفة الحسية التي تتركها الحواس من خلال معاينة هذا الدليل وفحصه، وثانيهما المعرفة العقلية التي يقوم بها القاضي عن طريق التحليل والإستنتاج، من خلال الربط بين هذا الدليل الإلكتروني والملابسات التي أحاطت بها، وإذا لم ينته القاضي إلى الجزم بنسبة الفعل أو الجريمة

¹ - هارون بحرية، المرجع السابق، ص 06.

² - علي حسن محمد الطوالة، المرجع السابق، ص 190.

³ - خالد ممدوح إبراهيم، المرجع السابق، ص 187.

الإلكترونية إلى المتهم يجب عليه أن يقضي بالبراءة فالشك يجب أن يستفيد منه المتهم المعلوماتي.¹

2- يجب الحصول على الدليل بصورة مشروعة.

يجب أن يكون الدليل الإلكتروني مشروعا، أي أن إجراءات جمع الأدلة الإلكترونية المتحصلة من الحاسب الآلي إذا خالفت قواعد الإجراءات التي تنظم كيفية الحصول عليها، فإنها تكون باطلة ولا تصلح لأن تكون أدلة تبنى عليها الإدانة في المواد الجزائية²، كما أن مسألة البحث على الدليل مقيدة باحترام حقوق الدفاع وقيم العدالة وأخلاقياتها، ومقتضيات الحفاظ على كرامة الإنسان، وهو ما لا يمكن أن يتأتى إلا إذا كان البحث عن الدليل قد تم بإستخدام إجراءات مشروعة، فالطرق غير المشروعة للتحقيق يترتب عليها عدم مشروعية الدليل المستمد منها³، ومن أمثلة الطرق غير المشروعة التي يمكن تستخدم في الحصول على الأدلة الجنائية ومن بينها الدليل الإلكتروني، نذكر على سبيل المثال إستخدام الإكراه المادي والمعنوي في مواجهة المتهم المعلوماتي من أجل فك شفرة النظام المعلوماتي، أو الوصول إلى دائرة حل التشفير، أو الوصول إلى ملفات البيانات المخزنة، أو إستخدام التدليس والغش في الحصول على مخرجات الوسائل الإلكترونية⁴، فمشروعية الدليل تتطلب صدقه في مضمونه وأن يكون هذا المضمون قد تم الحصول عليه بطرق مشروعة وتدل على الأمانة والنزاهة من حيث الحصول عليه.⁵

3- مناقشة الدليل الإلكتروني

الأصل الذي يحكم إجراءات المحاكمة، هو أن تكون المرافعة شفوية وحضورية والمقصود بالمرافعة هنا إجراءات التحقيق النهائي الذي تجريه المحكمة⁶، ويقصد بمبدأ مناقشة الدليل بصفة عامة أن القاضي لا يمكن أن يؤسس إقتناعه إلا على العناصر الإثباتية التي طرحت في جلسة المحاكمة وخضعت لحرية

¹ - ضياء علي أحمد النعمان، المرجع السابق، ص 311 .

² - مبارك بن الطيبي، محمد رحموني، شروط قبول الدليل الرقمي كدليل إثبات في الجريمة الإلكترونية، مجلة القانون والعلوم السياسية، المجلد 05، العدد 02، 2019، ص 27.

³ - سامية بلجراف، سلطة القاضي الجزائي في قبول وتقدير الدليل الرقمي، مجلة الدراسات القانونية المقارنة، المجلد 07، العدد 01، 2021، ص 686.

⁴ - ضياء علي أحمد النعمان، المرجع السابق، ص 315.

⁵ - خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص 191.

⁶ - مأمون محمد سلامة، قانون الإجراءات الجنائية معلقا عليه بالفقه والقضاء، دار الفكر العربي، القاهرة، د ط، 1981، ص 108.

مناقشة أطراف الدعوى¹، وقد نص المشرع الجزائري من خلال المادة 2/212 من ق.ا.ج.ج على أنه "...ولا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه" ويعني هذا إذا كانت مخرجات الوسائل الإلكترونية تعد أدلة إثبات قائمة في أوراق الدعوى التي ينتظرها القاضي، فإنه يجب عليه مناقشتها أمام الخصوم ويترتب على ذلك أن هذه المخرجات سواء كانت مطبوعة أو بيانات معروضة على شاشة الحاسب الآلي، أو اتخذت شكل أشرطة وأقراص ممغنطة أو ضوئية تكون محلا للمناقشة عند الإعتماد عليها كأدلة أمام المحكمة²، وعليه فإن كل دليل يتم الحصول عليه من خلال البيئة الرقمية، يجب أن يعرض في الجلسة بصفة مباشرة أمام القاضي لمناقشتها، وله الحرية والإجتهاد في الحكم في الجرائم الإلكترونية، وعدم الإعتماد على رأي الغير، إلا إذا كان هذا الغير من الخبراء، وقد إرتاح ضميره إلى التقرير المحرر منه وقرر الإستناد إليه ضمن حكمه وبناء عليه يكون متولدا من عقيدته هو وليس من تقرير الخبير.³

4- أن يكون الدليل الإلكتروني ذي علاقة بموضوع الجريمة الإلكترونية

إلى جانب الشروط السابقة الذكر، هناك بعض التشريعات المقارنة⁴، أضافت هذا الشرط وأسّمته بمبدأ العلاقة الكاشفة، حيث يتطلب ضرورة أن يكون هناك علاقة من نوع خاص ما بين الدليل وبين الواقعة محل الدعوى، وشروط ثبوت العلاقة الكاشفة في الدليل الإلكتروني يتطلب شرط آخر وهو مطابقة الدليل الإلكتروني المستخرج من الحاسب الآلي للأصل الموجود بداخله بحيث لا يكون هناك ثمة إدعاء أو دفع بأن البيانات غير صحيحة بسبب عدم دقة عمل الكمبيوتر.⁵

وخلاصة لما ذكرناه يمكن القول أن المعلومات والبيانات التي يحتويها الحاسب الآلي لها حجيتها في الإثبات مادام توفرت فيها الشروط السابقة الذكر.

¹ - نصر الدين مروك، محاضرات في الإثبات الجنائي النظرية العامة للإثبات الجنائي، الجزء الأول، دار هومة، الجزائر، 2003، ص 637.

² - ضياء علي أحمد نعمان، المرجع السابق، ص 311.

³ - نور الهدى محمودي، حجية الدليل الرقمي في إثبات الجريمة المعلوماتية، مجلة الباحث للدراسات الأكاديمية، العدد 11، جوان 2017، ص 919.

⁴ - كتشريع الولايات المتحدة الأمريكية الذي ضمن هذا الشرط من خلال قانون الإثبات الفيدرالي الأمريكي في المادة 401، أنظر في ذلك عمر أبو بكر بن يونس، المرجع السابق، ص 992.

⁵ - خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص 188.

الفرع الثاني: صعوبات إثبات الدليل الإلكتروني

تجد السلطات القضائية المختصة بالبحث والتحري صعوبات كبيرة في مجال إثبات الجريمة الإلكترونية ، لإعتمادها على إجراءات خاصة ومعقدة في إستخلاص الدليل الإلكتروني، ويرجع السبب في ذلك لوجود عدة صعوبات ومعوقات والتي تتمثل فيما يلي:

أولاً: إنعدام الدليل المرئي

إن الجرائم التي تقع على النظم المعلوماتية أو بواسطتها ماهي إلا بيانات غير مرئية، لا تفصح عن شخصية معينة، وهذه البيانات مسجلة إلكترونياً بكثافة بالغة وبصورة مشفرة على دعائم أو وسائط التخزين ضوئية أو ممغنطة، لا يمكن للإنسان قراءتها، إلا عن طريق الحاسب الآلي، ولعل مشكلة الطبيعة غير المرئية للدليل الإلكتروني تصعب من المهام الملقاة على الجهات التي تتعامل مع الجرائم التي تقع عبر الوسائل الإلكترونية، بحيث تجعلهم غير قادرين على فحص وإختيار البيانات محل الاشتباه، خاصة حالات التلاعب في برامج الحاسوب، وبالتالي إستحالة الوصول إلى الجناة.¹

ثانياً: سهولة محو الدليل أو تدميره في زمن قصير

من ضمن الصعوبات التي يمكن أن تعترض الإثبات في مجال الجرائم الإلكترونية، سهولة محو الجاني أو تدميره لأدلة الإدانة في زمن قصير، فضلاً عن تنصله من مسؤولية هذا العمل بسبب الخطأ في نظام الحاسب الآلي أو الشبكة أو في الأجهزة²، من الأمثلة الواقعية التي إستطاعت فيها السلطات الأمنية منع الجناة من تدمير الأدلة الخاصة بإدانتهم بطريقة إلكترونية، منها حالة في النمسا قام أحد مهربي الأسلحة بإدخال تعديلات على الأوامر العادية لنظام تشغيل حاسب آلي يستخدمه في تخزين عناوين عملائه، بحيث يترتب على إدخال أمر على الحاسب الآلي من خلال لوحة مفاتيحه بالنسخ أو الطبع محو وتدمير البيانات كلها، إلا أن المتخصصين في معالجة البيانات بالجهاز المركزي لمكافحة الغش المعلوماتي بالنمسا شعروا أن نظام تشغيل الحاسب الآلي للفاعل قد جرى تغييره وبالتالي قاموا بإستنساخ الأقراص الممغنطة المطبوعة عن طريق أنظمة حساباتهم الآلية.³

¹ - لينا محمد الأسدي، المرجع السابق، ص269.

² - عبد العالي الديري، محمد صادق إسماعيل، المرجع السابق، ص328.

³ - Ulrich Sieber, the international handbook on computer crime computer related economic crime and the infringement of provacy 1986,p141. مشار إليه لدى عن عبدالله حسين علي محمود، المرجع السابق، ص، ص345-346.

ثالثا: إستخدام كلمات السر أو الشفرات لإعاقة الوصول إلى الدليل

يقوم الجناة في الجرائم الإلكترونية عادة بتأمين أنفسهم بتدابير أمنية وافية، مما يزيد من صعوبة كشف أسرارهم وكذا الأفعال غير المشروعة التي يرتكبونها، وذلك عن طريق إستخدام كلمات السر والتشفير التي تمكنهم من إخفاء الأدلة التي تتخلف في الوسط الإلكتروني ضدهم، بالإضافة إلى دس بعض التعليمات الخفية بينها، أو ترميزها لإعاقة أو منع الإطلاع عليها أو ضبطها، فلا يمكن لغيرهم أن يفهم مقصدها، كما قد يتم تشفير التعليمات من خلال إستعمال بعض الطرق والبرامج المتطورة والخاصة بتشفير البيانات، الأمر الذي يجعل الوصول إليها في منتهى الصعوبة.¹

رابعا: كثافة البيانات المتعين فحصها

من الصعوبات أيضا التي تواجه السلطات المختصة بالبحث والتحري في هذا النوع من الجرائم الكم الهائل من البيانات، التي يتم تداولها من خلال الأنظمة المعلوماتية، التي تقع عائق أمام أجهزة التحقيق والدليل على ذلك أن طباعة كل ما يوجد على الدعامات الممغنطة لمركز حاسب متوسط الأهمية، يتطلب مئات الآلاف من الصفحات والتي قد لا تثبت كلها تقريبا شيئا على الإطلاق.²

لهذا كان لزاما لهذه الجهات أن تستعين بالخبراء التي تقوم على التمييز بين ما هو مفيد في التحقيق وما هو خارج عن إطار التحقيق وإلا دخلت السلطات المختصة بالبحث والتحري في دائرة مغلقة من المعلومات لن يخرج منها.³

¹ - لنا محمد الأسدي، المرجع السابق، ص270.

² - الطيبي البركة، إشكالية الإثبات في الجرائم الإلكترونية، مجلة افاق علمية، المجلد 11، العدد 01 سنة 2019، ص276.

³ - ميسون خلف حمد الحمدان، مشروعية الأدلة الإلكترونية في الإثبات الجنائي، مجلة كلية الحقوق المجلد 18، كانون الثاني، جامعة النهرين، 2016 ص227. مقال منشور على الموقع - <http://www.mlawnahrain.org/issue.php> - 58أطلع عليه يوم 2018/09/25 على الساعة 15h:30.

خامسا: إحجام المجني عليه عن التبليغ

يعد إحجام وإمتناع المجني عليه التبليغ عن هذه الجرائم ، من بين أكثر المشاكل والتحديات التي تقف في وجه القائمين على مواجهة الجريمة، ليس من حيث إثباتها فقط بل حتى في دراسة هذه الظاهرة¹، ويمكن رد الإحجام عن التبليغ إلى سببين الأول: يتمثل في الأضرار التي سوف تلحق بسمعتهم في حالة التبليغ، أو خسارة المستخدمين لديهم، أو ثقة عملائهم أو معرفة الضعف في أنظمتها المعلوماتية لغير الجاني، كما في المؤسسات المالية الكبرى كالبنوك والمنشآت الصناعية والتجارية، أما السبب الثاني هو الخوف من التشهير والفضيحة وخاصة في الجرائم الماسة بالعرض والشرف²، كما يلاحظ كذلك أن العديد من ضحايا الجرائم الإلكترونية لا يققون إلى حد عدم التبليغ، بل يرفضون أي تعاون مع الجهات المختصة خشية معرفة العامة بوقوع الجريمة، ويسعون بدلا من ذلك إلى محاولة تجاوز آثارها حتى ولو كانت الوسيلة هي مكافأة المجرم، ونذكر على سبيل المثال ما حدث في بنك marchant Bank city في بريطانيا تعرض لنقل 8مليون جنيه إسترليني من أحد أرصده إلى حساب في سويسرا، وقد تم القبض على الفاعل أثناء محاولته سحب المبلغ المذكور، وكان موقف البنك غريبا فبدلا من أن يقوم بإبلاغ السلطات، قام بدفع مبلغ مليون جنيه إسترليني للفاعل بشرط عدم إعلامه للآخرين بشيء عن جريمته، وإخطار البنك عن الآلية التي نجح من خلالها في إختراق نظام الأمن الخاص بحاسوب البنك الرئيسي³.

كما دلت دراسة أجريت في فرنسا أن الجرائم الإلكترونية التي تم إكتشافها لم تمثل سوى 1% فقط من الجرائم المرتكبة، أما تلك التي تم الإبلاغ عنها فلم تتعد 15% من النسبة السابقة⁴، مما يزيد من الصعوبة لا في مجال إكتشاف وإثبات الجرائم الإلكترونية فحسب بل في دراسة الظاهرة برمتها، وهو ما يعبر عنه علماء الإجرام بالرقم الأسود "chiffre noire" حيث يعيق رسم السياسة الجنائية السلمية لمواجهة الظاهرة الإجرامية المستجدة وإختيار أفضل الوسائل لمواجهتها⁵.

¹ عبد القادر عميمر، المرجع السابق، ص151.

² - أحمد عبد اللاه المراغي، المرجع السابق، ص119.

³ - عبد العال الديري، محمد صادق إسماعيل، المرجع السابق، ص339.

⁴ - سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت، دار النهضة العربية، القاهرة، ط1،

1999، ص95.

⁵ - رشيدة بوكور، المرجع السابق، ص471.

سادسا: نقص خبرة أجهزة العدالة

لا تملك أجهزة العدالة من ضباط الشرطة، وسلطات التحقيق والمحاكمة التأهيل الكافي في الميدان التقني، وهذا ما يزيد من صعوبة وصولهم إلى الدليل الإلكتروني وكيفية ضبطه والمحافظة عليه، فنقص الخبرة لدى هؤلاء قد يفضي إلى تدمير الدليل وإتلافه، على اعتبار أن جهلهم بأساليب ارتكاب الجرائم الإلكترونية يجعلهم في كثير من الأحيان يقعون في أخطاء، من شأنها أن تؤدي إلى محو الأدلة الإلكترونية أو تدميرها¹، وأثبتت بعض الوقائع أن هناك جرائم إلكترونية ارتكبت على مرأى ومسمع من رجال الأمن، بل قاموا بتقديم يد المساعدة لمرتكبي الجرائم المعلوماتية دون قصد وعن جهل²، ومن هنا كان من الضروري أن يكون الأشخاص المؤهلين للبحث والتحري في مجال الجرائم الإلكترونية، على دراية كافية فيما يتعلق بالحاسب الآلي وملحقاته والجرائم التي تقع في نطاقه.³

سابعا: ارتفاع تكاليف جمع الأدلة

إن التحقيق في الجرائم الإلكترونية يحتاج إلى خبراء ومختصين، وهؤلاء يحتاجون إلى دورات مستمرة متزامنة مع تطور التقنية الإلكترونية، وهذا الأمر يتطلب تكاليف باهظة، وكذلك التفتيش عن الأدلة يحتاج إلى فحص آلاف الصفحات خصوصا عندما لا تثبت تلك الصفحات شيئا.⁴

الفرع الثالث: القاضي الجزائي ودوره في تقدير الدليل الإلكتروني وحجيته في الإثبات

تذهب جل التشريعات المقارنة إلى قبول الدليل الإلكتروني، المتحصل عليه من أنظمة البرمجة الآلية أو مخرجات أنظمة المعالجة الآلية للبيانات المكتوبة على الشاشات، أو البيانات المسجلة على دعائم ممغنطة، أو مخرجات أنظمة المعالجة، كأداة يقوم عليها الإثبات الجزائي إلا أن هذه الأدلة المتحصل عليها من هذه الوسائل السالفة الذكر تخضع لسلطة القاضي الجزائي التقديرية ومدى إقتناع القاضي بها،

¹ - موسى مسعود أرحومة، الإشكاليات التي تثيرها الجريمة المعلوماتية عبر الوطنية، ورقة علمية مقدمة في إطار المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، ليبيا، المنعقد في 28-29/10/2009، ص5.

² - كمثال على ذلك طلب إحدى دوائر الشرطة بالولايات المتحدة الأمريكية من الشركة تعرضت للقرصنة أن تتوقف عن تشغيل جهازها الآلي للتمكن من وضعه تحت المراقبة بهدف كشف مرتكب الجريمة، وقد حدث نتيجة لذلك أن تسببت دائرة البوليس بدون قصد في إتلاف ما كان قد سلم من الملفات والبرامج انظر "يوسف الصغير، المرجع السابق، ص122.

³ - عبد القادر عمير، المرجع السابق، ص152.

⁴ - خالد عياد الحلبي، المرجع السابق، ص228.

كما أن مدى قبول هذه الأدلة يختلف من نظام قانوني لآخر¹، سوف نتطرق إلى نظم الإقتناع الذاتي للقاضي الجزائي (أولا) ثم الإقتناع الذاتي للقاضي الجزائي لقبول الدليل الإلكتروني (ثانيا).

أولا: نظم الإقتناع الذاتي للقاضي الجزائي

الإثبات الجنائي هو كل ما يؤدي إلى كشف غموض الجريمة وإقامة الدليل على وقوعها والتأكد من أن المتهم هو مرتكب الجريمة بالفعل ووجود الدليل على ذلك، ويعتبر الدليل الوسيلة القانونية التي يستعين بها القاضي للوصول إلى الحقيقة وكشف غموض الجريمة ونسبتها إلى المتهم².

ولقد ذهب الفقه الإجرائي إلى وضع نظامين إجرائيين في مجال الإثبات الجنائي، يختلفان من حيث الأسس التي يقوم عليها كل واحد منهما وهذه الأنظمة هي:

1- النظام الأنجلوسكسوني

يطلق عليه نظام الإثبات المحدد أو نظام الأدلة القانونية، حيث أن المشرع يحدد فيه الأدلة مسبقا فلا يجوز للقاضي أن يخرج عليها، وعليه فإنه في حالة توافر الدليل على شروط حددها وقيددها المشرع يكون القاضي ملزما بتأسيس حكمه حتى وإن كان القاضي غير مقتنع بالأدلة³ المقدمة له، إذ يقوم إقتناع المشرع محل إقتناع القاضي، وهكذا فإن اليقين القانوني يقوم أساسا إفتراض صحة الدليل بغض النظر عن حقيقة أو إختلاف ظروف الدعوى⁴، لذا فإن النظم التي تتبنى هذا النظام لا يمكن لها الإعتراف بالدليل الإلكتروني بأي قيمة إثباتية ما لم ينص القانون صراحة على ذلك، ومن ثم فإنه لا قيمة للدليل الإلكتروني مهما توافرت فيه شروط اليقين ما لم ينص عليه القانون، فلا يجوز للقاضي أن يستند إليه لتكوين قناعته⁵، إن التشريعات التي تبنت النظام الأنجلوسكسوني مثل الولايات المتحدة الأمريكية، إنجلترا، كندا وجنوب إفريقيا تستلزم شروطا خاصة في الأدلة بوجه عام، ولذلك فإنه يلزم في الأدلة الإلكترونية تقديم نسخ أصلية منها مع إستدعاء القائم بتحريرها أو إذاعتها وهو ما لا يتوافر في أغلب الأحيان، ما

¹ - نور الدين بن حميدوش، مكانة الدليل الإلكتروني في الإثبات الجزائي، مجلة الدراسات والبحوث القانونية، المجلد 04، العدد 02، جانفي 2020، ص 197.

² - نعيم سعيداني، المرجع السابق، ص 223.

³ - محمد بن فردية، المرجع السابق، ص 282.

⁴ - نصر الدين مروي، المرجع السابق، ص 56.

⁵ - خالد عياد الحلبي، المرجع السابق، ص 236.

جعل هذا النظام يتعارض مع نظام الإثبات في الجرائم الإلكترونية، مما دعا إلى ضرورة قبول الدليل المستمد من الحاسب الآلي بإعتباره إستثناء على نظام الأدلة القانونية، مع إستبعادها ممن صنفوها ضمن طائفة¹ الشهادة السماعية²، وتطبيقا لذلك نص المشرع البريطاني في قانون الإثبات في المواد الجزائية على قبول الأدلة الإلكترونية وحدد قيمتها الإثباتية، وذلك على إعتبار أن بريطانيا قد تبنت هذا النظام في إطار النظم القانونية في الإثبات، كذلك الأمر في الولايات المتحدة الأمريكية حيث أقر المشرع بأن مخرجات الحاسب الآلي مقبولة وذلك بوصفها أدلة إثبات بالنسبة للبرامج والبيانات المخزنة في الحاسب الآلي وهذا ما جاء في نص المادة 716 من قانون الحاسوب لسنة 1984³، وقد قبل القضاء الإنجليزي الدليل الإلكتروني في الإثبات الجنائي على أساس أنه إستثناء من قاعدة شهادة السماع، غير أنه في الحقيقة قد قبل الدليل على أساس أنه شهادة مباشرة وهذا من خلال قضية⁴ (R.V. Wood) وقد أجابت المحكمة في هذا الإطار " أن الورقة الناتجة عن الكمبيوتر مقبولة وفقا للشرعية العامة وتصلح للإثبات."⁵

2-النظام اللاتيني

يطلق عليه بنظام الأدلة الإقناعية (نظام الإثبات الحر)، وفقا لهذا النظام يتمتع القاضي الجنائي بحرية مطلقة في إثبات الوقائع المعروضة عليه، فلا يلزمه القانون بأدلة للإستناد إليها في تكوين قناعته، فكل الأدلة متساوية في قيمتها الإثباتية في نظر المشرع، والقاضي يختار ما يراه مناسباً للوصول إلى الحقيقة، وهو في ذلك يتمتع بمطلق الحرية لقبول الدليل أو رفضه، لذلك فالقاضي يتمتع بدور إيجابي في مجال

¹ - هارون بحرية، المرجع السابق، ص10.

² - ترفض الشهادة السماعية في الإثبات الجنائي في التشريعات التي تأخذ بالنظام الأنجلوسكسوني، غير أنه قد وضعت قائمة من الاستثناءات على قاعدة شهادة السماع ومن بين هذه الاستثناءات البيانات وكذا المعلومات التي تستخرج من جهاز الحاسب الآلي، أنظر عائشة بن قارة مصطفى، المرجع السابق، ص198 .

³ - سامية بلجراف، المرجع السابق، ص688

⁴ - تدور أحداث هذه القضية حول سرقة بعض المعادن من طرف أحد الأشخاص وبعد ذلك تم ضبطها في حيازة أحد الأشخاص وأصبح متهما، وقد كانت تركيبة المواد الكيماوية لهذه المعادن مسجلة في جهاز الحاسب الآلي للمجني عليه وقد قدم الورقة المستخرجة من جهازه كدليل إثبات، فأجابت المحكمة أن الورقة المستخرجة من الحاسب الآلي للمجني عليه مقبولة وتعد كدليل إثبات وفقا للشرعية العامة، فهي ليس من قبيل الشهادة السماعية بل هي شهادة مباشرة. أنظر نادية ضريفي، عبد الوهاب دراج، سلطات القاضي الجنائي في تقدير الدليل الإلكتروني المستمد من التفتيش الجنائي، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 04، العدد 02، سنة 2019، ص126 .

⁵ - عمر محمد أبو بكر بن يونس، المرجع السابق، ص 958.

الإثبات في مقابل إنحصار دور المشرع¹، وعليه لا تثور أي مشكلة فيما يخص اعتماد الدليل الإلكتروني كوسيلة إثبات، لذلك أصبح القاضي مضطرا للتعامل مع الأدلة المستحدثة باعتبارها ضرورية وتؤدي إلى كشف أنواع جديدة من الجرائم²، فالدول المعتمدة للنظام اللاتيني³ تخضع الأدلة الإلكترونية لحرية القاضي في الإقتناع بحيث يمكن طرحها بالرغم من قطيعيتها من الناحية العلمية إذا أثبت عدم تناسبها مع ظروف وملابسات الواقعة⁴، ففي فرنسا مشكلة حجية المخرجات المتحصلة من الحاسب الآلي ليست ملحة أو عاجلة في نظر الفقهاء، فالأساس هو حرية القاضي في تقدير هذه الأدلة، فالمشرع الفرنسي أخذ بالمبدأ الموسع في قبول الأدلة بمعنى أن جميع الأدلة الإلكترونية مقبولة إلا ما استبعد بنص⁵.

3- موقف المشرع الجزائري من مسألة قبول الدليل الإلكتروني في الإثبات الجنائي

ساير المشرع الجزائري النظم اللاتينية التي تتبنى نظام الإثبات الحر في مجال الإثبات الجنائي حيث لم ينص المشرع كغيره من التشريعات التي تأخذ بهذا النظام نصوصا خاصة بقبول الدليل الإلكتروني، ما يجعلها تخضع لطرق الإثبات العامة المطبقة على قبول الأدلة، والتي تخضع إلى السلطة التقديرية للقاضي الجزائي وهذا عملا بنص المادة 212 من ق.إ.ج.ج⁶ والتي تنص على " يجوز إثبات الجرائم بأي طريق من طرق الإثبات ماعدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص، ولا يصوغ للقاضي أن يبنى قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضورا أمامه " كما نصت المادة 307 من ق.إ.ج.ج بأن "القانون لا يطلب من القضاة أن يقدموا حسابا عن الوسائل التي بها قد وصلوا إلى تكوين إقتناعهم ولا يرسم لهم قواعد بها يتعين عليهم أن يخضعوا لها على الأخص تقدير تمام أو عدم كفاية دليل ما، ولكنه يأمرهم أن يسألوا أنفسهم في صمت

¹ - خالد عياد الحلبي، المرجع السابق، ص، ص237، 238.

² - نادية ضريفي، المرجع السابق، ص 127.

³ - من أهم الدول التي تعتنق النظام اللاتيني فرنسا وألمانيا وتركيا، اليونان والبرازيل وكذا مصر، سوريا والجزائر.

⁴ - علي حسن الطوالة، مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي -دراسة مقارنة- مركز الاعلام الامني، ص بدون ترقيم منشور على الموقع www.policemc.gov.bh أطلع عليه يوم 2019/05/27، على الساعة 15:30.

⁵ - هارون بحرية، المرجع السابق، ص10.

⁶ - تقابلها المادة 427 من قانون إجراءات جزائية فرنسي والتي جاء نصها كما يلي :

ART 427du c.p.p.f dispose que « Hors les cas où la loi en dispose autrement les infractions peuvent être établies par tout mode de preuve et le juge décide d'après son intime conviction. »

وتدبر، ويبحثوا بإخلاص ضمائرهم في أي تأثير قد أحدثته في إدراكهم الأدلة المسندة إلى المتهم، وأوجه الدفاع عنها ولم يضع لهم القانون سوى هذا السؤال الذي يتضمن كل نطاق وجباتهم: هل لديكم إقتناع شخصي.¹ ويتضح من نص هذه المواد أن مبدأ حرية الإثبات يعد مبدأ عاما وإستثناء نجد المشرع أخذ بالنظام المقيد في إثبات بعض الجرائم² على سبيل الحصر.

لهذا نجد المشرع الجزائري ترك المجال مفتوحا لقبول أي دليل من شأنه إثبات الجرائم الإلكترونية بما فيها الدليل الإلكتروني، فمعظم الإجراءات الواردة في القانون 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال تدل على قبول الدليل الإلكتروني في الإثبات، حيث نص على المراقبة الإلكترونية، وحفظ المعطيات المتعلقة بحركة السير، وإلزام مقدمو الخدمات بحفظ وتسجيل معطيات زبائنهم، كذلك النص على كيفية تفتيش المنظومة المعلوماتية وحجز المعطيات المفيدة في كشف الجرائم أو مرتكبيها بعد أن يتم نسخ المعطيات على دعامة تخزينها وحرزها وهي شكل من أشكال الأدلة الإلكترونية، فالمشرع هنا يقصد الأدلة الإلكترونية إلا أنه لم يسميها إلا أنه يحرص على حجزها في احسن الظروف لتقديمها امام الجهات القضائية كأدلة إثبات³، كذلك الإستعانة بكل شخص له مؤهلات لمساعدة الجهات القضائية المختصة.

بالإضافة إلى وجود أحكام وقرارات تدل على أن القضاء الجزائري قد اعتمد على الدليل الإلكتروني كأساس لإصدار أحكامه، وذلك من خلال قبوله إعتداد الآليات المستحدثة في إجراءات البحث والتحري عن الدليل في الجريمة الإلكترونية، وقبول مستخرجات الحاسب الآلي والاستئناس بالخبرة التقنية المنجزة على الحواسيب والأقراص الصلبة لإستخراج الدليل، وهو يدعونا إلى القول بأن الدليل الإلكتروني مكرسا في القضاء الجزائري.⁴

ومن هنا يمكن القول أنه رغم ما يتمتع به الدليل الإلكتروني من مصداقية في نقل الوقائع إلا أنه

¹ - وقد أكدت المحكمة العليا في إحدى قراراتها أنه "يمكن لقاضي الموضوع تأسيس إقتناعه الوجداني على أية حجة حصلت مناقشتها أمامه." ونفس الشيء ذهبت إليه محكمة النقض الفرنسية حيث أقرت "من حق القضاة ان يقدروا بكل حرية قيمة عناصر الإثبات التي طرحت في المداولة والتي يستند عليها اقتناعهم أنظر محمد مروان، نظام الإثبات في المواد الجنائية في القانون الوصفي الجزائري، الجزء الثاني، ديوان المطبوعات الجامعية، الجزائر، ط 1999، ص 471.

² - أنظر المادتين 339، 341 من قانون العقوبات الجزائري.

³ - هارون بحرية، المرجع السابق، ص 11.

⁴ - عبد القادر عمير، المرجع السابق، ص 170.

يبقى يخضع للسلطة التقديرية للقاضي، وهو المخول بقبول الدليل أو رفضه وتقدير حجيته حيث تقوم السلطة التقديرية للقاضي بتحويل الحقيقة العلمية إلى حقيقة قضائية.¹

ثانيا: الإقتناع الذاتي للقاضي الجزائي لقبول الدليل الإلكتروني

يقوم الإثبات في المواد الجزائية على مبدأ الإقتناع القضائي، ويعني هذا المبدأ السماح للقاضي بقبول جميع الأدلة المقدمة إليه من أطراف الدعوى وتقديرها بكل حرية، فيكون له الأخذ بما يطمئن إليه منها وإستبعاد ما دون ذلك وتقدير قيمة كل دليل على حدة والتنسيق بين الأدلة التي قدمت إليه، وإستخلاص نتيجة منطقية في تقرير البراءة أو الإدانة² وبالرجوع إلى نص المادة 212 من ق.إ.ج.ج نجد أن المشرع الجزائري أقر مبدأين هامين متلازمين في مجال الإثبات الجنائي وهما مبدأ حرية الإثبات ومبدأ الإقتناع الحر للقاضي الجزائي بالدليل المطروح عليه في جلسة المحاكمة، فإذا كان الدليل الإلكتروني ذو الطبيعة العلمية هو الأنسب في إثبات الجريمة الإلكترونية فما مدى إمكانية إعمال القاضي الجزائي لمبدأ الإقتناع الشخصي حيال هذا الدليل.³

1- مفهوم الإقتناع الشخصي للقاضي الجزائي

إن الإقتناع الشخصي للقاضي الجزائي هو عبارة عن نشاط عقلي، لا يتدخل المشرع ليبين للقاضي كيفية ممارسته وترجمته إلى واقع منتج، ولا يرسم له كيف يشكل معادلاته الذهنية في مجال تقدير الأدلة ليصل من خلالها إلى الحقيقة.

أ: تعريف مبدأ الإقتناع الذاتي (الشخصي)

لقد اختلف فقهاء القانون الجنائي في تعريف الإقتناع فمنهم من عرفه بأنه " التقدير الحر المسبب لعناصر الإثبات في الدعوى وهو البديل عن نظام الأدلة القانونية "⁴ وعرف كذلك بأنه " الإيمان العميق والركون إلى صحة الوقائع التي تقدمها الأطراف المتنازعة الذي يخلف في نفس القضاة الجزائي أثرا

¹ - سامية بلجراف، المرجع السابق، ص 691.

² - محمود نجيب حسني، شرع قانون الإجراءات الجنائية، د.د.ن، ط2، 1988، ص412.

³ - نعيم سعيداني، المرجع السابق، ص226.

⁴ - محمود محمود مصطفى، الإثبات في المواد الجنائية في القانون المقارن الجزء الاول، مطبعة جامعة القاهرة، ط2، 1977، ص95.

عميقا يجعله يصدر حكمه عن قناعة وجدانية وإحساس كبير بإصابته الحقيقة في حكمه.¹

ب- وسائل تكوين الإقتناع الشخصي للقاضي الجزائي

إن الجهد الإستنباطي الذي يبذله القاضي من خلال نشاطه العقلي المكون لقناعاته والذي ينصرف إلى فرز الحقيقة من الدليل محل تقديره يتبع فيه القاضي ثلاث طرق هي:

- قبول القاضي جميع الأدلة المطروحة أمامه في جلسة المحاكمة، إذ لا يمنع على القاضي قبول دليل أو يفرض عليه دليلا، كما أنه لا يتقيد في ذلك إلا بقيد مشروعية إجراءات تحصيل الدليل أو طرحه للمناقشة العلنية في الجلسة.

- أن يقوم القاضي بموازنة كل دليل على حدة بمعزل عن باقي الأدلة المطروحة أمامه ويقدر قيمته التدليلية وقوته الثبوتية بالنظر إلى ما يعبر عنه من حقيقة.

- أن يقوم القاضي بتنسيق كافة الأدلة المعروضة عليه من خلال التحقيق والتمحيص والتأكد من انها متسادة تشد بعضها البعض وليست متعارضة.²

2- الضوابط المتعلقة بالإقتناع الشخصي للقاضي الجزائي

يسعى القاضي الجنائي للوصول إلى الحقيقة الواقعية، ويسخر في سبيل ذلك نشاطه وجهده الذهني، قصد الوقوف على الوقائع كما حدثت، فإذا إستقرت لديه تلك الحقيقة إرتاح ضميره للصورة الذهنية التي تكونت لديه، يمكننا القول عندئذ أن القاضي قد وصل إلى حالة الإقتناع³ ويتقيد القاضي عند تكوين عقيدته بأي دليل جنائي بما فيها الدليل الإلكتروني بالضوابط التالية:

أ- بلوغ الاقتناع القضائي درجة اليقين

تبنى الأحكام الجزائية على الجزم واليقين⁴ لا الظن والإحتمال، ففي حالة الشك على المحكمة أن تقضي ببراءة المتهم، لأن الأصل في الإنسان البراءة، وإذا كان من المسلم به فقها وقضاء أن القاضي لا يبني إقتناعه إلا على الجزم واليقين وعلى أدلة ذات دلالة قوية في حجيتها، فإن الوصول إلى اليقين

¹ - سيد محمد حسن الشريف، النظرية العامة للإثبات الجنائي، دار النهضة العربية، القاهرة، د ط، 2002، ص28.

² - جمال إبراهيمي، المرجع السابق، ص173

³ - أحمد بن مالك، أثر الإثبات بالأدلة العلمية الحديثة على الاقتناع الشخصي للقاضي الجزائي بها، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد 10، العدد 01، 2021، ص437.

⁴ - يعرف اليقين لغة هو العلم وزوال الشك وعدم وجود أدنى ريب، أما في الإصطلاح فقد عرفها الفقهاء بأنه اعتقاد القاضي بأن ما وصل إليه هو الحقيقة، أو هو حالة ذهنية وعقلية تؤكد وجود الحقيقة. أنظر في ذلك عائشة بن قارة مصطفى، المرجع السابق، ص180 .

المطلق لا يمكن تحقيقه إلا في المسائل الحسابية¹، ومن هذا المنطلق يمكن لنا القول بأن الأدلة الإلكترونية الصحيحة، المشروعة باعتبارها أدلة علمية قاطعة فإنها تجعل من الإقتناع القضائي يبلغ درجة اليقين بشأن الحقيقة العلمية الواقعية للدليل الإلكتروني لكن على شرط معرفي.

فالقاضي يصل إلى يقينية الأدلة الإلكترونية المجسدة بمخرجات الحاسب الآلي، حيث تتطلب نوعين من المعرفة أولهما المعرفة الحسية التي تدركها الحواس، من خلال معاينة هذه المخرجات وتفحصها وثانيهما المعرفة العقلية عن طريق التحليل والإستنتاج من خلال الربط بين هذه المخرجات والملابسات التي أحاطت بها²، إضافة إلى ذلك فإنه في نطاق الجزم بوقوع جرائم إلكترونية ونسبتها إلى المتهم يستدعي نوع آخر من المعرفة ألا وهي المعرفة العلمية في مجال المعلوماتية³ ولاسيما أن القاضي يلعب دورا كبيرا في إثبات الجرائم، وقد يؤدي الجهل في بعض الأحيان إلى التشكيك في قيمة الدليل الإلكتروني ومن ثم يقضي بالبراءة، إستنادا إلى قاعدة الشك يفسر في مصلحة المتهم، وهذا ما يؤدي إلى إفلات المتهم من تطبيق القانون.

ب-عدم مخالفة الإقتناع القضائي مقتضيات العقل والمنطق

يستند القاضي الجزائي في بناء قناعته إلى أدلة رقمية مشروعة، ومن قرائن محيطة بها بالدليل الإلكتروني يثبت حقائق علمية قاطعة، لا يمكن تجاهلها حيث تتماشى مع العقل، فالمحكمة لا تحل بنفسها محل الخبير المعلوماتي لإبداء رأي فني خالص، ولا بد لها أن تستند إلى مبدأ تساند الأدلة من أجل الوصول إلى الحقيقة العلمية وأن تسعى إلى عدم الإعتماد على الدلائل وتستبعد الدليل الحاسم الرقمي، كل ذلك في إطار منطقي سليم متواءم مع منطق العقل والعدالة المنشودة.⁴

مجمل القول أن الدليل الإلكتروني فرض نفسه كأدلة إثبات جديدة يدخل في نطاق الأدلة العلمية، وبالرغم من الخصائص العلمية الثابتة التي يتميز بها، إلا أنه لا يختلف عن الدليل التقليدي، إذ يمكن أن يكون دليل إدانة أو دليل براءة، وبذلك فهو يخضع للسلطة التقديرية للقاضي الجزائي وتحويله من حقيقة علمية إلى حقيقة قضائية.

¹ - أحمد بن مالك، المرجع السابق، ص 437.

² - هارون بحرية، المرجع السابق، ص 16.

³ رشيد بوكر، المرجع السابق، 518 .

⁴ - هارون بحرية، المرجع السابق، 16 .

الفصل الثاني: مواجهة الجريمة الإلكترونية وفقا للقانون 04/09

فبعد أن رأينا في الباب الأول من هذه الدراسة أن وسائل وأساليب الكشف الكلاسيكية أو التقليدية غير قادرة على مواجهة الجريمة الإلكترونية، والصعوبات التي تعتريها بادر المشرع الجزائري في توجيه سياسته الجنائية في إيجاد وسائل كفيلة لمواجهة الإجرام المعلوماتي، فأصدر القانون رقم 04-09 المؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، فمعظم قواعده إستقاها المشرع من إتفاقية بودابست المتعلقة بمكافحة الجريمة الإلكترونية لسنة 2001 الصادرة عن المجلس الأوروبي، القانون رقم 04-09 جاء مكملًا لقانون العقوبات في مجال مكافحة الجريمة الإلكترونية، وكذا للنقص الذي اعتري قانون الإجراءات الجزائية في مواجهة هذه الجريمة ، حيث إحتوى على قواعد للوقاية من الجرائم الإلكترونية ودعم وسائل مكافحتها ،من خلال وضع ترتيبات تسمح برصدها المبكر وجمع أدلة عنها كإجراء المراقبة الإلكترونية، التفتيش عن بعد، أنشأهيئة وطنية مهمتها الوقاية من خطورة هذه الجرائم، وكذلك نظرا لإعتبار الجريمة الإلكترونية صورة من صور الجريمة العابرة للحدود الوطنية فهل للتعاون الدولي سواء القضائي أو الأمني، ضرورة حتمية لمواجهة والتصدي لهذا النوع المستحدث من الإجرام؟

المبحث الأول: الإجراءات المستحدثة للوقاية من الجريمة الإلكترونية

إن الإجراءات التقليدية الواردة في قانون الإجراءات الجزائية تبين عجزها عن مواجهة هذه الجريمة، فجاء القانون 04-09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، بقواعد تتلاءم وطبيعة الجريمة، فمن جهة جاء بإجراءات وقائية التي تسمح للرصد المبكر للاعتداءات المحتملة الوقوع والتعرف على مرتكبها ومن بينها المراقبة الإلكترونية (المطلب الأول)، كما نظم إجراءات التفتيش عن بعد عن طريق الدخول لمنظومة معلوماتية (المطلب الثاني)، وفرض إلتزامات على مقدمي الخدمات لمساعدة السلطات القضائية المختصة (المطلب الثالث)، ثم أسند مهمة الوقاية من الجرائم الإلكترونية للهيئة الوطنية في (المطلب الرابع).

المطلب الأول: المراقبة الإلكترونية كإجراء للوقاية من الجريمة الإلكترونية

بالرغم من إنتشار وتطور وتعدد وسائل الأمن التقنية لحماية ووقاية المعطيات والمعلومات في العالم الافتراضي، حيث تعتبر حماية مبكرة من الإعتداءات المحتملة لعمليات الإختراق كتقنية التشفير، الجدران النارية، التوقيع الإلكتروني، إلا أن تلك الوسائل الأمنية أضحت غير كافية لمواجهة هذه الإعتداءات المجرمة ومن هنا ظهرت الحاجة لإستحداث إطار قانوني يسمح للرصد المبكر لهذه الإعتداءات المحتملة، وتعتبر المراقبة الإلكترونية إجراء وقائي لمنع المخططات الإجرامية، كما تتخذ كإجراء من إجراءات البحث والتحري أو في إطار المساعدة القضائية الدولية¹، وقد نص المشرع الجزائري على إجراء المراقبة الإلكترونية بموجب المادة 3 من القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، فمن خلال هذا المطلب نتطرق إلى مفهوم المراقبة الإلكترونية (الفرع الأول) وحالات حصر اللجوء إلى هذا الإجراء (الفرع الثاني) الضمانات المقررة لتنفيذه في (فرع ثالث).

الفرع الأول: مفهوم المراقبة الإلكترونية

تعتبر المراقبة الإلكترونية من الإجراءات المستحدثة ظهرت للوجود ببروز الجرائم الإلكترونية، تم إستحداثها بموجب القانون 04-09 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

أولا: تعريف المراقبة الإلكترونية

استخدمت عدة مصطلحات للدلالة على المراقبة الإلكترونية منها الإعتراض²، الإنقاط والمراقبة الإلكترونية، لم يتطرق المشرع الجزائري شأنه في ذلك شأن أغلب التشريعات إلى وضع تعريف للمراقبة الإلكترونية سواء في قانون الإجراءات الجزائية، ولا في مواد قانون 04-09 المتعلقة بالقواعد الخاصة

¹ - شريفة سوماتي، السياسة الجنائية للمشرع الجزائري في مواجهة الجريمة المستحدثة، أطروحة لنيل شهادة دكتوراه علوم، كلية الحقوق، جامعة الجزائر 01، الجزائر، 2017-2018، ص99.

² - استعملت إتفاقية بودابست لسنة 2001 مصطلح "الإعتراض" في المادة 21 من الإتفاقية، بينما المشرع الجزائري تبنى مصطلح المراقبة الإلكترونية بالرغم أن معظم أحكام القانون 04-09 مستمد من هذه الإتفاقية، بينما نظم الإعتراض في المادة 65 مكرر من قانون الإجراءات الجزائية الذي يخص الإتصالات السلكية واللاسلكية، أما المراقبة الإلكترونية فهي خاصة بالجرائم الإلكترونية.

للقااية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال، مكتف في ذلك بتحديد مفهوم الإتصالات الإلكترونية فعرفها بأنها " أي تراسل أو إرسال أو إستقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية".¹

وترك أمر ذلك للفقهاء للتصدي لهذه المهمة، الذي إختلف هو الآخر في ضبط تعريف دقيق لإجراء المراقبة الإلكترونية، فعرفها بعض الفقهاء بأنها " إجراء يعتمد فيه الإتصالات والتسجيل ومحلها المحادثات الخاصة سواء أكانت مباشرة أو غير مباشرة، أي سواء كانت مما يتبادلها الناس من مواجهة بعضهم البعض أو عن طريق وسائل الإتصال السلكية واللاسلكية".²، كما عرفت أيضا " وضع شخص أو مكان أو حديث تليفوني تحت ملاحظة ونظر رجال الضبطية القضائية لتسجيل كل ما عسى أن يحدث من تصرفات غير قانونية، قد تقع من الأفراد ويكون من شأنها أن تخل بالأمن أو النظام العام في المجتمع، أو تحول الخطر إلى ضرر وذلك بطريقة غير محسوسة وفي جو من السرية والكتمان".³، كما يقصد بهامراقبة شبكة الإتصالات، أو ذلك العمل الذي يقوم به المراقب بإستخدام التقنية الإلكترونية لجمع البيانات والمعلومات حول المشتبه فيه، سواء كان شخصا أو مكانا أو شيئا، حسب طبيعته وذلك مرتبط بالزمن لتحقيق غرض أمني أو لأي غرض آخر.⁴

إذا فإن إجراء المراقبة الإلكترونية من إجراءات جمع الدليل في الشكل الإلكتروني، عن المشتبه فيه فمحلها مراقبة الحاسوب أو المواقع عبر الأنترنت، أو البريد الإلكتروني بما يحويه من مراسلات إلكترونية وحلقات نقاش، وغرف الدردشة، أو الهاتف النقال المتصل بشبكة الأنترنت، حتى ساعة اليد الذكية واللوح الرقمي.⁵

¹ - المادة 2 من القانون 04-09 / المادة 5 من المرسوم الرئاسي 15-162 وكذا المادة 10 من القانون 04-18 المؤرخ في 10/05/2018، يحدد القواعد العامة المتعلقة بالبريد والإتصالات الإلكترونية، الجريدة الرسمية للجمهورية الجزائرية، عدد 27، صادرة بتاريخ 13/05/2018 .

² - عوض محمد عوض، المبادئ العامة في قانون الإجراءات الجنائية، دار المطبوعات الجامعية، الإسكندرية مصر، 1999 ص 404.

³ - مصطفى محمد الدغدي، التحريات والإثبات الجنائي، دار الكتب القانونية، المحلى الكبرى، 2006، 218.

⁴ - مصطفى محمد موسى، المراقبة الإلكترونية عبر شبكة الأنترنت - دراسة مقارنة بين المراقبة الأمنية التقليدية والإلكترونية، الكتاب الخامس - دار الكتب والوثائق القومية المصرية، القاهرة، ط1، 2003، ص 192.

⁵ - دلال مولاي ملياني، المرجع السابق، ص 209.

وقد سلك المشرع الجزائري نفس الإتجاه الذي سلكته إتفاقية بودابست لسنة 2001، إذ ميز بين البيانات المتعلقة بحركة السير معطيات المرور، والمعطيات المتعلقة بمحتوى المرور نص على هذه الأخيرة في المادة 4 من قانون 04-09 أما الأولى فعرفها بموجب المادة 02 من نفس القانون وخصها بإجراءات وردت في المادة 11 من ذات القانون.

وقد نص المشرع الجزائري على إجراء المراقبة الإلكترونية في القانون 04-09، ليس كإجراء فقط تقتضيه التحريات والتحقيقات القضائية مثلما ما هو في قواعد قانون الإجراءات الجزائية، وإنما اعتبره إجراء وقائي من جرائم يمكن أن تشكل خطرا على أمن الدولة والنظام العام والدفاع الوطني، والتي تصنف عادة في خانة الجرائم الإرهابية، حيث نصت المادة 03 من ذات القانون على " مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والإتصالات، يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات والتحقيقات القضائية الجارية، وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الإتصالات وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية".¹

وعليه تعتبر المراقبة الإلكترونية إجراء إستثنائي لمساسه بالحق في سرية المراسلات بكافة أشكالها، كما أجازته في حالة وجود معلومات كافية عن إحتمال وقوع إعتداء على منظومة معلوماتية، على نحو يهدد النظام العام، أو الدفاع الوطني، أو مؤسسات الدولة أو الإقتصاد الوطني وهذا ما نصت عليه المادة 4 فقرة ب من قانون 04-09.²

¹ - وهذا ما أكدته المادة 21 من إتفاقية بودابست تحت "عنوان بيانات المحتوى" "يجب على كل طرف أن يتبنى الاجراءات التشريعية آية إجراءات أخرى يرى أنها ضرورية من أجل تخويل سلطاته المختصة سلطة فيما يتعلق بالجرائم الخطيرة التي يحددها القانون الداخلي الممكنات التالية :

P - جمع أو تسجيل عن طريق تطبيق الوسائل الفنية المتواجدة على أرضه

ب - الزام مقدم الخدمات في نطاق قدراته الفنية المتوافر على :

1 - على أن يجمع أو يسجل عن طريق وسائل فنية موجودة على أرضه أو

2 - أن يمنح السلطات المختصة عونه ومساعدته من أجل تجميع أو تسجيل، وفي الوقت الفعلي، المعطيات المتعلقة بمحتوى اتصالات معينة على أرضه، منقولة عن طريق نظام معلوماتي. " أنظر عبد اللاه أحمد هلال، إتفاقية بودابست لمكافحة جرائم المعلوماتية معلقا عليها، المرجع السابق، ص 287.

² - المادة 4 فقرة ب من قانون رقم 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها.

ثانيا: الطبيعة القانونية للمراقبة الإلكترونية

إختلف الفقه في تحديد الطبيعة القانونية لإجراء المراقبة الإلكترونية، فإنقسموا في ذلك إلى عدة اتجاهات.¹

1 - مراقبة الاتصالات الإلكترونية نوع من التفتيش

يرى أنصار هذا الاتجاه أن المراقبة الإلكترونية هي نوع من التفتيش، وذلك أن مراقبة الاتصالات الإلكترونية كالتفتيش يشكل إنتهاكا لحرمة الحياة الخاصة للإنسان، وبالتالي يخضع لشروط وضمانات التفتيش، فالتفتيش هو الإطلاع على محل له حرمة خاصة للكشف عن ما يفيد في إظهار الحقيقة، ويسوي أصحاب هذا الاتجاه أن الأشياء المضبوطة كضبط رسالة، أو محادثة تليفونية أو إلكترونية، تفيد في كشف الحقيقة.

2 - مراقبة الاتصالات الإلكترونية نوع من الإطلاع على الرسائل

يرى هذا الاتجاه أن مراقبة الاتصالات الإلكترونية نوع من أنواع الإطلاع على الرسائل، لما في ذلك من إطلاع على أسرار الحياة الخاصة التي يفترض حمايتها وعدم إنتهاكها، وتعرض هذا الرأي للانتقاد بإعتبار أن الرسالة مستند مثبت للتهمة، ويقدم ضمانات للمتهم أما الاتصالات الإلكترونية فلا تتمتع بهذه الصفة المادية.

3 - مراقبة الاتصالات الإلكترونية إجراء خاص

إتجه هذا الرأي إلى إعتبار المراقبة الإلكترونية إجراء ذو طبيعة خاصة، فهو يشبه التفتيش لكنه ليس تفتيشا، وهو يهدف إلى ضبط الأدلة التي تكشف الحقيقة في جريمة وقعت وجاري التحقيق فيها، لأنها كذلك ترد على البيانات الإلكترونية المتحركة وهي الاتصالات الإلكترونية حال إجراءها، دون تلك التي إنتهت وخزنت، وبالتالي لا يمكن ضبطها لأنها عبارة عن نبضات إلكترونية، داخل أسلاك، بينما التفتيش في الجرائم الإلكترونية يرد على بيانات ساكنة أو مخزنة.²

¹ - سامي جلال فقي حسين، التفتيش في الجرائم المعلوماتية -دراسة تحليلية -، دار الكتب القانونية، القاهرة، ط1، 2011، ص، ص 286 - 287.

² - عبد القادر عمير، المرجع السابق، ص 279.

وباستقراء هذه الآراء، نجد أن المشرع الجزائري إعتبر إجراء المراقبة الإلكترونية مستقلا عن إجراء التفتيش المنظومة المعلوماتية لكونه، نظم كل إجراء بنصوص قانونية مستقلة عن بعضها البعض.

الفرع الثاني: حصر حالات اللجوء للمراقبة الإلكترونية

نص القانون 04-09 بموجب المادة 4، على الحالات التي تسمح باللجوء إلى المراقبة الإلكترونية أو دخول منظومة معلوماتية، بغرض التفتيش وهي الحالات التي جاءت على سبل الحصر متمثلة في:

أولا: الوقاية من ارتكاب الأفعال الموصوفة بجرائم الإرهاب والتخريب أو الجرائم الماسة بأمن

الدولة

نظرا لإرتباط المجتمعات العالمية فيما بينها بنظم معلومات تقنية عبر شبكات الإتصال العالمية، إزدادت الخطورة الإجرامية للجماعات والمنظمات الإرهابية، فقامت بتوظيف طاقتها للاستفادة من تلك التقنية وإستغلالها في عملياتها الإجرامية وأغراضها غير المشروعة¹، كإختراق الأنظمة والشبكات المعلوماتية وإستخدامها في تحقيق أغراضها الإجرامية، أو للدعوة لمبادئهم المنحرفة، ولإبراز قوة التنظيم الإرهابي، أو إنشاء مواقع إرهابية لبيان كيفية صناعة القنابل والمتفجرات²، فإن ظهور جرائم الإرهاب الإلكتروني تولد عنه زيادة في نشاط المراقبة الإلكترونية للأفراد عبر الشبكات، بدعوى الوقاية ومكافحة هذا النوع من الجرائم الإلكترونية³، فأجاز المشرع المراقبة المسبقة للاتصالات الإلكترونية بمجرد توافر شكوك إحتمال وقوع لجرائم إرهابية أو تخريبية أو الجرائم الماسة بأمن الدولة، فالوقاية لا تفرض القيام بأعمال تحضيرية لارتكاب هذه الأفعال وإنما مجرد تكهنات أو حتى دلائل بسيطة قد توحى بأن هؤلاء الأشخاص يمكنهم ارتكاب تلك الأفعال⁴.

ثانيا: حالة توافر معلومات عن احتمال إعتداء على منظومة معلوماتية على نحو يهدد النظام

العام أو الدفاع الوطني أو مؤسسات الدولة أو الإقتصاد الوطني

يمكن اللجوء إلى إجراء المراقبة الإلكترونية، كإجراء وقائي بمجرد توافر معلومات عن إحتمال وقوع

¹ - رفد عيادة الهاشمي، الإرهاب الإلكتروني، د ر للنشر، د ط د س ص 5.

² - علي عدنان الفيل، المرجع السابق، ص 82.

³ - حسين ربيعي، المراقبة الإلكترونية وحق الفرد في الخصوصية داخل الفضاء الرقمي، المرجع السابق، ص 410.

⁴ - مريم أحمد مسعود، آليات مكافحة جرائم تكنولوجيا الإعلام والإتصال في ضوء القانون رقم 04/09 مذكرة لنيل شهادة الماجستير، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، 213، ص 82.

جريمة تمس المصالح السابقة، مما يجعل من إجراء المراقبة الإلكترونية فعلا مشروعا، سواء كانت تلك المعلومات تتوافر عليها السلطات بذاتها، أو عن طريق تلقي شكاوي أو بلاغات من المواطنين، وفي هذه الحالة إشتراط المشرع أن تتوافر معلومات عن احتمال إعتداء على المنظومة المعلوماتية تمس المصالح السابقة، ولم يكتف بمجرد الشك.¹

ثالثا: مقتضيات التحريات والتحقيقات القضائية من الصعب الوصول إلى نتيجة دون اللجوء إلى المراقبة الإلكترونية

في هذه الحالة لا يعتبر إجراء المراقبة الإلكترونية إجراء وقائيا، وإنما يتخذ أثناء مرحلة جمع الإستدلالات أو التحقيق القضائي، والغرض منه الوصول إلى مرتكبي الجرائم في حالة عدم التمكن من الوصول إلى الحقيقة وفق الإجراءات التقليدية، وبإستقراء المادة 4 من قانون 09-04 يتبين أنها لم تحدد الجرائم المقصودة، مما يستدعي أنها تطبق على كافة جرائم القانون العام، بما فيها الجرائم الإلكترونية، مما يعني إمكانية اللجوء في كل قضية مستعصية إلى المراقبة الإلكترونية فيؤدي إلى تعميم إستخدام الآلية دون حد.²

رابعا: في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة

ويدخل في إطار التعاون الدولي للحد من الجرائم العابرة للحدود الوطنية، خاصة بإعتبار الجرائم الإلكترونية إحدى صورها ولخصوصية الجريمة الإلكترونية وصعوبة إكتشافها، وصعوبة إستخلاص الدليل الإلكتروني يتم ذلك في إطار تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بهذا النوع من الجرائم ويكون في إطار الإتفاقيات الدولية ومبدأ المعاملة بالمثل.

ونظرا لخطورة هذا الإجراء على حق الشخص في الخصوصية وما يتفرع عنها من حرية المراسلات وسرية الأحاديث الخاصة، لهذا أحاط المشرع هذه الإباحة ببعض الضمانات القانونية لحماية حق الإنسان في سرية إتصالاته بمختلف أنواعها وهذا ما سوف نتناوله فيما يلي:

¹ - فطيمة جبار، مراقبة الإتصالات الإلكترونية بين الحظر والإباحة في التشريع الجزائري، مجلة الدراسات القانونية المقارنة ن المجلد 2، العدد 2، 2016، ص 18.

² - آمنة محمد ي بوزينة، إجراءات التحري الخاصة في مجال الجرائم المعلوماتية دراسة تحليلية لأحكام قانون الإجراءات الجزائية وقانون الوقاية من جرائم الإعلام، ورقة علمية في إطار الملتقى الوطني حول آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، مركز جيل البحث العلمي، لجزائر، 29 مارس 2017، ص 74.

الفرع الثالث: الضمانات المقررة لتنفيذ المراقبة الإلكترونية وكيفية إجرائها

أولا: الضمانات المقررة لتنفيذ المراقبة الإلكترونية

أباح المشرع عملية مراقبة الاتصالات الإلكترونية، لكن قيد اللجوء إليها ضمن ضوابط أو ضمانات قانونية إقتضتها ضرورة الوقاية من بعض الجرائم، التي جاءت على سبيل الحصر فيما تتمثل هذه والقيود والتي ندرجها كما يلي:

1 -الحصول على إذن من السلطة القضائية المختصة

نص القانون 09 - 04 في الفقرة 2 من المادة 4 أنه "لا يجوز إجراء عمليات المراقبة الإلكترونية إلا بإذن مكتوب من السلطة القضائية المختصة"، المتمثلة في وكيل الجمهورية قبل فتح تحقيق، أو قاض التحقيق في حالة فتح تحقيق قضائي، إذن فالسلطة القضائية تعد ضمانة لازمة لمشروعية الاعتراض على الاتصالات الإلكترونية، فالإذن الممنوح من السلطة القضائية يكون وفق القواعد المنصوص عليها في قانون الإجراءات الجزائية.

كما تطرق المشرع الجزائري إلى حالة خاصة منصوص عليها في القانون 09 - 04 بمقتضى المادة 3/4 فإن النائب العام لدى مجلس قضاء الجزائر، يختص بمنح ضباط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، إذن لمدة ستة أشهر قابلة للتجديد وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة، والأغراض الموجهة لها، وهذا عندما يتعلق الأمر بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.¹

وعليه لا يتم القيام بمراقبة الاتصالات الإلكترونية إلا بإذن مكتوب من السلطات القضائية المختصة، غير أن ما يلاحظ أن المشرع لم يحدد مدة الإذن للقيام بعملية المراقبة، مكتفيا فقط بتحديد مدة الإذن الممنوح من طرف النائب العام لدي مجلس قضاء الجزائر ب6 أشهر قابلة للتحديد، في حالة الوقاية من الأفعال الموصوفة بجرائم الإرهاب، أو التخريب أو الجرائم الماسة بأمن الدولة، أما الإذن الممنوح في الحالات الأخرى الواردة في المادة 4 من قانون 09-04، فهي خاضعة لأحكام قانون الإجراءات الجزائية

¹ - المادة 6/4 من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

والمحددة بالمواد 65 مكرر 5 وما يليها طبقا لنص المادة 3 من القانون 04-09.

2- أن تكون ثمة ضرورة تدعو إليه

بالرجوع إلى نص المادة 4 من القانون 04-09، أن ضابط الوقاية من وقوع بعض الجرائم يعتبر السند الشرعي والمبرر الوحيد للقيام بمراقبة الاتصالات الإلكترونية، ومن قبيل ذلك أن تكون هناك معلومات كافية تنذر بإحتمال إعتداء على منظومة معلوماتية، على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة، أو لمقتضيات التحريات أو التحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.

3 - إستخدام هذا الإجراء ضمن نطاق ضيق

لقد حدد المشرع الحالات التي يجوز فيها مراقبة الاتصالات الإلكترونية، وقد ذكرها على سبيل الحصر، محاولة منه من إنشاء موازنة بين حق المجتمع في الأمن ومنع الجريمة، حق الفرد في السرية والخصوصية، حتى لا يتم الإخلال بالأحكام القانونية التي تضمن سرية المراسلات والاتصالات في حالة ما إذا تركت الحرية لرجال الضبطية في مراقبة الاتصالات الإلكترونية.

ثانيا: كيفية القيام بإجراء المراقبة الإلكترونية للاتصالات

تتم عملية المراقبة الإلكترونية عبر مراحل تتمثل في:

1 - وضع الترتيبات التقنية اللازمة

لم تحدد وسائل المراقبة الإلكترونية الواردة في المادة 4 من قانون 04-09، وإنما اكتفى المشرع بما ذكره من ضرورة لوضع الترتيبات التقنية الخاصة بالمراقبة.

إن التقنية المستعملة في مراقبة الاتصالات الإلكترونية، هي التقنية الإلكترونية والتي تعني " مجموعة الأجهزة المتكاملة مع بعضها البعض بغرض تشغيل مجموعة من البيانات الداخلية، وفق لبرنامج موضوع مسبقا للحصول على النتائج المطلوبة." ¹

¹ - مصطفى محمد موسى، المرجع السابق، ص 205.

ويعد أسلوب كارنيفور¹ carnivore من أكثر الأساليب لمراقبة البريد الإلكتروني²، وهو برنامج طورته إدارة تكنولوجيا المعلومات التابعة لمكتب التحقيقات الفيدرالي الأمريكي، وتتحصر مهمته في تعقب وفحص رسائل البريد المرسل، أو الواردة عبر أي جهاز حاسوب خادم، يحمل معلومات عن جرائم أو حوادث جنائية³، ولا يتم تنفيذ هذه العملية إلا بعد أخذ الإذن من المحكمة المختصة بوضع أجهزة تلك الشركة تحت المراقبة، وأثار هذا البرنامج جدلا واسعا بين أوساط المدافعين عن الحقوق والحريات الشخصية، وذلك أن إعداد برمجيات تتولى بذاتها البحث عن الجرائم ومرتكبيها مثل برمجة كارنيفور، أمر لا يتوافق مع الضمانات الدستورية المعاصرة، لما يشكله مثل هذا الإجراء من عدوان على الحق في الخصوصية والذي يعد أقوى مظاهر الحقوق الدستورية الفردية⁴، ويتم تنفيذ المراقبة الإلكترونية من خلال إستهداف الاتصالات التي يجريها المشتبه فيه من خلال إستعماله لأي وسيلة إلكترونية، إما في شكل تراسل أو إرسال أو إستقبال علامات، أو إشارات أو كتابات، أو صور أو معلومات، أي كانت طبيعتها تمت عن طريق وسيلة إلكترونية⁵، وتقوم الجهة المختصة بهذا الإجراء الممثلة في الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، بوضع الترتيبات التقنية اللازمة الموضوعة لأغراض المراقبة الإلكترونية موجهة حصريا، لتجميع وتسجيل معطيات ذات صلة بالحالات الواردة على سبيل الحصر السالفة الذكر على غرار الأفعال الإرهابية وأي جرائم خطيرة، أما عن التقنيات التكنولوجية التي يمكن أن تستعمل في إطار المراقبة الإلكترونية، فهي تتمثل في إعتراض المراسلات الإلكترونية، تسجيل الأصوات والنقاط الصور، تفتيش المنظومات المعلوماتية وحجزها المادة 5 و7 من القانون 04-09⁶.

¹ - كلمة carnivore كلمة إنجليزية الأصل تعني آكل اللحوم، في إشارة إلى أن هذا البرنامج يقوم بتصفح كافة البيانات المندفعة عبر الشبكة ويلتهم المعلومات كآكل اللحوم.

² - " تقنية مراقبة البريد الإلكتروني": هو برنامج صممه الأمريكي ريتشارد داتوني من أجل سير محتوى البريد الإلكتروني موضوع المراقبة وقراءة الرسائل التي قام صاحبها التي قام صاحبها بإتلافها، أو تلك لم يتم بتخزينها أساسا، ولقد أستخدمت من أجهزة الإستخبارات الأمريكية هذا البرنامج لكشف مشتبه فيه من الجنسية الروسية حاول إختراق مواقع على شبكة الأنترنت، أنظر هبة بيلة هروال، الجوانب الإجرائية لجرائم الأنترنت، المرجع السابق، ص 203.

³ - سامي جلال فقي حسين، المرجع السابق، ص 297.

⁴ - رشيدة بوكري، المرجع السابق، ص 375.

⁵ - المادة 1/5 من المرسوم الرئاسي رقم 261/15 المؤرخ في 2015/10/8 المحدد فتنشيلة وتنظيم وكيفيات تسيير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها.

⁶ - زينة محمد ي بوزينة، المرجع السابق، ص 75.

2 - تجميع الاتصالات الإلكترونية وتسجيل محتواها

بالرغم أن الرسالة الإلكترونية ذات طابع خاص، لكنها لا تختلف عن الرسالة الورقية من حيث أن مآلها من حيث حفظها أو الإستغناء عنها وإهمالها، لكن ما يميز الرسائل الإلكترونية سواء المهمة أو المحفوظة يمكن الوصول إليها، عن طريق صناديق البريد الخاصة أو الملفات المحفوظة أو الرجوع إلى سلة المهملات¹، ويتم تجميع وتسجيل محتوى الاتصالات الإلكترونية بكل وسيلة إلكترونية على وسائل تخزين معلوماتية مثل الأقراص (صلبة أو مضغوطة، الذاكرة الويضية إلخ) خاصة تلك الاتصالات التي تتم على شبكة الأنترنت بإستعمال برامج متخصصة، أو التي تتم بإستعمال الهاتف الذكي المزود بشريحة يمكن من خلالها الإتصال بشبكة الأنترنت، ونقل الإتصال بالصوت والصورة بواسطة برامج متخصصة مثل ما سنجبر messenger سكيب skype، واتساب wats app والتي تتم بواسطة البريد الإلكتروني².

ومن جانب آخر يمكن تطبيق المراقبة الإلكترونية، على شبكات الحاسوب بالنسبة للمحادثات التي تتم بواسطة شبكة الأنترنت والتي تستعمل تطبيقات جديدة، مثل وسائل التواصل الاجتماعي مثل face book twitter التي توفر هذه الخدمة والتي تكون نتيجتها سماع المحادثات وتسجيل محتواها في حينها والإحتفاظ بها كدليل على وقوع جريمة أو الوقاية منها³.

ولمسايرة التطور المستمر للوسائل التقنية والتي تستعمل في مراقبة الاتصالات الإلكترونية، وحتى تؤدي السلطات القضائية المختصة، وكذا الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، مما يستدعي أن توفر الدولة تجهيزات تفيد في الرصد المبكر لهذا النوع من الجرائم، مع مراعاة التأهيل والتكوين لدى الأشخاص المؤهلين لذلك⁴.

وفي الأخير نصل إلى القول أن الإجراءات التي استحدثها المشرع الجزائري، في إطار مكافحة الجريمة الإلكترونية المتمثلة في المراقبة الإلكترونية، بما أنها تعد إنتهاكا صارخا لحق الشخص في الخصوصية، بقدر ما أصبحت ضرورة لا يمكن الإستغناء عنها خاصة مع تطور أساليب إرتكاب الجريمة.

¹ - زيدان ربيعة، المرجع السابق، ص 128.

² - يزيد بوحليط، المرجع السابق، ص 314.

³ - أمينة علالي، المرجع السابق، ص 192.

⁴ - يزيد بوحليط، المرجع السابق، ص 915.

المطلب الثاني : التفتيش في الجريمة الإلكترونية

إن التفتيش سواء في العالم المادي أو الافتراضي، يعتبر من إجراءات التحقيق ذو الأهمية الكبيرة في كشف الأسرار وتوضيح مسار التحقيق، وهذه الأهمية إما تتعلق بالواقعة المراد إثباتها أو بطرق أخرى، ويعد التفتيش في الجريمة الإلكترونية من أصعب الإجراءات، ويعود ذلك إلى التطور الكبير في تكنولوجيا الإعلام والاتصال، وإن كان ذلك يخضع للقواعد المتعارف عليها في التفتيش، طبقا لقانون الإجراءات الجزائية، إلا أنه يتميز بخصوصية معينة¹، وهو إجراء من إجراءات التحقيق يهدف إلى البحث عن ملبسات الجريمة، كما يتضمن مساسا بحقوق الأفراد وحياتهم التي حرصت الدساتير على حمايتها²، إذ لا يمكن المساس بها إلا بالقدر الذي يخدم السلطات المختصة بإجرائه.³

الفرع الأول: مفهوم التفتيش في الجريمة الإلكترونية

يعرف التفتيش بصفة عامة بأنه "إجراء من إجراءات التحقيق، التي تهدف إلى البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل يتمتع بحرمة المسكن أو الشخص، وذلك بهدف إثبات ارتكابها أو نسبتها إلى المتهم وفقا لإجراءات قانونية محددة".⁴، أو هو "إجراء من إجراءات التحقيق يقوم به موظف مختصا طبقا للإجراءات المقررة قانونا، في محل يتمتع بالحرمة بهدف الوصول إلى أدلة مادية لجناية أو جنحة تحقق وقوعها، لإثبات ارتكابها أو نسبتها إلى المتهم".⁵، وعليه فالتفتيش ليس من إجراءات كشف الجريمة قبل وقوعها، بل هو من إجراءات التحقيق فيها بعد ارتكابها، بينما يرى الفقهاء أن

¹ - رضا هميسي، تفتيش المنظومات المعلوماتية في القانون الجزائري، مجلة العلوم القانونية والسياسية، العدد 5، 2012، ص 157.

² - نصت المادة 47 من دستور 2016 على أنه "تضمن الدولة عدم إنتهاك حرمة المسكن، فلا تفتيش إلا بمقتضى القانون، وفي إطار إحترامه، ولا تفتيش إلا بأمر مكتوب صادر عن السلطة القضائية المختصة."

³ - التفتيش كإجراء من إجراءات التحقيق الابتدائي هو من إختصاص سلطة التحقيق وقاضي التحقيق، وإستثناء يمكن لرجال الضبطية القضائية في حالات محدودة قانونا، منها حالة التحقيق في جنابة أو جنحة متلبس بها المنصوص عليها في المادة 41 من ق.إ.ج.ج وفي التحقيق الابتدائي المنصوص عليها في المادة 69 وما يليها من ق.إ.ج.ج.

⁴ - على عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية دراسة مقارنة، المكتب الجامعي الحديث، 2011، ص 38.

⁵ - عبد الفتاح بيومي مجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجريمة المعلوماتية، المرجع السابق، ص 244.

التفتيش في الأنظمة المعلوماتية عبارة عن تفتيش تقليدي ينصب على الأجهزة المعلوماتية¹، إذ عرف بأنه "إطلاع على محل منحه القانون حماية خاصة، بإعتباره مستودع سر صاحبه يستوي في ذلك أن يكون هذا المحل جهاز حاسوب أو نظمه أو الأنترنت".²

ومن هذه التعاريف نستخلص أن التفتيش هو وسيلة للإثبات المادي، مما يجعله يتنافى مع الطبيعة غير المادية لبيانات ومعطيات الحاسب الآلي، التي ليس لها كيان مادي محسوس في العالم الخارجي مما يثير التساؤل عن مدى صلاحية مكونات الحاسب الآلي أن تكون محلا يرد عليه التفتيش، وماهي ضوابط التفتيش في البيئة الإلكترونية ؟ وهذا ما سنحاول دراسته في هذا الفرع.

الفقرة الأولى: مدى خضوع مكونات الحاسب الآلي للتفتيش

يتكون الحاسب الآلي من مكونات مادية، hard ware كوحدات الإدخال والإخراج، ووحدات التخزين ووحدات المعالجة المركزية (processeur)، ومكونات منطقية³ soft ware كبرامج النظم الأساسية، البرامج التطبيقية والبيانات المعالجة آليا، كماله شبكات إتصالات بعدية سلكية ولا سلكية متواجدة على مستوى المحلي والدولي⁴، والسؤال الذي يمكن طرحه حول مدى خضوع مكونات الحاسب الآلي سواء المادية أو المنطقية للتفتيش؟

أولا: تفتيش المكونات المادية للحاسب الآلي

إن التفتيش الواقع على المكونات المادية الحاسب الآلي، بحثا عن شيء ما يتصل بجريمة إلكترونية وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبيها يخضع للقواعد الإجرائية الخاصة بالتفتيش⁵، و بعبارة

¹ -Olivier Decima , les investigations numériques en procédure pénale français : du piratage informatique aux réquisitions et saisie numériques ?Revue la faculté de droit, université de galatasaray,no1,2017,p3.

² - علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والأنترنت . دراسة مقارنة، عالم الكتب الحديث عمان، ط 1، 2004، ص 13 .

³ - يعرف الكيان المنطقي بأنه "مجموع البرامج والأساليب والقواعد وعند الإقتضاء الوثائق المتعلقة بتشغيل وحدة معالجة البيانات "أنظر رشا مصطفى، الحماية القانونية للكيانات المنطقية، دار الفكر الجامعي، الإسكندرية، د ط، 2006، ص5.

⁴ - عبد اللاه أحمد هلال، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، دار النهضة العربية، القاهرة ط2، 2008، ص 17 وما يليها.

⁵ - حسين بن سعيد الغافري، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الأنترنت، ص11، بحث منشور على الموقع الإلكتروني <http://www.eastlaws.com>، أطلع عليه يوم 2017/02/12 على الساعة 13h.

أخرى أن تفتيش تلك المكونات يتوقف على طبيعة المكان الموجودة فيه، هل هي الأماكن العامة أو الأماكن الخاصة، كمسكن المتهم أو أحد ملحقاته كان لها حكمه، فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكنه وبنفس الضمانات التي يقرها القانون في التشريعات المختلفة.¹

قد نص المشرع الجزائري على ذلك في المادة 64²، وكذلك أحكام المواد من 44 إلى 47 من قانون الإجراءات الجزائية، وقد إستثنى المشرع في هذا الخصوص بعض الجرائم من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، من أن تطبق عليها القواعد الواردة في المواد السابقة إذ جاء في نص المادة 3/47 " أنه يجوز إجراء التفتيش في كل محل سكني في كل ساعة من ساعات النهار أو الليل، ذلك بناء على إذن مسبق من وكيل الجمهورية. " ويفهم من ذلك أن المشرع إستثنى تطبيق ضمانات التفتيش على هذا النوع من الجرائم، إلا أنه أخضع إجراء التفتيش وأباحه في هذه الحالة إلى صدور إذن من وكيل الجمهورية المختص، أما إذا كانت المكونات المادية للحاسوب متواجدة في أماكن عامة كمحلات بيع الحواسيب وبيع البرامج الحاسوبية، فإن إجراءات التفتيش تكون وفقا للقواعد الخاصة بتلك الأماكن، إذ أن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص، وبنفس الضمانات والقيود المنصوص عليها في هذا المجال.³

وبناء على ذلك فالمكونات المادية للحاسب الآلي تخضع لنفس الإجراءات المطبقة على التفتيش الواردة في قانون الإجراءات الجزائية.

ثانيا: تفتيش المكونات المنطقية (المعنوية) للحاسب الآلي

لقد أثار تفتيش المكونات المعنوية الحاسب الآلي، جدلا كبيرا حول صلاحيتها لأن تكون موضوعا للتفتيش من عدمه، وهذا ما سعت إليه بعض القوانين وجانب من الفقه في بعض الدول، إلى إزالة هذا الخلاف على نحو يسمح بإمكانية إجراء التفتيش للبحث عن أدلة الجريمة في بيئة الحاسب الآلي، في حين أن البعض الآخر يرى غير ذلك ويتجسد هذا الخلاف في الإتجاهين التاليين:

¹ - عبد الله حسين علي محمود، المرجع السابق، ص 370.

² - تنص المادة 64 من ق.إ.ج.ج على أنه "لا يجوز تفتيش المساكن ومعاينتها وضبط الأشياء المثبتة للتهمة إلا برضا صريح من الشخص الذي سيتخذ لديه هذه الإجراءات يجب أن يكون هذا الرضا بتصريح مكتوب بخط يد صاحب الشأن، فإن كان لا يعرف الكتابة فبإمكانه الاستعانة بشخص بنفسه، ويذكر ذلك في المحضر مع الإشارة صراحة إلى رضا".

³ - نبيلة هبة هروال، الجوانب الإجرائية لجرائم الأنترنت في مرحلة جمع الإستدلالات، المرجع السابق، ص 238.

ذهب الرأي الأول إلى جواز ضبط البيانات الإلكترونية بمختلف أشكالها، ويستند هذا الرأي على أن القوانين الإجرائية عند ما تنص على إصدار الإذن بضبط "أي شيء" فإن ذلك يجب تفسيره بأنه يشمل بيانات الكمبيوتر المحسوسة وغير المحسوسة.

ومن ثم فوفقا لهذا الإتجاه، فإنه إذا كانت الغاية من التفتيش هي ضبط الأدلة المادية التي تفيد في كشف الحقيقة، فإن هذا المفهوم يمتد ليشمل البيانات الإلكترونية بمختلف أشكالها، وذلك إستنادا إلى عمومية نصوص التفتيش التي تجيز تفتيش أي شيء، أو إتخاذ أي إجراء يكون ضروريا لجمع أدلة الجريمة.¹

وعلى النقيض من ذلك ذهب جانب من الفقه إلى القول إذا كانت الغاية من التفتيش هي ضبط الأدلة المادية التي تفيد في كشف الحقيقة، فإن هذا المفهوم لا ينطبق على بيانات الحاسب الآلي غير الملموسة، ويقترح هذا الرأي ولمواجهة هذا القصور التشريعي، ضرورة إضافة إلى الغاية التقليدية عبارة "المواد المعالجة عن طريق الحاسب الآلي أو بيانات الحاسب الآلي".²، وبذلك تصبح الغاية الجديدة من التفتيش هي البحث عن الأدلة المادية أو أي مادة معالجة بواسطة الحاسب.³

و لهذا نجد أغلب التشريعات المقارنة تميل إلى هذا الإتجاه، كالتشريع الأمريكي الذي نظم نصوص جديدة خاصة بإجراء التفتيش والضبط في بيئة الحاسب الآلي، في القسم 2000 من القانون الإجرائي الإتحادي الخاص بجرائم الحاسب الآلي⁴، وهو نفس المسلك الذي تبناه المشرع الجزائري، إستجابة لهذه التغيرات أجاز تفتيش المعطيات المعلوماتية، وذلك بموجب المادة 5 من القانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، التي تجيز للسلطات القضائية المختصة ولضباط الشرطة القضائية، في إطار قانون الإجراءات الجزائية وفي

¹ - نعيمة إزويري، التفتيش في الجرائم الإلكترونية، مجلة المتوسط للدراسات القانونية والقضائية، العدد 4، 2017، ص 253.

² - إستجاب المشرع الفرنسي لهذه التغيرات وقام بتعديل نصوص التفتيش بالقانون 545 - 2004 المؤرخ في 21 جوان 2004 المتعلق بالثقة في الإقتصاد الرقمي حيث قام بإضافة عبارة "المعطيات المعلوماتية" في المادة 94 والذي جاء نصه: Art 94 du C.P.P.F. dispose que « les perquisitions sont effectuées dans tous les lieux où peuvent se trouver des objets ou des données informatique dont la découverte serait utile à la manifestations de la vérité. »

³ - جاسم خريبوط خلف، التفتيش في الجرائم المعلوماتية، مجلة الخليج العربي، المجلد 41، العدد 3-4، 2013، ص 243.

⁴ - نبيلة هبة هروال، الجوانب الإجرائية لجرائم الأنترنت في مرحلة جميع الاستدلالات، المرجع السابق، ص 226.

الحالات المنصوص عليها في المادة 4 من ذات القانون، ومن بين هذه الحالات توفر معلومات عن احتمالا على منظومة معلوماتية على نحو يهدد النظام العام، أو الدفاع الوطني أو مؤسسات الدولة، أو الإقتصاد الوطني، وللوقاية من الجرائم الماسة بأمن الدولة، الدخول بغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها، وكذا منظومة تخزين معلوماتية.¹

وهذا ما أكدته إتفاقية بودابست التي حثت الدول الأعضاء، على إجراء تفتيش النظم المعلوماتية وتجسيد هذا الحق بكل وضوح في قوانينها الإجرائية، لتفادي أي إشكال يمكن أن يثار حول الموضوع وذلك من خلال المادة 1/19 من الإتفاقية السالفة الذكر والتي جاء نصها كما يلي " لكل طرف الحق في سن من القوانين ما هو ضروري لتمكين السلطات المختصة من تفتيش أو الدخول إلى:

- نظام الحاسب أو جزء منه أو المعلومات المخزنة فيه.

- الوسائط التي يتم فيها تخزين معلومات الحاسب بها مادامت مخزنة في إقليمها.²

كما أجازت الإتفاقية العربية لمكافحة جرائم تقنية المعلومات³ المحررة بالقاهرة بتاريخ 21 ديسمبر 2010 التفتيش، من خلال المادة 26/1 التي جاء فيها "على أن تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين سلطاتها المختصة من التفتيش أو الوصول إلى:

أ- تقنية معلومات أو جزء منها والمعلومات المخزنة فيها أو المخزنة عليها.

ب- بيئة أو وسيط تخزين معلومات تقنية معلومات والذي قد تكون معلومات التقنية مخزنة فيه او

عليه..."

¹ - المادة 05 من القانون 04-09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

² - Art 19 alinéa 1 du C.C.C dispose que ;

1-chaque partie adopte les mesures législatives et autres qui se relèvent nécessaires pour habiliter ses autorités compétentes à perquisitionner à accéder d'une façon similaire.

a- à un système informatique ou à une partie de celui -ci ainsi qu'au données informatique qui y sont stockées, et

b- à un support du stockage informatique permettant de stocker des données informatique sur son territoire.

³ - صادقت عليها الجزائر بالمرسوم الرئاسي رقم 14-252 المتضمن الإتفاقية العربية لمكافحة جرائم تقنية المعلومات.

الفقرة الثانية: تفتيش المنظومة المعلوماتية عن بعد

من المشكلات التي تواجه القائم بالتفتيش، مشكلة إتصال الحاسب الآلي موضوع التفتيش بحاسب آلي آخر موجود داخل أو خارج إقليم الدولة، أي عبر شبكات الإتصال العالمية، فكثيرا ما يقوم المجرم المعلوماتي بتخزين بياناته ومعلوماته في حواسيب أخرى بهدف عرقلة التحقيقات¹، لكن السؤال الذي يمكن أن نطرحه عن إمكانية إمتداد التفتيش ليشمل الحواسيب الأخرى المرتبطة بالحاسوب الآلي المراد تفتيشه، وللإجابة على هذا التساؤل نجد أن المشرع الجزائري ميز بين تفتيش المنظومة المعلوماتية بين ما إذا كانت المنظومة متصلة بنظام آخر داخل التراب الوطني، ومنظومة معلوماتية متصلة بمنظومة معلوماتية تقع خارج الإقليم الجزائري، وهذا ما جاء في نص المادة 5 من قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها.

أولا: إتصال حاسوب المتهم بحاسوب موجود في مكان آخر داخل الدولة

يجب أن يكون الحاسب الآلي الذي تسعى السلطات المختصة بتفتيشه، متصلا بأجهزة معلوماتية موجودة في أماكن معينة داخل إقليم الدولة، كمقر عمل المتهم أو منزل آخر غير منزله، وأن ثمة بيانات مطلوبة كأدلة إثبات تفيد في كشف الحقيقة مخزنة داخله.²

بالرجوع إلى قانون الإجراءات الجزائية الجزائري، نجده لم ينظم التفتيش عن بعد للكيانات المنطقية في نظام المعالجة الآلية للمعطيات، وإزاء هذا القصور إستدرك المشرع الأمر بنص خاص ضمنه القانون 04-09، وذلك ما جاء بمقتضى المادة 2/5 حيث أجاز تفتيش هذه المنظومة بشكل له طابع السرعة والاستعجال، إذا كانت هناك أسباب تدعو للإعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى، وأن هذه المعطيات يمكن الدخول إليها إنطلاقا من المنظومة الأولى، وهذا دون شرط صدور إذن قضائي، وإنما يكفي إعلام السلطة القضائية المختصة مسبقا بذلك، وهذا ما أكدته المادة 2/5 من القانون 04-09 بقولها "بعد إعلام السلطة القضائية المختصة مسبقا بذلك"، ولعل إنتظار صدور الإذن من السلطات المختصة قد يأخذ بعض الوقت ما قد يؤدي إلى تلاشي الدليل الإلكتروني وإندثاره في

¹ - محمد طارق عبد الرؤوف الخن، المرجع السابق، ص 282.

² - نعيمة إزويري، المرجع السابق، ص 255.

وقت قياسي كأن يقوم الجاني بمحوه وإتلافه¹، إذ يكفي الضغط على مكان معين لإنهاء وجود المعلومة ومن ثم تتبخر عناصر الإثبات، ما يشكل صعوبة في إيجاد دليل حاسم، لذلك فإن إستصدار إذن قضائي في مثل هذه الحالات لا طائل منه.²

ثانيا: إتصال حاسوب المتهم بحاسوب في مكان آخر خارج الإقليم

هنا يثور التساؤل حول مدى إمكانية إمتداد الحق في التفتيش إلى أجهزة الحاسب الآلي المتصلة بجهاز المتهم أو المشتبه فيه خارج إقليم الدولة، ودخوله في المجال الجغرافي لدولة أخرى، وقد يتعذر القيام به بسبب تمسك كل دولة بسيادتها وحدودها الإقليمية³، فإهتدت أغلب التشريعات إلى حل هذه المشكلة، على جواز التفتيش للنظم المعلوماتية المتصلة بالحاسب الآلي الذي يجري تفتيشه، وتسجيل كل البيانات والمعلومات التي تساعد في كشف الحقيقة وتعتبر كأداة إثبات⁴، لذلك أجاز المشرع الجزائري تفتيش الأنظمة المتصلة حتى ولو كانت متواجدة خارج إقليم الدولة الجزائرية، فالمادة 3/5⁵ من القانون 04-09 أوجبت خضوع عملية التفتيش بشأنها للاتفاقيات الدولية المبرمة في هذا المجال، ووفقا لمبدأ المعاملة بالمثل، إذ من المتصور أن يقدم مرتكبو الجرائم بتخزين بياناتهم في أنظمة معلوماتية خارج الدولة عن طريق شبكات الإتصال البعيدة، بهدف عرقلة السلطات المختصة في جمع الأدلة، وبالتالي فإنه يتم الحصول على هذه المعطيات بمساعدة السلطات الأجنبية المختصة وهو الأمر الذي يؤكد على ضرورة التعاون الدولي في مجال مكافحة الجرائم الإلكترونية.⁶

لكن ما يمكن ملاحظته أن إتفاقية بودابست لسنة 200، أجازت إمكانية الدخول بغرض التفتيش والضبط في أجهزة شبكات تابعة لدول أخرى بدون إذنهما في حالتين: إذا تعلق التفتيش بمعلومات أو

¹ - موسى مسعود أرحومة، المرجع السابق، ص8.

² - رضا هميسي، المرجع السابق، ص167.

³ - خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص205.

⁴ - نعيم سعيدي، المرجع السابق، ص157.

⁵ - تنص المادة 3/5 من قانون 04-09 على أنه "إذا تبين مسبقا أن هذه المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى مخزنة في منظومة معلوماتية، تقع خارج الإقليم الوطني فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات صلة وفقا لمبدأ المعاملة بالمثل".

⁶ - فاطمة الزهراء عربوز، التفتيش الإلكتروني كإجراء للتحقيق في الجرائم المعلوماتية، مجلة جيل الأبحاث القانونية المعمقة، مركز جيل الأبحاث العلمي، العدد34، جويلية2019، ص108.

بيانات مباحة للجمهور، والثانية إذا رضي صاحب هذه المعلومات، بهذا التفتيش وهذا تضمنته المادة 32 من ذات الاتفاقية.¹

الفرع الثاني: شروط التفتيش في البيئة الرقمية

تضمنت معظم التشريعات الوطنية ضوابط وشروط معينة، يجب إتباعها عند التعرض للحريات الشخصية بإجراء من الإجراءات الماسة بالحرية، كالتفتيش الذي ينبغي أن يجري وفقا لشروط معينة وعلى الجهة القضائية أن تراعيها وإلا كان عملها خاليا من أي أثر قانوني وتتمثل هذه الشروط في شروط موضوعية وأخرى شكلية

الفقرة الأولى: الشروط الموضوعية

تتضمن القواعد الموضوعية لتفتيش الحاسب الآلي عدة شروط هي: السبب، المحل والسلطة القضائية المختصة بالقيام به.

أولا: سبب التفتيش في نظام المعلوماتية

سبب التفتيش في الجرائم عموما هو السعي نحو الحصول على دليل في التحقيق قائم من أجل الحصول على حقيقة الحدث²، ويتحقق عادة عند وقوع جريمة من الجرائم وإسنادها إلى شخص معين، سواء بصفته مرتكبا لها أو مساهما فيها، أو توافر قرائن على وجود أشياء لدى المتهم المعلوماتي وغيره تفيد في كشف الحقيقة.

1- وقوع جريمة إلكترونية تحمل وصف جنائية أو جنحة

حتى يكون إجراء التفتيش في نظم المعلوماتية صحيحا، لا بد أن يكون بصدد جريمة إلكترونية واقعة بالفعل، سواء أكانت جنائية أو جنحة³، وبالتالي تستبعد من ذلك المخالفات بسبب ضعف خطورتها على إهدار الحرية الفردية وحرمة المساكن عن طريق إجراء التفتيش.⁴

¹ - Art32 du c.c.c dispose que : « une partie peut, sans l'autorisation d'une autre partie à accéder à des données informatique stockées accessible. » convention sur la cybercriminalité, op cit.

² - عائشة بن قارة مصطفى، المرجع السابق، ص 60.

³ - وهذا تصديقا للمادة 66 من قانون إجراءات جزائية التي تنص على " التحقيق الابتدائي وجوبي في مواد الجنايات أما في مواد الجناح فيكون اختياري ما لم يكن ثمة نصوص خاصة...."

⁴ - جمال إبراهيمي، المرجع السابق، ص 38.

2- توجيه التهمة إلى شخص وإسنادها إليه

ينبغي أن تتوفر في حق الشخص المراد تفتيشه، دلائل كافية تدعو إلى الاعتقاد بأنه قد ساهم في ارتكاب الجريمة الإلكترونية، سواء بصفته فاعلا أصليا أو شريكا فيها¹، وأن تعبير الدلائل يقصد بها مجموعة من المظاهر أو القرائن المعينة، التي تقوم على المضمون العقلي والمنطقي لملاحظات الواقعة، وكذلك على خبرة وحرفية القائم بالتفتيش، والتي تؤيد إستناد الجريمة إلى شخص معين بوصفه فاعلا أو شريكا²، من الدلائل المستمدة من الواقع والقرائن التي تنبأ عن ارتكاب الشخص لجريمة إلكترونية، ومن أمثلتها إرتباط عنوان أنترنت بروتوكول الخاص بجهاز الحاسوب الذي يحتوي على صور فاضحة، مع رقم حساب المتهم لدى مزود الخدمات، ووجود رقمين للهاتف لديه يستخدمان في ذلك.³

3- توافر إمارات قوية على وجود أدلة مادية تفيد في كشف الجريمة

يجب أن يكون الإتهام مبنيًا على أدلة وقرائن قانونية، وعليه يتعين على الجهة التي تمنح الإذن بالتفتيش أن تراقب هذه الإجراءات، فالتفتيش لا يجوز إجراؤه إلا إذا كان هناك احتمال العثور على دليل من وراءه⁴، فلا يكفي مجرد الظن أو الإشتباه، بل يجب توفر بعض الأدلة والقرائن المعقولة التي تحمل على الاعتقاد بوقوع جريمة إلكترونية، ونسبتها إلى المتهم المراد تفتيش منظومته المعلوماتية أو نظام إتصالاته الإلكترونية.⁵

ثانيا: محل التفتيش

ويقصد بمحل التفتيش المستودع الذي يحتفظ فيه المرء بالأشياء المادية التي تتضمن سره، والسر الذي يحميه القانون هو ذلك الذي يستودع في محل له حرمة، كالمسكن أو الشخص أو الرسائل، وبالتالي فقد يكون محل ذلك التفتيش، إما المسكن أو الشخص أو الرسالة، مع مراعاة الإجراءات القانونية المقررة

¹ - عبد اللاه أحمد هلاي، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق، ص115.

² - جاسم خريبط، المرجع السابق، ص249. / عائشة بن قارة مصطفى، المرجع السابق، ص62.

³ - شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2007، ص282.

⁴ - سامي حسين الحسيني، النظرية العامة للتفتيش، دار النهضة العربية، القاهرة، 1972، ص36.

⁵ - رضا هميسي، المرجع السابق، ص165.

لكل محل على حدة¹، فمحل التفتيش في الجرائم الإلكترونية، فهو نظام المعالجة الآلية بكل مكوناته المادية والمعنوية وشبكات الاتصال الخاصة به والتي توجد في حوزة شخص، أو تكون موضوعة في مكان حرمة خاصة كالمسكن أو المكتب.

وسبق أن أشرنا إلى مدى قابلية المكونات المادية والمعنوية للحاسوب للتفتيش فضلا عن شبكات الاتصال الخاصة به فلا داعي لتكرار ذلك.

ثالثا: الجهة المختصة بالتفتيش

يعتبر إجراء التفتيش من إجراءات التحقيق الابتدائي، والتي تمس بالحرية الشخصية وانتهاك حرمة الحياة الخاصة للأفراد، حرص المشرع الجنائي بصفة عامة الى إسناد مهمة التفتيش لجهة قضائية تكفل الحقوق والحريات²، وتضمنها وحدد الجهة المختصة بهذا الإجراء، فبالنسبة للمشرع الجزائري فقد أوكل مهمة إجراء التفتيش للسلطات القضائية المختصة الممثلة في قاضي التحقيق، ووكيل الجمهورية أو لضباط الشرطة القضائية، في مرحلة الاستدلال وذلك بأمر من السلطة المختصة يستشف من المادة³⁵ من القانون 04-09 التي تضمنت عبارة "يجوز للسلطات المختصة وكذا ضباط الشرطة القضائية..."

وبالنظر للمهارات الفنية التي تتطلبها الجريمة الإلكترونية⁴، فقد أجاز المشرع للسلطات المكلفة بالتفتيش، الإستعانة بخبير له دراية بالمعلوماتية محل البحث أو التدابير المتخذة، لحماية المعطيات المعلوماتية التي تتضمنها بهدف مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها، وذلك طبقا لمقتضيات المادة 3/5 منها ويتمثل دور الخبير في تقديم التوضيحات الكافية حول كيفية تشغيل هذه الأنظمة وطريقة الدخول إليها أو إلى المعطيات المخزنة أو المعالجة أو المنقولة في شكل يمكن فهمه أو إدراكه.⁵

¹ - نبيلة هبة هروال، الجوانب الإجرائية لجرائم الأنترنت، المرجع السابق، ص234.

² - نبيلة هبة هروال، الجوانب الإجرائية لجرائم الأنترنت، المرجع نفسه، ص241.

³ - تنص المادة 5 من قانون 04-09 على "يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 4 أعلاه الدخول التفتيش ولو عن بعد إلى:

أ- منظومة معلوماتية أو جزء منها وكذا المعطيات المخزنة فيها

ب - منظومة تخزين معلوماتية."

⁴ - نداء نائل فايز المصري، المرجع السابق، ص68.

⁵ - رضا هميسي، المرجع السابق، ص 172.

الفقرة الثانية: الشروط الشكلية

إضافة للشروط الموضوعية لصحة إجراء تفتيش المنظومة المعلوماتية، توجد شروط أخرى ذات طابع شكلي يجب مراعاتها عند ممارسة هذا الإجراء، وتتمثل في:

أولاً: الحضور الضروري لبعض الأشخاص أثناء التفتيش

بما أن التفتيش يشكل إعتداء على حرمة أو حرية الأشخاص والإطلاع على أسرارهم، فقد أوجبت التشريعات حضور المشتبه فيه، أو من ينوب عنه أو الشهود في إجراء عملية التفتيش، وذلك لضمان سلامة هذا الإجراء والحيلولة دون تعسف الجهة القائمة بالتفتيش.

ولقد اشترط المشرع الجزائري بموجب المادة 1/45 على أن يتم إجراء التفتيش الخاص بالمساكن وملحقاته بحضور المشتبه فيه أثناء عملية التفتيش في مسكنه من طرف ضباط الشرطة القضائية، وإن تعذر ذلك بإمتناعه عن الحضور أو كان هاربا، يتم بحضور شاهدين من غير الموظفين الخاضعين لسلطة ضباط الشرطة القضائية القائم بالتفتيش¹، والهدف من ذلك ضمان الإطمئنان إلى سلامة الإجراء وصحة الضبط²، وبالرغم من أهمية مثل هذه الضمانات التي تهدف إلى عدم التعسف في إستخدامها، إلا أنها قد تتحول إلى صعوبات ومشكلات تحول دون الوصول إلى النتائج المرجوة من التفتيش، في حالة التفتيش الذي يخص الجريمة الإلكترونية، ولأن إشعار الأشخاص المطلوب حضورهم قد يتيح لهم التلاعب بالمعطيات والبرامج المراد تفتيشها، ونظر لخصوصية الجرائم الإلكترونية وما يتطلبه الأمر من بسط نوع من السرية أثناء جمع الدليل الإلكتروني، بالإضافة إلى الإسراع في إستخلاصه قبل فقده³، مما جعل المشرع الجزائري لا يتقيد بقاعدة حضور صاحب المسكن وهذا ما جاء في الفقرة الأخيرة من نفس المادة حيث نص على إستثناء، فأسقط تطبيق هذا الشرط، وخول لضباط الشرطة القضائية إجراء التفتيش دون التقيد بحضور المتهم أو صاحب المنزل المراد تفتيشه.

ثانياً: الميعاد الزمني لإجراء التفتيش

تحرص بعض التشريعات على حظر القيام بتفتيش المساكن وما في حكمها في وقت معين، وذلك

¹ - المادة 1/45 من قانون إجراءات جزائية جزائري.

² - عبد الله أحمد هلال، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق، ص 164.

³ - نعيم سعيداني، المرجع السابق، ص 153.

حرصا على تضيق نقاط الإعتداء على الحرية الفردية وحرمة المساكن، في حين تركت بعض التشريعات الإجرائية أمر تحديد ذلك الوقت للقائم بالتفتيش¹، مثل قانون الإجراءات الجنائية المصري الذي لم يحدد وقتا محددا للتفتيش فيجوز إجراءه في أي وقت ليلا أو نهارا²، وعلى عكس ذلك حدد المشرع الجزائري الفترة الزمنية لتفتيش المنازل وما في حكمها بمقتضى المادة 1/47³ من ق.إ.ج.ج، وفي الوقت المحصور بين الساعة الخامسة صباحا والثامنة مساء، إلا أن هذا الشرط لا يؤخذ على إطلاقه، فأستثنى المشرع عدة حالات⁴ تضمنت الخروج عن الميقات المحدد في إجراء التفتيش منها الجرائم الإلكترونية، حيث جاءت المادة 3/47 من ق.إ.ج.ج لتتص على جواز إجراء ضباط الشرطة القضائية للتفتيش كل ساعة من ساعات الليل والنهار، أي الإستغناء على شرط الميقات الزمني للتفتيش على جرائم تعد خطيرة، وهذا عندما يتعلق الأمر بجرائم المخدرات، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، الجريمة المنظمة عبر الحدود الوطنية وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف⁵، والقيد الوارد في هذه المادة على هذا النوع من الجرائم ومنها الجريمة الإلكترونية ترجع لفطنة المشرع بخطورة وخصوصية هذه الجريمة من حيث إرتكابها في أي وقت، وكذلك يمكن إخفاء أدلة إثباتها فهي سهلة المحو والتدمير وهي غير مرئية، وبالتالي إن تأخير إجراء التفتيش في الموعد القانوني، قد يعرقل السير الطبيعي لمجريات التحقيق هذامن جهة⁶، ومن جهة أخرى فإن هذه الضمانة بدأت تقل أهميتها مع ظهور ما يسمى بالتفتيش عن بعد والذي يتم إجراءه في أي وقت من الزمن.

¹ - عبد اللاه أحمد هلالي، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق، ص175.

² - قضت محكمة النقض المصرية في هذا الصدد بأنه "لما كان التفتيش الذي قام به الضابط في هذه الدعوى مأذونا به قانونا فإن له يجزبه بالطريقة التي يراها مناسبة محققة للغرض منه مادام أنه قد التزم الحدود التي نظمها إذن النيابة ومن ثم فلا تثريب عليه أن هو اقتحم غرفة نوم المطعون ضده فجر يوم الحادث بعد ان تمكن أحد معاونيه من فتح باب المسكن الخارجي بواسطة التسور مادام الضابط قد رأى ذلك. أنظر عبد اللاه أحمد هلالي، نفس المرجع، ص 175.

³ - تنص المادة 1/47 من ق.إ.ج.ج على أنه "لا يجوز البدء في تفتيش المساكن ومعاينتها قبل الساعة الخامسة صباحا ولا بعد الساعة الثامنة ليلا، إلا إذا طلب صاحب المنزل أو وجهت نداءات من الداخل أو الأحوال الاستثنائية المقررة قانونا".

⁴ - أجاز المشرع التفتيش في أية ساعة من ساعات الليل والنهار وذلك عندما يتعلق الأمر بالجرائم المنصوص عليها في المواد من 342 الى 345 من ق.ع.ج، حالة رضا صاحب المسكن، حالة الضرورة.

⁵ - المادة 3/47 من قانون إجراءات جزائري.

⁶ - رشيدة بوكري، المرجع السابق، ص417.

ثالثا: تحرير محضر بالتفتيش

إضافة إلى الضمانات السابقة الذكر يجب تحرير محضر، يتم تدوين ما تم من إجراءات بصدد التفتيش وما أسفر عنه من أدلة، ولم يتطلب القانون شكلا خاصا في محضر التفتيش، ومن ثم فإنه لا يشترط لصحته سوى ما تستوجبه القواعد العامة في المحاضر عموما، والتي تقتضي بأن يكون المحضر مكتوبا باللغة الرسمية للدولة، وأن يحمل تاريخ تحريره وتوقيع محرره، كما يتضمن كافة الإجراءات التي أتخذت بشأن الوقائع التي يثبتها.¹

ومن أهم الشروط الجوهرية التي ينبغي مراعاتها في محضر التفتيش الإستعانة بكاتب يصحبه المحقق لتحرير المحضر وتدوين ما تم من إجراءات والتأشير عليها، وإلا أعتبرت باطلة وهو ما جاء في نص المادة 2/68 من ق.إ.ج.ج "تحرير نسخة من هذه الإجراءات وجمع الأوراق، ويؤشر كاتب التحقيق أو ضابط الشرطة القضائية المنتدب على كل نسخة بمطابقتها للأصل"، كما تؤكد المادة 79 من ق.إ.ج.ج "... ويستعين قاضي التحقيق دائما بكاتب التحقيق ويحرر محضر بما يقوم به من إجراءات."²

وهو نفس الأمر بالنسبة لمحضر التفتيش في الجرائم الإلكترونية، فإنه يستلزم إلى الشكلية السابقة ضرورة إحاطة الشخص القائم بالتفتيش بتقنية المعلومات، أو إستعانتة بأهل الخبرة الفنية والإختصاص حتى يمكنه من صياغة محضر التفتيش.

وتبعا لما سبق فإنه يترتب على عدم مراعاة الضوابط الموضوعية والشكلية التي تناولناها بالدراسة بطلان إجراء التفتيش، وبالتالي فقدان الدليل المستمد من قيمته، ولا يجوز التعويل عليه سواء من طرف جهات التحقيق أو جهات الحكم، ولا يبقى له سوى قيمته الإستدلالية.

إذا أولى المشرع الجرائم الإلكترونية بخصوصية تامة عند القيام بعملية التفتيش وقد إستثنى تطبيق هذه القواعد والضوابط، وأبقى على شرطي الحصول على الإذن وإحترام السر المهني، وكذلك ما يمكن ملاحظته أن المشرع أشرك عدة أشخاص للقيام بعملية التفتيش، تتمثل في السلطات القضائية، وتسخير أشخاص لهم دراية في هذا المجال، و كذا السلطة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها.

¹ - عبد الله أحمد هلال، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق، ص 167.

² - المادتان 2/68 و 79 من قانون الإجراءات الجزائية الجزائري.

الفرع الثالث: حجز المعطيات المعلومات (الضبط)

يهدف التفتيش إلى ضبط الأدلة المادية التي تفيد في كشف الحقيقة، فالضبط هو غاية التفتيش القريبة أي الأثر المباشر الذي يسفر عنه الإجراء، والعلاقة وثيقة بين التفتيش الضبط فإذا ما بطل إجراء التفتيش بطل الضبط¹، فسوف نتناول في هذا الفرع الضبط في الجريمة الإلكترونية من خلال التطرق إلى مفهوم الضبط (الفقرة الأولى) واساليب ضبط (حجز) المعطيات (الفقرة الثانية).

الفقرة الأولى: مفهوم الضبط

يعتبر الضبط الوسيلة القانونية، التي تضع بواسطتها السلطة المختصة يدها على جميع الأشياء التي وقعت عليها الجريمة أو نتجت عنها أو أستعملت لإقترافها²، وقد أجاز القانون ضبط كل ما يعد من آثار الجريمة التي تساعد إظهار الحقيقة، فالضبط يقع على الأشياء المادية ولا ينصب على الأشياء المعنوية، والسؤال الذي يطرح هل يمكن أن ينصب الضبط على المكونات المعنوية للحاسوب؟ لهذا سوف نتطرق إلى تعريف الضبط (أولا) وموقف الفقه من ضبط الأدلة الرقمية (ثانيا).

أولا: تعريف الضبط

يعرف الضبط بالمعنى التقليدي "وضع اليد على شيء يتصل بجريمة وقعت، ويفيد في كشف الحقيقة عنها وعن مرتكبيها."³، فيما يعرف الضبط في المجال المعلوماتي بأنه "وضع اليد على الدلائل المادية المخزنة فيها البيانات الإلكترونية أو المعلوماتية، التي تتصل بالجريمة الإلكترونية، التي وقعت وتفيد في كشف الحقيقة عنها وعن مرتكبيها."⁴، لكن الأستاذ سامي جلال خالف هذا التعريف لسبب أن المعلومات تضبط كذلك عبر الشبكة أي عندما تكون في طريقها إلى محل إرسالها، ويكون ذلك عند مراقبة الاتصالات الإلكترونية، وأعطى تعريفا آخر بقوله أنه "وضع اليد على المكونات المادية للحاسوب والأدلة المعلوماتية المخزنة في الحاسوب محل التفتيش، أو في الشبكة أو في الحاسوب الخادم، والتي تفيد في كشف الحقيقة في جريمة وقعت جاري التحقيق فيها."⁵، لهذا يمكن أن نفرق بين الضبط المادي والضبط الرقمي، فالضبط

¹ - علي حسن محمد الطوالة، المرجع السابق، ص 135.

² محمد طارق عبد الرؤوف الخن، المرجع السابق، ص 290.

³ عبد الفتاح بيومي حجازي، الجوانب الاجرائية لأعمال التحقيق الابتدائي، المرجع السابق، ص 669.

⁴ عادل عبد الله خميس العمري، التفتيش في الجرائم المعلوماتية، الفكر الشرطي، المجلد 22، العدد 86، 2013، ص 267.

⁵ - سامي جلال فقي حسين، المرجع السابق، ص 263.

المادي يؤدي إلى تدخل سلطة التحقيق في سيطرة المتهم على أملاكه، بينما الأمر يختلف في مجال ضبط المعلومات، أن سلطة التحقيق تقوم بنسخ نسخة إلكترونية للبيانات الموجودة لدى المتهم ولو تعددت النسخ، وتبقى النسخة الأصلية بحوزة المتهم، بحيث يتمتع بكل حقوقه على هذه النسخة، لذا يمكن أن نقول أن الضبط الرقمي يراد منه إستبقاء بيانات محوسبة قد تقيّد في كشف الحقيقة تحت تصرف سلطة التحقيق ريثما يتم تقديمها للقضاء، وقد تبنت هذه القاعدة الإتفاقيات والتشريعات.¹

ثانيا: موقف الفقه من ضبط الأدلة الإلكترونية

إذا كانت الأشياء التي تضبط في الجرائم التقليدية تتصف بالمادية، ويمكن ضبطها وحجزها ولا تنثير أي غشكالات من الناحية القانونية، غير أنه ليس من السهل توقيع الضبط أو الحجز على منظومة معلوماتية، وذلك أن المعلومات هي في الأصل شيء معنوي غير محسوس وملمس، فالسؤال الذي يمكن طرحه هل يمكن أن ينصب الضبط أو الحجز على المكونات المعنوية للحاسب الآلي؟ وهذا ما سنحاول الإجابة عليه من خلال آراء الفقهاء، حيث إنقسم الفقه في ذلك إلى رأيين هما:

1- الرأي الأول

يرى أنصار هذا الإتجاه² أنه لا يمكن تصور ضبط الأدلة على المكونات المعنوية للنظام المعلوماتي، لإنتفاء الكيان المادي لها، لذلك فإن الأشياء المعنوية غير قابلة للضبط فهي تنقصها الخاصية المادية، ولا سبيل لضبطها، إلا إذا كانت مخزنة في دعامة أو وسيط إلكتروني، أو كانت من مخرجات الحاسب الآلي.³

2- الرأي الثاني

على عكس الرأي الأول يذهب هذا الإتجاه إلى القول، بأنه لا يوجد مانع من حجز هذه البيانات والمعطيات المعالجة بالنظام المعلوماتي، على أساس يمكن تمديد مفهوم ضبط الأدلة المادية ليشمل البيانات الإلكترونية، والتي تتكون من المعلومات والتي لا يمكن حجزها وضبطها بإعتبارها أشياء معنوية

¹ - رابح لهوى، الشرعية الإجرائية للأدلة المعلوماتية المستمدة من التفتيش، أطروحة لنيل شهادة دكتوراه علوم، كلية الحقوق والعلوم السياسية، جامعة باتنة 1، 2020-2021، ص، ص، 91-92.

² - تبنى هذا الإتجاه الفقه الألماني، وسابره كل من التشريع الياباني، وتشريع رومانيا. أنظر عبد اللاه أحمد هلال، تفتيش نظم الحاسب الآلي، المرجع السابق، ص 201.

³ - نبيلة هبة هروال، الجوانب الإجرائية لجرائم الأنترنت، المرجع السابق، ص 266.

غير محسوسة، في حين نجد أن البيانات المعالجة آليا تأخذ الطابع المادي على أساس أنها ذبذبات إلكترونية وإشارات أو موجات كهرومغناطيسية، يمكن تخزينها على وسائط ودعامات معينة¹، كما إستندوا في ذلك إلى غاية التفتيش هو ضبط الأشياء التي تفيد كشف الحقيقة، وأن هذا المفهوم يمتد ليشمل المعلومات والبيانات.²

وهذا ما أقرته إتفاقية بودابست المتعلقة بمكافحة الجريمة الإلكترونية، أكدت صراحة إمكانية وصلاحيات المكونات المعنوية لأن تكون محلا للضبط، وهذا ما جاء في نص المادة 3/19³ منها، والتي نصت على "...يجب على كل طرف تبني الإجراءات التشريعية التي يراها ضرورية من أجل تخويل هيئاتها المختصة سلطة ضبط أو الحصول بطريقة مشابهة على البيانات المعلوماتية وفقا 1، 2 وهذه الإجراءات تشمل السلطات التالية:

أ- ضبط أو الوصول بطريقة مشابهة إلى نظام معلوماتي أو جزء منه أو إلى دعامات تخزين معلوماتية.

ب- التحقق والتحقق على نسخة من هذه البيانات المعلوماتية.

ج- المحافظة على سلامة البيانات المخزنة .

د- منع الوصول إلى هذه البيانات أو رفعها من النظام المعلوماتي.

¹ - رضا هميسي، المرجع السابق، ص175.

² - وهذا ما ذهب إليه الفقه في لوكسمبورغ إلى أن الضبط يشمل كل الأشياء التي تفيد في إظهار الحقيقة، وبالتالي يمكن ضبط الأدلة المعلوماتية المخزنة في الحاسوب، والإستفادة منها في إظهار الحقيقة. أنظر عبد اللاه أحمد هلاي، المرجع السابق، ص202.

كذلك نجد الولايات المتحدة تتبنى هذا الإتجاه، وأكدت أنه يمكن ضبط سجلات الحاسوب وأن لم يكن لها مظهر مادي محسوس. أنظر سامي جلال فقي حسين، المرجع السابق، ص270.

³ - Art 19/3 du c.c.c dispose que : chaque partie adopte les mesures législatives et autre qui se révèlent nécessaires pour habiliter ses autorités compétentes à saisir ou à obtenir d'une façon similaire les données informatique pour lesquelles l'accès à été réalisé en application des paragraphes 1 ou 2. ces mesures incluent les prérogatives suivantes :

a-saisir ou obtenir d'une façon similaire un système informatique ou une partie de celui -ci ou un support de stockage informatique.

b- réaliser et conserver une copie de données informatique,

c- préserver l'intégrité des données informatiques stockées pertinentes et,

d-rendre inaccessibles ou enlever ces données informatiques du système informatique consulté. » convention sur la cybercriminalité, op cit.

فمن خلال هذه المادة نستنتج أن الاتفاقية إستخدمت المصطلح التقليدي لإجراء الضبط، بما يفيد تطبيق الإجراءات التقليدية المنصوص عليها في قانون الإجراءات الجزائية، كما أضافت إلى جانب ذلك مصطلح "الحصول بطريقة مشابهة" على البيانات لتشير بوجود أساليب أخرى للضبط في البيئة الرقمية بإتخاذ تدابير تقنية والتي لا يسهل الوصول إليها، وعليه فإن الضبط أو الحصول على البيانات عن طريق وسيلة مشابهة، له وظيفتان الأولى تتمثل في جمع الأدلة والثانية مصادرة هذه الأدلة بجعلها غير قابلة للوصول إليها.¹

وهو نفس الإتجاه الذي تبنته الاتفاقية العربية لمكافحة تقنية المعلومات، فحثت الدول الأطراف على سن نصوص تشريعية فيما يخص ضبط وحجز الأدلة الرقمية وقواعد تحريزها، من خلال المادة 27 منها تحت عنوان "ضبط المعلومات المخزنة".²

و أسوة بما تضمنته الاتفاقية الأوروبية ولسد الفراغ التشريعي في هذا المجال، تدخلت عدة دول لتعديل قوانينها في مجال ضبط المعلومات، فوجد المشرع الفرنسي إستحدث بموجب قانون الأمن الداخلي رقم 239 لسنة 2003 فنصت المادة 17-1 الفقرة 03 على أن "المعطيات التي يتم بلوغها في ظل الشروط المنصوص عليها في المادة السابقة يتعين نسخها على دعائم، ودعائم التخزين هذه يتعين تحريزها في أحرار مختومة وفق الشروط المنصوص عليها في هذا القانون".³، أما بالنسبة للمشرع الجزائري فلم يتأخر عن باقي التشريعات المقارنة وبعد تبنيه التفتيش عن بعد كان لزاما عليه إستكمال ما تبقى من فراغ تشريعي فيما يخص الضبط في مجال الجريمة الإلكترونية، فبموجب القانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، سن

¹ - محمد بن فردية، المرجع السابق نص 145.

² - تنص المادة 27 من الاتفاقية العربية لمكافحة تقنية المعلومات على أنه " تلزم كل دولة طرف بتبني الاجراءات الضرورية لتمكين السلطات المختصة من ضبط وتأمين معلومات تقنية المعلومات التي يتم الوصول اليها حسب الفقرة (1) من المادة السادسة العشرون من هذه الاتفاقية هذه الإجراءات تشمل صلاحيات:

أ- ضبط وتأمين تقنية المعلومات أو جزء منها أو وسيط تخزين معلومات تقنية المعلومات.

ب- عمل نسخة من معلومات تقنية المعلومات والاحتفاظ بها.

ج - إزالة أو منع الوصول إلى تلك المعلومات في تقنية المعلومات التي يتم الوصول إليها.

³ - Art (57-1-3) du CPCP dispose que « les données auxquelles il aura été permis d'accéder dans les conditions prévues par le présent article peuvent êtres copiées sur tout supports, les supports de stockage informatique être saisie et placés sous scellés dans les conditions prévues par le présent code. »

إجراءات حديثة وخاصة بضبط المعطيات المعلوماتية تحت عنوان "حجز المعطيات المعلوماتية" ذلك من خلال المادة 6 من نفس القانون، فالملاحظ أن المشرع استعمل مصطلح "الحجز" "saisie" بدلا من الضبط لأن هذه العبارة أكثر تلاءما مع الطبيعة المنطقية للأدلة الإلكترونية¹، فخصص لها مواد تبين كيفية قيام السلطة المختصة بالتفتيش والأساليب المتبعة لضبط الأدلة الرقمية.

الفقرة الثانية: أساليب حجز (ضبط) المعطيات

اعتمد المشرع الجزائري بموجب القانون رقم 04-09 أساليب للحجز منها حجز المعطيات عن طريق النسخ، وحجز المعطيات عن طريق منع الوصول إليها.

أولا: حجز المعطيات عن طريق النسخ

طبقا لأحكام المادة 6 من القانون 04-09 عندما تكتشف السلطة المختصة بالتحقيق أثناء إجراء التفتيش في منظومة معلوماتية، معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة، فإنه يتم حجز هذه المعطيات عن طريق نسخ المعطيات² محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية، تكون قابلة للحجز والوضع في أحرار وفقا للقواعد المعمولة بها في قانون الإجراءات الجزائية، والواردة في نص المادة 84 منه كالإطلاع على المستندات المبحوث عنها، والإحترام التام لمقتضيات وضرورات التحقيق خاصة، إحترام سر المهنة وحقوق الدفاع، وهذا ما جاء في المادة 4/19 من إتفاقية بودابست التي نصت "على سلطة كل دولة طرف أن تتخذ الإجراءات التالية: أن تضبط نظام الكمبيوتر أو جزء منه أو المعلومات المخزنة على أي وسيط من وسائط التخزين الخاصة بالكمبيوتر وأن تحافظ على سلامة تلك المعلومات المخزنة."

ثانيا: الحجز عن طريق منع الوصول إلى المعطيات المعلوماتية

في بعض الأحيان يستحيل نسخ المعطيات على دعامة تخزين إلكترونية، وذلك راجع لأسباب تقنية، كما لو كانت المعطيات مخزنة بأنظمة التشغيل التي لا يمكن نسخها، فأوجب المشرع على السلطة

¹ - جمال إبراهيمي، المرجع السابق، ص58.

² - يتم إستخدام عدة برامج متخصصة في النسخ منها برنامج "lap Link" وهو برنامج يمكن للمحقق من نسخ كل البيانات من حاسوب المتهم الى قرص آخر، من خلال تقنية المنفذ المثالي أو المنفذ الموازي، وهو برنامج مفيد جدا يسمح بنسخ المعطيات بكل أمان ودقة قبل أي محاولة لتدميرها. أنظر حسن طاهر داود، المرجع السابق، ص229.

المكلفة بالتفتيش، إستعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية والموضوعة تحت تصرف الأشخاص المرخص لهم بإستعمال هذه المنظومة، وهذا جاء بموجب المادة 07 من قانون 09-04¹، ويهدف هذا الإجراء الإحترازي الحفاظ على الأدلة الرقمية في محيطها الإلكتروني، والملاحظ أن من مثل هذه الإجراءات هي إجراءات تقنية وليست قانونية، الأمر الذي يتطلب توظيف ضباط شرطة قضائية مختصين في الجانب التقني، لكي يتم توظيفهم على مستوى مصالح الأمن والدرك الوطني، وكذلك ضرورة تكوين قضاة التحقيق ووكلاء الجمهورية في هذا الجانب لمكافحة هذا الاجرام المستحدث.²

ثالثا: المعطيات المحجوزة ذات المحتوى المجرم

منح المشرع بموجب المادة 8 من قانون 09-04 للسلطة التي تباشر التفتيش الحق في إتخاذ الإجراءات اللازمة لمنع الاطلاع على المعطيات، التي يشكل محتواها جريمة كحجب المواقع التي تحتوي شعارات تمس برموز الدولة مثلا، على خلاف المشرع الفرنسي الذي أعطى لوكيل الجمهورية أو قاضي التحقيق، بإعطاء أوامر للقيام بحذف المعطيات نهائيا من الدعائم التي تم نسخها، أو في حالة إستعمالها أو حيازتها تكون مجرمة أو تشكل خطرا على الأشخاص أو الممتلكات، مثل الصور المتعلقة بالإعتداءات الجنسية على القصر³، وبالإضافة إلى هذه التدابير وضع المشرع الجزائري على عاتق مقدم خدمات الأنترنت، جملة من الإلتزامات تساعد سلطات التحقيق على ممارسة مهام التفتيش والضبط على الكيانات المعنوية للحاسب الآلي عندما تستدعي ضرورة التحقيق وهذا ما سنتناوله في المطلب الثالث من هذا المبحث.

وفي الأخير يمكن أن نستخلص أن بالرغم من تدارك المشرع وتبنيه إجراءات التفتيش والحجز فيما يخص الجريمة الإلكترونية المتميزة بالطابع الخاص ووجود طرق حديثة تواكبها، إلا أن الواقع أثبت وجود صعوبات كثيرة مازالت تواجه عملية ضبط الأدلة أهمها:

¹ - تنص المادة 07 من قانون 09-04 على أنه " إذا إستحال إجراء الحجز وفقا لما هو منصوص عليه في المادة 6 أعلاه لأسباب تقنية، يتعين على السلطة التي تقوم بالتفتيش إستعمال التقنيات المناسبة لمنع الوصول إلى المعطيات، التي تحتويها المنظومة المعلوماتية، أو أى نسخها، الموضوعة تحت تصرف الأشخاص المرخص لهم بإستعمال هذه المنظومة."
² - دنيا زاد ثابت، مراقبة الإتصالات الإلكترونية والحق في حرمة الحياة الخاصة في القانون الجزائري، مجلة العلوم الإجتماعية والسياسية، المجلد 5، العدد 1، 2014، ص، ص226-227.

³ - Myriam quémener, Yves charpenel ,op.cit,p179.

- الحجم الهائل للمعلومات المعالجة إلكترونيا، التي تحتويها الشبكة المعلوماتية الواجب فحصها من طرف المحقق، للوصول إلى إستخلاص البيانات التي تصلح كأدلة جنائية وضبطها.
- قد تكون هذه الأدلة في شبكات أو أجهزة تابعة لدولة أجنبية، مما يعيق أجهزة التحقيق الوطنية للوصول إليها وضبطها دون تعاون ومساعدة أجهزة التحقيق التابعة لتلك الدولة.¹
- كما يمكن أن تثار مشكلات بمناسبة ضبط البيانات المخزنة في نظام جهاز الحاسب الآلي أو شبكة المعلومات، مشكلة مدى قبول القاضي النسخة المأخوذة عن تلك البيانات في حالة صعوبة ضبط النسخة الأصلية كدليل إثبات، لأن القضاء في عدة دول خاصة الدول الأنجلو سكسونية يشكك في حجيتها ولا يعتبرها كالنسخة الأصلية لإحتمال التلاعب فيها.²
- ومن الصعوبات التي تعيق الوصول إلى ضبط الدليل الرقمي كذلك تلك الأحزمة الأمنية المفروضة من مستخدم النظام للحد من الدخول والاطلاع على البيانات التي يحتويها هذا النظام، وهذا ما يزيد من صعوبة ضبط الدليل الإلكتروني لعدم معرفة المحقق الجنائي لكلمة السر وشفرات المرور.³

المطلب الثالث: الإستعانة بمزودي الخدمات

لما كان الدليل في الشكل الإلكتروني يمتاز بسرعة التبخر أو التعديل، مما يجعل السلطات المختصة بالبحث والتحري تجد صعوبة في كشف الأدلة الإلكترونية والوصول إليها، هذا ما جعل التشريعات تدرك أنه من الضروري الإستعانة بمزودي الخدمات من أجل حفظ المعطيات التي تفيد في جمع الدليل الإلكتروني، ويعتبر هذا الإجراء من بين السبل الحديثة فيما يتعلق بمكافحة الجريمة الإلكترونية، ويلعب هذا الأخير دورا كبيرا سواء في الوقاية من الجريمة قبل وقوعها، أو حتى في الكشف عن مرتكبيها، وهذا ما تضمنه قرار الجمعية العامة للأمم المتحدة رقم 63/55 المؤرخ في 2001/01/22 والمتعلق بمكافحة إساءة إستعمال تكنولوجيا المعلومات لأغراض إجرامية، وذلك بموجب المادة 9/1 منه والتي ألزمت الدول أن تسمح بالحفظ السريع للمعطيات الإلكترونية المتعلقة بالتحقيقات الجنائية وسرعة الحصول عليها.⁴

¹ - جمال إبراهيمي، المرجع السابق، ص54.

² - أثارت محكمة النقض الفرنسية هذه المسألة في إحدى قراراتها واعتبرت ضبط نسخة من البيانات لا يعد من قبيل الضبط الصحيح بمفهوم المادتين 76-97 من قانون إجراءات جزائية، أنظر جمال إبراهيمي، المرجع نفسه، ص61.

³ - جمال إبراهيمي، المرجع نفسه، ص55.

⁴ - قرار الجمعية العامة للأمم المتحدة رقم 63/55 المؤرخ في 2001/01/22 والمتعلق بمكافحة إساءة إستعمال تكنولوجيا

ونظرا لأهمية هذا الإجراء والدور الهام لمقدي الخدمات، نص المشرع الجزائري عليه بموجب المادتين 10 و 11 من قانون 04-09 من الفصل الرابع تحت عنوان "التزامات مقدمي الخدمات". سوف نتناول من خلال هذا المطلب مفهوم مقدمو الخدمات (الفرع الأول) أهم الإلتزامات المفروضة عليهم في (الفرع الثاني).

الفرع الأول: المقصود بمقدم الخدمات الأنترنت

إن دخول أي فرد إلى شبكة الأنترنت، يمكن أن يتم بطرق عديدة سواء بإستعمال طريق IDSL, ISDN, LEASED، إلا أنه في جميع الأحوال لا بد من وجود مقدم خدمة، ويطلق عليهم كذلك مسميات عديدة، منها متعهدي الوصول، أو مقدم الخدمة، أو مزود خدمة الأنترنت، وينحصر دورهم في إتاحة وصول المستخدم إلى الشبكة، ولكل واحد منهم دوره في إيصال المعلومة.¹

أولاً: تعريف مقدم الخدمات

يعرف مقدم خدمات الأنترنت بأنه "الهيئة أو الجهة في بلد معين تمنح حق إشترك الراغبين في شبكة الأنترنت، أو هو من يقوم بخدمة الإتصال، أو خدمة معالجة البيانات أو خدمة معالجة البيانات، أو خدمة تخزين البيانات، و خدمة الاستضافة، أو التخزين المؤقت أو الربط بالشبكات."² وقد عرفت منظمة التنمية الإقتصادية في تقريرها الصادر في أبريل 2010 حول الدور الإقتصادي والإجتماعي لوسطاء الأنترنت بأنهم "يقومون بعقد أو تسهيل المعاملات بين الغير على الأنترنت، ويوفرون إمكانية الدخول، ويستضيفون، وينقلون، وينقلون ويفهرسون المحتويات، والمنتجات والخدمات، التي أنشأها الغير على الأنترنت، أو يقدمون للغير خدمات تستند إلى الأنترنت."³

كما عرفت إتفاقية بودابست مقدمي الخدمات بموجب، المادة 01/ج التي تنص على "يقصد بمزودي الخدمات:

- أي كيان عام أو خاص الذي يوفر لمستخدميه القدرة على التواصل من خلال النظام المعلوماتي.

المعلومات لأغراض إجرامية.

¹ - عبد اللاه أحمد المراغي، المسؤولية الجنائية لمقدمي خدمات الأنترنت، مجلة حقوق حلوان للدراسات القانونية والإقتصادية، د.ع، د.س ن، ص 132.

² - دلال مولاي ملياني، إشكالية الإثبات في الجريمة الأنترنت، المرجع السابق، ص 117.

³ - Deprez, responsabilité des fournisseurs de revete sur internet ,expertise,1997,p 183.

- أي كيان آخر يقوم بمعالجة أو تخزين البيانات الحاسوبية لخدمة الاتصالات أو لخدمة مستخدميه...¹، وما يمكن ملاحظته أن هذه الإتفاقية قسمت مقدم الخدمة إلى طائفتين، الطائفة الأولى تتمثل في مزودو خدمة الاتصالات، أما الطائفة الثانية فتشمل كل من يقدم للجمهور خدمة معالجة أو تخزين المعلومة.

كما أعطت الإتفاقية العربية لمكافحة جرائم تقنية المعلومات تعريفا لمقدم الخدمة بأنه "أي شخص طبيعي أو معنوي عام أو خاص يزود المشتركين بالخدمات للتواصل بواسطة المعلومات، أو يقوم بمعالجة أو تخزين المعلومات نيابة عن خدمة الاتصالات أو مستخدميه".²

بالعودة للمشرع الجزائري نجده عرفها في المادة 02/د من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، التي جاء فيها "يقصد في مفهوم هذا القانون ما يأتي...

د- مقدمو الخدمات:

- أي كيان عام أو خاص يقدم لمستعملي خدماته، القدرة على الإتصال بواسطة منظومة معلوماتية و/أو نظام اتصالات.

- وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها.³ وما يمكن ملاحظته أن تعريف المشرع الجزائري هو نفسه تعريف إتفاقية بودابست وهذا طبيعي لأن كل أحكام القانون السابق الذكر مستوحاة من هذه الإتفاقية، كما بين هذا التعريف الجوانب التقنية لمقدمي خدمة الأنترنت فقط، بالرغم من وجود جهات أخرى تقوم بتوريد خدمات المحتوى

¹ - Art1- définitions

Aux fins de la présente convention, l'expression ...

c-« fournisseurs de service désigne :

i-toute entité publique ou privée qui offre aux utilisateurs ses services la possibilité de communiqué au moyen d'un système informatique.

ii-toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou aux ses utilisateurs. » Convention sur la cybercriminalité, op, cit.

² - المادة 3/02 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات .

³ - وهو نفس التعريف لمقدم الخدمات الوارد في المادة 1/3 من القانون رقم 18-07 المؤرخ في 10/06/2018 المتعلق بحماية الأشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي.

المعلوماتي في شبكة الأنترنت إلى الجمهور ويعتبر أهم مصدر للتدفق المعلوماتي، وجهات أخرى مهمتها تخزين التطبيقات والسجلات المعلوماتية، وتمدهم بالوسائل التقنية والمعلوماتية التي تمكنهم من الوصول إلى ذلك المخزون عبر شبكة الأنترنت،¹ مما يؤدي إلى القول بأن المشرع لم يبين الأصناف المختلفة لمقدمي الخدمات بعكس بعض التشريعات كالتشريع الفرنسي الذي تعرض لتعريف كل من متعهد الإيواء، وكذا مقدم خدمات الإستضافة وذلك بموجب المادة 1/6 و 2 من القانون رقم 575-2004 المتعلق بالثقة في الإقتصاد الرقمي.²

ثانيا: أصناف مقدم خدمات الأنترنت

على إثر الدور الهام التي يقوم بها مزود خدمات الأنترنت، يمكن تصنيف مقدمي خدمة الأنترنت إلى:

1- متعهد الوصول أو مقدم خدمة الدخول Fournisseur d'accès

يسمى كذلك متعهد الدخول، مورد الدخول، وقد يكون شخصا من أشخاص القانون العام أو جمعية أو شركة تجارية، ويتمثل دوره في توفير إمكانية الإتصال بشبكة الأنترنت للجمهور، وعن طريقه يتم إتصال مستخدم الأنترنت بالمواقع التي يرغبون الدخول إليها، بعد إمدادهم بالوسائل المادية التي تمكنهم من إستخدام شبكة الأنترنت.³

وقد نظم المشرع الجزائري الخدمات التي يؤديها مقدم خدمة الوصول في المادة 1/د من قانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، فحدد مقدمي الخدمات بأنهم " أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية أو نظام للإتصالات"، ومن أمثلة خدمات الوصول في الجزائر "Djawab" و "fawri"

¹ - عبد القادر عمير، المرجع السابق، ص 339.

² - 1. ART 6 du loi n°2004-575 du 21 juin pour la confiance dans l'économie numérique : « Les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne informent leurs abonnés de l'existence de moyens techniques permettant de restreindre l'accès à certains services ou de les sélectionner et leur propose au moins un de ces moyens....

2-les personnes physiques ou morales qui assurent, même à titre gratuit ,pour mise à disposition du public par des services de communication au public en ligne ,le stockage des signaux ,d'écrits , d'image ,de sons ou message de toute nature. »

³ - محمد عبد الظاهر حسين، المسؤولية القانونية في مجال شبكات الأنترنت، دار النهضة العربية، القاهرة، د ط، 2004، ص 37.

في القطاع العام Assila Box EEPAD, في القطاع الخاص¹.

فدور مزود الخدمة فني كأصل عام، فهو لا يقوم بتوريد المعلومة، وإنما يتعهد بوضعها على الموقع وتسهيل إمكانية الإطلاع عليها من خلال المنفذ الذي أعده لهذا الغرض، وبالتالي لا يكون على علم بالمعلومات المنقولة على شبكة الأنترنت.²

2- متعهد الإيواء Fournisseur d'hébergement

يطلق عليه إسم مقدم خدمة الإيواء، أو مورد الإيواء، ومتعهد الإيواء وهذا المصطلح الأخير هو أكثر المصطلحات شيوعا، وهو قد يكون شخصا طبيعيا أو شخصا معنويا، كالشركات التجارية أو الجامعات أو المؤسسات العامة التي تقوم بإيواء صفحات الويب (web) كحساباتها الخاصة serveur، ويتم ذلك غالبا بمقابل أجر، فهو بمثابة مؤجر لمكان على الشبكة للمستأجر (الناشر)، والذي ينشر ما يريد من نصوص أو صور أو ينظم مؤتمرات مناقشة أو ينشئ روابط معلوماتية من المواقع الأخرى³، وعرفه المشرع الجزائري بموجب القانون رقم 04-09 بنص المادة 2/د على أنه "أي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الإتصال المذكورة أو لمستعملها".

3- مورد المعلومة Fournisseur d'informations

هو شخص طبيعي أو معنوي، يقوم ببث المعلومات والرسائل المتعلقة بموضوع معين على الأنترنت، بحيث يتمكن مستخدم هذه الشبكة، من الحصول عليها مجانا أو بمقابل مادي⁴، ويعتبر القلب النابض لبث الحياة في هذه الشبكة، وهو يملك رقابة مشروعية هذه المعلومات، و التحكم في بثها عبر الأنترنت، ويقوم بتحميل النظام بالمعلومات التي قام بتأليفها، أو جمعها حول موضوع معين، كما يتولى جمع وتوريد المادة المعلوماتية لإيصالها إلى المستخدم.⁵

¹ - فاطمة الزهراء عكو، المسؤولية المدنية لمقدمي الخدمة الوسيطة في الأنترنت، أطروحة لنيل شهادة دكتوراه في القانون، كلية الحقوق، جامعة الجزائر 1، الجزائر، 2014-2015، ص 26.

² - محمد عبد الظاهر حسين، المرجع السابق، ص 38.

³ - جميل عبد الباقي الصغير، الأنترنت والقانون الجنائي، المرجع السابق، ص 155.

⁴ - Feral-schuhl Christiane, cyber droit, le droit à l'épreuve de l'internet, 3em édition, dunod, paris, 2002, p129.

⁵ - عبد الفتاح محمود كيلاني، مدى المسؤولية القانونية لمقدمي خدمة الأنترنت، دار الجامعة الجديدة، مجلة الفكر

القانونية الإقتصادية جامعة بنها، 2011، ص 487. مقال منشور على الموقع الإلكتروني

4- ناقل المعلومة

هو عبارة عن عمل فني يقوم من خلاله العامل له سواء كان شخصا طبيعيا أو معنويا، بالربط على شكل (Bucket) وهذا من جهاز المستخدم إلى الحاسب الخادم لمتعهد الوصول، ثم تحويلها من هذا الحاسب الأخير إلى الحاسبات المرتبطة بمواقع الأنترنت.¹

5- ناشر خدمة الشبكة المعلوماتية

يقوم هذا الأخير بإنشاء موقع على الشبكة وتحريرها²، ويسمح فيه بإضافة أشخاص، وتلقي برامج ومعلومات وتطبيقات من قبلهم، بالإضافة إلى قيامه بتدوين المحتوى، وتحريره وصياغته وإرساله إلى موقع إلكتروني، وجعله متاح أمام مستخدمي الشبكة بشروط وأحكام وضوابط.³

وفي الأخير بعد التعريف بأهم أصناف مقدمو الخدمات بصورة عامة ومختصرة، نتساءل إن كان هناك التزامات تقع على عاتق هؤلاء؟ وهذا ما نتناوله في هذا الفرع.

الفرع الثاني: إلتزامات مقدمي خدمات الأنترنت

حدد المشرع الجزائري الإلتزامات الواقعة على كل من مقدمي الخدمات، في مجال الإتصالات الإلكترونية من أجل الوقاية والحيلولة من إرتكاب الجرائم الإلكترونية، وهي إلتزامات عامة (أولا) كما أوجب إلتزامات خاصة بمقدمي خدمة الدخول إلى الأنترنت، وهي إلتزامات خاصة (ثانيا) وذلك بموجب القانون رقم 04-09.

أولا: إلتزامات مزود الخدمات (إلتزامات عامة)

نص قانون 04-09 على مجموعة من الإلتزامات التي تقع على مقدمي الخدمات المتمثلة في مساعدة السلطات القضائية المختصة في التحريات القضائية.

¹ - فاطمة الزهراء عكو، المرجع السابق، ص154. <http://www.flaw.bu.ed.eg./flaw/images/parts2.pdf> أطلع عليه يوم 25/10/2018 على الساعة 00:14h.

² - Myriam quémener, yves charpenel, op.cit,p44

³ - دلال مولاي ملياني، إشكالية الإثبات في جرائم الأنترنت، المرجع السابق، ص124.

1 - مساعدة السلطة القضائية المختصة

نصت المادة 10 من القانون 04-09 على هذا الالتزام، وتقابلها المواد 16 و 17 من إتفاقية بودابست الخاصة بمكافحة الجرائم الإلكترونية، وكذا المواد 23، 24، و 25 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، وبالرجوع إلى المادة 10 التي ألزمت مقدمو الخدمات بتقديم المساعدة للسلطات المكلفة بالتحريات القضائية، لجمع وتسجيل المعطيات بمحتوى الاتصالات أيا كانت، (مكالمات صوتية هاتفية أو مكالمات فيديو عبر مواقع الأنترنت SMS , EMAIL , MMS) ، ولكنه إشتراط أن تكون في حينها، كما أن المشرع الجزائري لم يشر إلى الأشخاص المكلفين بتسخير مقدمو الخدمات، للقيام بهذا الإجراء ولم يحدد المدة الزمنية، لتسجيل هذه الاتصالات وتركها مفتوحة، عكس المشرع الفرنسي الذي سمح لضباط الشرطة القضائية بتسخير من وكيل الجمهورية، مع ترخيص مسبق من قاضي الحريات والحبس، بتسخير مقدمي الخدمات عبر الأنترنت للقيام بكل الإجراءات، التي تؤمن الحفظ لمدة سنة وهذا ما تضمنته المادة 60فقرة 2 من قانون الإجراءات الجزائية الفرنسي، ونستنتج من ذلك أن المشرع الفرنسي يكفل ضمانات لحماية الحياة الخاصة للأفراد عند القيام بهذا الإجراء¹، لهذا ندعو المشرع الجزائري تدارك الأمر والسير على نهج المشرع الفرنسي.

كما أوجبت المادة 10 في فقرتها الثالثة من القانون 04-09 على ضرورة أن يلتزم مقدمو الخدمات كتمان السر المهني عند القيام بأي العمليات التي ينجزونها بطلب من المحققين، وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق، ولعل الغرض من هذا الإلتزام هو ضمان حماية الحق في الخصوصية، وكذا تجنب إحداث تغيير في البيانات أو محوها من طرف أشخاص آخرين.²

2 - حفظ المعطيات المتعلقة بحركة السير

نظم المشرع الجزائري هذا الإلتزام بمقتضى القانون 04-09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، فألقت المادة 11 منه على عاتق مقدمي الخدمات إلتزاما آخر

1- مريم أحمد مسعود، آليات مكافحة جرائم تكنولوجيا الإعلام والاتصال في ضوء القانون رقم 04-09، مذكورة لنيل شهادة الماجستير، كلية الحقوق و العلوم السياسية، جامعة قاصبي مرياح، ورقلة، 2012-2013، ص 101.

2 - جمال إبراهيمي، المرجع السابق، ص 112.

يتمثل بحفظ المعطيات المتعلقة بحركة السير، والتي عرفت بموجب المادة 2 ف (هـ) من القانون 09-04 بأنها "أي معطيات متعلقة بالإتصال عن طريق منظومة معلوماتية، تنتجها هذه الأخيرة بإعتبارها جزء من حلقة الإتصالات، توضيح مصدر الإتصال والوجهة المرسل إليها والطريق الذي يسلكه، ووقت وتاريخ وحجم مدة الإتصال، ونوع الخدمة".¹ بإستقراء المادة 11 من القانون السالفة الذكر حدد المشرع الجزائري على سبيل الحصر المعطيات الواجب حفظها من طرف مقدمي الخدمات وهي:

- المعطيات التي تسمح بالتعرف على مستعملي الخدمة.
- المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال.
- الخصائص التقنية وكذا تاريخ ووقت ومدة كل إتصال.
- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها .
- المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الإتصال وكذا عناوين المواقع المطلع عليها.

بالنسبة لنشاطات الهاتف، يقوم المتعامل بحفظ المعطيات التي تسمح بالتعرف على مستعملي الخدمة، وكذا تلك التي تسمح بالتعرف على مصدر الإتصال وتحديد مكانه.

وقد حدد المشرع مدة حفظ المعطيات المذكورة في المادة 11 من القانون 09-04 بسنة واحدة إبتداء من تاريخ التسجيل، وذلك حفاظا على حرمة الحياة الخاصة للأفراد، وكما يهدف هذا الإجراء لمساعدة ومنح الوقت الكافي للسلطات القضائية المختصة، بمواصلة البحث والتحري بهدف الوصول إلى مرتكب الجريمة.

ثانيا: إلتزامات مقدم خدمة الإنترنت(الإلتزامات خاصة)

إلى جانب الإلتزامات المفروضة على مقدمي الخدمات، بموجب المادة 11 من ق 09-04 المتمثلة في مساعدة السلطة المختصة، وحفظ المعطيات المتعلقة بحركة السير، فجاءت المادة 2/12 لتضيف إلتزامين فرضته على مقدم خدمة الإنترنت وتتمثل في:

¹ - المادة 2/هـ من القانون رقم 09-04 المتعلق بالوقاية من الجرائم المصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

1 - التدخل الفوري لسحب المحتويات أو منع الوصول إليها

ألزم المشرع الجزائري مقدمو خدمة الأنترنت بالتدخل الفوري، في حالة علمهم بطريقة مباشرة أو غير مباشرة بالمحتوى المخالف للنظام العام والآداب العامة، وذلك بسحبه من التداول ثم تخزينه أو حفظه لينتأى للمحققين إتخاذ كدليل إثبات،¹ أو جعل الدخول إليه غير ممكن، والإخلال بهذا الإلتزام يعرض مقدم خدمة الأنترنت للمساءلة الجزائية، طبقا لما جاء في المادة 398 مكرر 8 من قانون العقوبات²، في حالة عدم وضع حد للأنشطة غير المشروعة، سواء تم بناء على إعدار من الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، أو صدور قرار قضائي من السلطات القضائية.

2 -وضع الترتيبات التقنية لحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات

نجد المشرع من خلال نص المادة 12 من القانون 04-09 نص على منع المواقع التي تنشر أو تبث محتويات مضامينها غير مشروعة، وبالتالي فهي مخالفة للنظام العام والآداب العامة، ومن ثم ألزم المشرع مقدمو خدمة الأنترنت بحصر إمكانية الدخول إليها، وذلك بوضع ترتيبات تقنية تكون من خلالها كشف تلك المواقع التي تحتوي مضامين غير مشروعة، وما يمكن ملاحظته أن هذا الإلتزام هو نفسه الإلتزام المفروض على مقدمي خدمات الأنترنت، بموجب الفقرة الأخيرة من المادة 14 من المرسوم التنفيذي 98-257 المؤرخ في 25/08/1998، التي تؤكد على ضرورة إتخاذ كل الإجراءات اللازمة لتأمين حراسة دائمة لمضمون الموزعات المفتوحة لمستخدميه، قصد منع النفاذ إلى الموزعات التي تحتوي معلومات تتعارض مع النظام العام.

الفرع الثالث: مسؤولية مقدمي الخدمات

ظهرت عدة آراء وإتجاهات فقهية، حول إمكانية تحميل المسؤولية الجنائية لمقدمي الخدمات عن الجرائم الإلكترونية المرتكبة وانقسمت هذه الآراء إلى:

- الرأي الأول

ذهب أصحاب هذا الإتجاه إلى القول بعدم المسؤولية الجنائية لمقدمي الخدمات، وحثهم في ذلك

¹ - محمد بعجي، المرجع السابق، ص 27 .

² - القانون رقم 16-02 المؤرخ في 19 يونيو 2016 يتم الأمر 66-156 المؤرخ في 8 يونيو 1966، المتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، عدد 37، الصادرة بتاريخ 22 يونيو 2016.

أن دور مقدم الخدمة يقتصر على ربط المستخدم بالموقع الذي يريده عبر الشبكة، فهو مجرد دور فني لا يتضمن أية رقابة على محتوى الموقع الذي يختاره المستخدم بمحض إرادته¹، وحتى تقوم المسؤولية في حقه يتطلب أن يكون له دور إيجابي في بث المحتوى المجرم، وهو الأمر المنعدم في هذه الحالة لأنه يملك الوسائل الفنية التي تمكنه من مراقبة ملايين المعلومات،² وهذا الاتجاه أخذ به الفقه والقضاء الإيطالي اللذان يذهبان إلى عدم مسؤولية مقدم الخدمة، لأنه لا يقوم بتوريد المعلومات ولكنه يؤمن خدمة الوصول إليها فقط.³

- الرأي الثاني

أما أصحاب هذا الاتجاه ذهبوا إلى القول، بأن مقدمو الخدمات يتحملون المسؤولية على أساس قواعد المسؤولية الجنائية، طبقا لأحكام مسؤولية التابع عن أفعال المتبوع، وذلك لأن المشرع أقام نظاما يتعلق بكيفية النشر على الأنترنت، ومزود الخدمة حلقة في هذه السلسلة، لذلك فهو ملزم بمحو المعلومات غير المشروعة، كما لا يعتد بعدم علمه بهذه المواد على إعتبار أنه موزع للمادة المعلوماتية، لكن يصعب أيضا قبول هذا الرأي لأن متعهد الخدمة ما هو إلا مجرد وسيط فني، يقتصر دوره على تمكين المشترك من ولوج شبكة الأنترنت أو الخدمة وبالتالي لا يمكن مساءلته جنائيا.⁴

-الرأي الثالث

يرى أنصار هذا الرأي عدم مسؤولية متعهد الخدمة مطلقا، لكن يتوقف الأمر على طبيعة الدور الذي يقوم به، ولاسيما وأنه يقوم بأدوار متعددة، فقد يكون متعهدا للإيواء، وقد يكون ناقلا للمعلومات، أو لمجموعات الإخبارية على صفحات التواصل الإجتماعي عبر شبكة الأنترنت، وعليه ووفقا لهذا الرأي لو كان متعهدا لخدمة مجرد ناقل فلا تقوم المسؤولية الجنائية عن مراقبة المادة المعلوماتية، التي يتم نقلها أما إذا كان دوره غير ذلك فيسأل جنائيا، وعليه يسأل مزود الخدمة إذا كان عالما بمحتوى المادة المجرمة

¹ - محمد حسين منصور، المسؤولية الإلكترونية، دار الجامعة الجديدة الاسكندرية، د ط، 2003، ص 13 .

² - محمد عبد الظاهر حسين، المرجع السابق، ص 38.

³ - Lebrun (n) et Mboutcha (e), évolution de la responsabilité des intermédiaires technique en Italie in, <http://www.juriscom.net/ variations/ responsabilité des intermédiaires technique en Italie. Html> 2.

مشار إليه عند عبد الفتاح محمود الكيلاني، مدى المسؤولية القانونية لمقدمي خدمات الأنترنت، المرجع السابق، ص 476.

⁴ - جميل عبد الباقي الصغير، المرجع السابق، ص 132.

المنشورة عبر الخدمة التي يوفرها أو كان هو من طلبها أو قام بتعديلها.¹

أما بالنسبة للمشرع الجزائري أقر بالمسؤولية الجنائية لمقدمي خدمة الأنترنت، وهذا ما تضمنته المادة 394 مكرر 8 والتي نصت على "دون الإخلال بالعقوبات الإدارية المنصوص عليها في التشريع والتنظيم الساري المفعول، يعاقب بالحبس من سنة (1) إلى ثلاث (3) سنوات وبغرامة من 2000.000 دج إلى 10.000.000 دج أو بإحدى هاتين العقوبتين فقط، مقدم خدمات "الأنترنت" بمفهوم المادة 2 من القانون رقم 04-09 المؤرخ في 5 أوت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الذي لا يقوم رغم إعداره من الهيئة الوطنية المنصوص عليها في القانون المذكور أو صدور أمر أو حكم قضائي يلزمه بذلك

أ - بالتدخل الفوري لسحب أو تخزين المحتويات، التي تتيح الإطلاع عليها أو جعل الدخول إليها أو جعل الدخول إليها غير ممكن عندما تتضمن محتويات تشكل جرائم منصوص عليها قانونا.

ب - وضع ترتيبات تقنية تسمح بسحب أو تخزين المحتويات التي تتعلق بالجرائم المنصوص عليها في الفقرة (أ) من هذه المادة أو جعل الدخول إليها غير ممكن.²

وكذلك أقر بالمسؤولية لمقدمي خدمة الأنترنت، وذلك بموجب نص المادة 14 من المرسوم التنفيذي رقم 98-257 المؤرخ في 25/08/1998 المتعلق بضبط شروط وكيفيات إقامة خدمات الأنترنت واستغلالها، كذلك المادتان 11 - 12 من ق 04-09 وذلك إعتماذا على مبررات واقعية مقبولة نظرا لإساءة إستخدام هذا الفضاء السيبراني بما يخالف النظام العام والآداب العامة، ووقاية المجتمع خطر الجريمة الإلكترونية.³

وبالرجوع إلى المادة 8/11 من قانون 04-09 والتي تنص على "... دون الإخلال بالعقوبات الإدارية المترتبة على عدم إحترام الإلتزامات المنصوص عليها في هذه المادة تقوم المسؤولية الجزائية للأشخاص الطبيعية والمعنويين عندما يؤدي ذلك إلى عرقلة حسن سير التحريات القضائية، ويعاقب

¹ - يزيد بوحليط، المرجع السابق ص 328.

² - قانون رقم 16-02 المؤرخ في 19/07/2016 يتم الأمر رقم 66 - 156 المؤرخ في 8/07/1966 والمتضمن قانون العقوبات، الجريدة للجمهورية الجزائرية، عدد 37، الصادرة بتاريخ 27/07/2016.

³ - يزيد بو حليط، المرجع السابق، ص 328.

الشخص الطبيعي بالحبس من ستة (6) أشهر خمس (5) سنوات وبغرامة من 50.000 دج إلى 500.000 دج.

ويعاقب الشخص المعنوي بالغرامة وفقا للقواعد العامة المقررة في قانون العقوبات ومن جانب آخر عاقب المشرع على إفشاء الأسرار بمناسبة تأدية مهامهم بموجب المادتين 301-302 من ق.ع.ج.

ومن ثم يمكن القول أن مقدمو الخدمات يلعبون دورا كبيرا للوقاية من الجريمة أو الحيلولة دون إرتكاب تلك الجرائم، من خلال الإلتزامات سواء العامة أو الخاصة، التي فرضها المشرع الجزائري عليهم، وإن الإخلال بهذه الإلتزامات المفروضة عليهم تؤدي إلى قيام المسؤولية الجزائية تجاه مقدمو الخدمات وهذا ما أقره المشرع الجزائري.

المطلب الرابع: إنشاء الهيئات والأجهزة الوطنية للوقاية ولمكافحة الجريمة الإلكترونية

فرضت الجريمة الإلكترونية على المشرع الجزائري، إستحداث هيئات وأجهزة متخصصة سواء للوقاية أو لمواجهة الظاهرة المستحدثة، وهي آليات تابعة لمختلف المؤسسات التي لها علاقة بمكافحة الجريمة، إكتشافها ومعرفة طبيعتها وكذا كيفية الوقاية منها ميدانيا، والمتمثلة في الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، المصلحة المركزية لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام وأتصال التابعة للمديرية العامة للأمن الوطني، ومركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني، وأخيرا المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني.

الفرع الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها

تم إنشاء هذه الهيئة بموجب المادة 13 من قانون رقم 04/09 المؤرخ في 5 أوت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، والتي نصت على "تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال وتحدد تشكيلة الهيئة وتنظيمها وكيفية سيرها عن طريق التنظيم."، ولكن ما يمكن ملاحظته أن المبدأ المكرس في النظام الدستوري والقانون الجزائري أن الإحالة على التنظيم يعني صدور مرسوم تنفيذي من الطرف الوزير الأول، لكن بالنسبة للهيئة الوطنية فقد تم إصداره بموجب مرسوم رئاسي بدلا من مرسوم تنفيذي، وذلك يعتبر تعديا

على إختصاصات الوزير الأول¹، وبحلول سنة 2015 صدر المرسوم الرئاسي رقم 15-261 المتضمن تشكيل الهيئة وتنظيمها وكيفية سيرها²، لكن تم إلغاء هذا المرسوم، وصدر المرسوم الرئاسي آخر يحمل رقم 19-172³ المتضمن تحديد تشكيلة الهيئة للوقاية من الجرائم المتصلة بالإعلام والاتصال، وتم إلحاقها بوزارة الدفاع الوطني بعدما كانت خاضعة للوزير المكلف بالعدل في ظل المرسوم الرئاسي رقم 15 - 261 الملغى، ويرى الخبراء أن إتخاذ هذا القرار بسبب فشل هذه الأخيرة من كبح جماح الجريمة الإلكترونية، وكذا أن وزارة الدفاع تمتلك تجهيزات متطورة في مجال مكافحة الجوسسة والتتصت⁴، وكيفها على أنها مؤسسة عمومية ذات طابع إداري، وتتمتع بالشخصية المعنوية والاستقلال المالي.

و مرة أخرى ألغي هذا المرسوم، وصدر المرسوم الرئاسي 20-183 المؤرخ في 13 يوليو 2020 لتسترجع صفتها الأولى كسلطة إدارية مستقلة تتمتع بالشخصية المالية بموجب المادة 02 من المرسوم الرئاسي رقم 20-183 وتخضع الهيئة تحت سلطة رئيس الجمهورية، فلم يستقر على العمل بهذا المرسوم فصدر المرسوم الرئاسي رقم 21-439 المؤرخ في 2021/11/07 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها⁵، مما يجعلنا لا ندرك وعدم فهم توجه المشرع في هذا الأمر، لكن أحسن المشرع في إبقاء الهيئة على أنها سلطة إدارية مستقلة، وحدد مقر الهيئة بمدينة الجزائر، وأضاف أنه يمكن نقل مقرها إلى مكان آخر من التراب الوطني بموجب

¹ - إلهام خرشي، النظام القانوني للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، مجلة البحوث القانونية والسياسية، المجلد 04، العدد 01، 2022، ص 61.

² - المرسوم الرئاسي رقم 15-261 المؤرخ في 2015/10/8، يحدد تشكيلة وتنظيم وكيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكاف، الجريدة الرسمية للجمهورية الجزائرية عدد 52، الصادرة بتاريخ 2015/10/08.

³ - المرسوم الرئاسي رقم 19 - 172 المؤرخ في 2019.06.06، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، عدد 37 الصادرة بتاريخ 2019/06/06.

⁴ - حكيمة ذهبي، خبراء يشرحون أسباب التغيرات التي طرأت على الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، مقال منشور على الموقع [http / m . elilad . net / art....](http://m.elilad.net/art....) بتاريخ 2019/06/26 وأطلع عليه يوم 2019/08/25 على الساعة 15:45.

⁵ - المرسوم الرئاسي رقم 21-439 المؤرخ في 2021/11/07، المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، عدد 86، الصادرة بتاريخ 2021/11/11.

مرسوم رئاسي وهو الأمر الذي لم يكن منصوصا عليه في المادة الثالثة من المرسوم الرئاسي رقم 15-261 الملغى، بل كان مقرر إنشاء ملحقات جهوية¹، وذلك بمقتضى المادة 11 من المرسوم نفسه، وعلى ضوء المرسوم الرئاسي رقم 21-439 الذي يحدد تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال تتطرق لتشكيلية (أولا) ومهامها (ثانيا).

أولا: تشكيلية الهيئة الوطنية

تضم الهيئة من حيث تشكيلتها مجلس توجيه ومديرية عامة، يوضعان تحت السلطة المباشرة لرئيس الجمهورية مع تقديم عرضا لنشاطهما.²

1- مجلس التوجيه

أ- تشكيلته

يتشكل مجلس التوجيه بموجب المرسوم الرئاسي 21-439 المؤرخ في 7/11/2021 من مجموعة من الأعضاء، هم الأمين العام لوزارة الشؤون الخارجية والجالية الوطنية بالخارج، الأمين العام لوزارة الداخلية والجماعات المحلية والهيئة العمرانية، الأمين العام لوزارة العدل، الأمين العام لوزارة البريد والمواصلات السلكية واللاسلكية، المدير العام للأمن الداخلي، قائد الدرك الوطني، المدير العام للأمن الوطني، والمدير المركزي لأمن الجيش لأركان الجيش الوطني، الشعبي، وممثل عن رئيس مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة لأركان الجيش الوطني الشعبي، وأيضا ممثل عن رئاسة الجمهورية، يعينه رئيس الجمهورية، ويتولى الأمين العام لرئاسة الجمهورية رئاسة مجلس التوجيه، أما أمانة المجلس يتولاها المدير العام للهيئة.³

¹ - حسب المادة 08 من القرار الوزاري المشترك المؤرخ في 17/12/2017، الذي يحدد التنظيم الداخلي لهيكل الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الصادر بالجريدة الرسمية للجمهورية الجزائرية عدد 14 والمصادرة بتاريخ 04/03/2018، تتكون الملحقة الجهوية من أربعة مكاتب: مكتب الإدارة العامة، المراقبة الإلكترونية، مكتب المتابعة والتحليل، ومكتب العمليات التقنية.

² - المادة 05 من المرسوم الرئاسي 21-439.

³ - المادة 06 من المرسوم الرئاسي 21-349.

ب - مهامه

يدل مهام المجلس من إسمه، حيث تضمنت المادة 7 من المرسوم الرئاسي 21-439 على المهام الموكلة إليه فيكلف بتوجيه عمل الهيئة والإشراف عليه ومراقبته، كما يقوم بدراسة كل مسألة تخضع لمجال إختصاص الهيئة لاسيما فيما يتعلق بتوفر شروط اللجوء إلى المراقبة الوقائية للاتصالات الإلكترونية المنصوص عليها في المادة 4 من القانون رقم 04-09 المؤرخ في 5 أوت 2009، كذا المداولة حول الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، والتباحث حول مسائل تطوير التعاون مع المؤسسات والهيئات الوطنية والأجنبية المعنية بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال، مع القيام دوريا بتقييم حالة التهديد في مجال الجرائم الإلكترونية، للتأكد من تحديد مضامين العمليات الواجب القيام بها والأهداف المنشودة بدقة، مع إقتراح كل نشاط يتصل بالبحث وتقييم الأعمال المباشرة في مجال الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

إلى جانب هذه المهام يكلف مجلس التوجيه، بإعداد نظامها الداخلي والمصادقة عليه، و كذا الموافقة على برنامج عمل الهيئة، كما يقوم بدراسة تقارير سنوية لنشاطات الهيئة والمصادقة عليه مع إبداء رأيه في كل مسألة تتصل بمهام الهيئة.¹

وللقيام بالمهام الموكلة إليه، فإن مجلس التوجيه يجتمع مرة واحدة في السنة في دورة عادية، بناء على إستدعاء من رئيسه، كما يمكنه الإجتماع في دورة غير عادية كلما كان ذلك ضروريا، بناء على إستدعاء من رئيسه، أو بطلب من أحد أعضائه، أو من المدير العام للهيئة، كما يعد مجلس التوجيه تقريرا بعد كل دورة.²

2- المديرية العامة

يتولى إدارتها مدير عام يعين بموجب مرسوم رئاسي، وتنتهى مهامه بنفس الطريقة، وتعد وظيفة المدير العام وظيفة عليا في الدولة³، وتضم المديرية العامة، مديرية للمراقبة الوقائية واليقظة الإلكترونية، المديرية للإدارة والوسائل، ومصلحتان هما مصلحة الدراسات والتخليص، ومصلحة التعاون واليقظة

¹ - المادة 7 من المرسوم الرئاسي رقم 21-439.

² - المادة 8 من المرسوم الرئاسي 20 - 183.

³ - المادة 9 من المرسوم الرئاسي 21-3-439.

التكنولوجية إضافة إلى وجود ملحقات جهوية.¹

حيث يمتلك المدير العام العديد من الصلاحيات للسير الحسن للهيئة، وهذا ما جاءت به المادة 10 من المرسوم 21-439 السالفة الذكر أهمها، يمكنه إقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، كما يسهر على تنفيذها، إلى جانب إقتراح مخطط عمل الهيئة والسهر على تنفيذه، مع تنشيط أعمال هياكل الهيئة وتنسيقها ومتابعتها ومراقبتها، تحضير إجتماعات مجلس توجيه الهيئة، وكذلك السهر على إحترام قواعد حماية السر المهني في الهيئة، ويمثل الهيئة لدى القضاء وفي جميع أعمال الحياة المدنية، وكذا تمثيلها لدى السلطات والمؤسسات الوطنية والدولية، والسهر على القيام بإجراءات التأهيل وأداء اليمين فيما يخص المستخدمين المعنيين في الهيئة، بالإضافة إلى إعداد مشروع النظام الداخلي للهيئة وكذا مشروع ميزانيتها، لضمان التسيير المالي والإداري للهيئة، و إعداد التقارير الدورية لنشاطات الهيئة ورفعها إلى رئيس مجلس التوجيه.²

ألزمت الفقرة الأخيرة من المادة 10 من نفس المرسوم، أن يقوم المدير العام للهيئة بإخطار رئيس الجمهورية فوراً، عن كل حادثة من شأنها المساس بأمن الدولة، أو تلك المرتبطة بالأعمال الإرهابية أو التخريبية، كما يخطر أيضاً رئيس أركان الجيش الوطني الشعبي، عندما يتعلق بمسائل تخص الدفاع الوطني.

أ - مديرية المراقبة الوقائية واليقظة الإلكترونية

أشارت المادة 12 من المرسوم الرئاسي 21-439 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، على أن مدير المراقبة الوقائية واليقظة يعين بموجب مرسوم رئاسي بناء على إقتراح من المدير العام للهيئة، وتنتهى مهامه بنفس الأشكال، وحددت المادة 14 من ذات المرسوم المهام الموكلة لها، فهي تكلف بتنفيذ عمليات المراقبة الوقائية للاتصالات الإلكترونية من أجل الكشف عن الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، بناء على إذن مكتوب من السلطة القضائية وتحت مراقبتها طبقا لقانون الإجراءات الجزائية، تنفيذ طلبات المساعدة القضائية الأجنبية في مجال تدخل الهيئة، وجمع المعطيات المفيدة لتحديد مكان تواجد مرتكبي الجرائم الإلكترونية

¹ - المادة 11 من المرسوم الرئاسي 21-439.

² - المادة 10 من المرسوم الرئاسي 21-439.

والتعرف عليهم، مع جمع وإستغلال كل المعلومات التي تسمح بالكشف عن الجرائم الإلكترونية وحفظها، كما تكلف بتزويد السلطات القضائية تلقائيا، أو بناء على طلبها بالمعلومات والمعطيات المتعلقة بالجرائم الإلكترونية، وكذا القيام بالتدقيق والتفتيش في أي مكان أو هيكل أو جهاز يحوز أو يستعمل وسائل وتجهيزات موجهة لمراقبة الإتصالات الإلكترونية، واستثنت من تلك التابعة لوزارة الدفاع الوطني، وتعمل على تنشيط عمل الملحقات الجهوية تحت إشراف المدير العام، إلى جانب ذلك عليها أن تتحلى باليقظة الإلكترونية في مجال الجرائم الإلكترونية.¹

يتبين من المهام الموكلة إلى مديرية المراقبة الوقائية واليقظة الإلكترونية بإعتبارها المركز العملياتي للهيئة، فمهمتها الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال، مستعملة في ذلك كل الوسائل والأجهزة التقنية الضرورية من أجل تنفيذ مهامها وبمساعدة المختصين كمقدمي الخدمات،² كما تمارس مديرية المراقبة الوقائية واليقظة الإلكترونية مهامها المرتبطة بالشرطة القضائية وفقا لقانون الإجراءات الجزائية³، مما يعطيها صفة الضبطية القضائية.

ب - مديرية الإدارة والوسائل

يعين مدير الإدارة والوسائل بموجب مرسوم رئاسي، بناء على إقتراح من المدير العام للهيئة، وتتهى مهامه بحسب الأشكال نفسها، وتعتبر وظيفته وظيفة عليا في الدولة، و هذا ما تضمنته المادة 12 فقرة 1، تكلف مديرية الإدارة والوسائل بتسيير الموارد البشرية والوسائل والمالية الخاصة بالهيئة، وصيانة العتاد والوسائل والمنشآت القاعدية، مع إعداد إحتياجات الهيئة في إطار تحضير تقديرات الميزانية الإسناد التمويني التقني للهيئة ويمكن أن تنظم مديرية الإدارة في مديريات فرعية.⁴

ج- مصلحة الدراسات والتلخيص ومصلحة التعاون واليقظة الإلكترونية

تتمثل مهام وصلاحيات مصلحة الدراسات والتلخيص في إعداد مشروع مخطط عمل الهيئة بالتشاور مع الهياكل الأخرى للهيئة، تقوم بتلخيص الوثائق المتعلقة بنشاطات الهيئة، ودراسة وبحث تتعلق

¹ - المادة 15 من المرسوم الرئاسي 20-183.

² - المادة 17 من المرسوم 20 - 183.

³ - المادة 16 من المرسوم 20 - 183.

⁴ - المادة 16 من المرسوم الرئاسي رقم 21-439.

بنشاطات الهيئة، وتعمل على مراقبة الإجراءات المتعلقة بالطلبات القضائية وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية، بالإضافة إلى حفظ الوثائق والأرشيف.¹

أما في ما يخص مصلحة التعاون واليقظة التكنولوجية فمهمتها الأساسية هي التعاون مع الشركاء لتنفيذ عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها²، فمهمتها إذا مساعدة وتسهيل عمل مديرية الوقاية واليقظة الإلكترونية.

د - الملحقات الجهوية

أنشئت هذه الملحقات الجهوية بصدور المرسوم الرئاسي 21-439 المؤرخ في 2021/11/7، يرأس كل ملحقة جهوية رئيس ملحقة، يعين بموجب مرسوم رئاسي وباقتراح من المدير العام للهيئة، وتنتهي المهام بنفس الأشكال³، ويتم وضع الملحقات قيد الخدمة والتشغيل من طرف مديرية المراقبة الوقائية واليقظة⁴، و تكلف الملحقة الجهوية بتنفيذ عمليات المراقبة الوقائية للاتصالات الإلكترونية، من أجل الكشف عن الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، بناء على إذن مكتوب من السلطة القضائية وتحت مراقبتها طبقا لقانون الإجراءات الجزائية.

ثانيا: مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها

تناولت المادة 14⁵ من القانون 09 - 04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة

¹ - المادة 17 من المرسوم الرئاسي رقم 21-439.

² - المادة 18 من المرسوم الرئاسي رقم 21-439.

³ - المادة 12 من المرسوم الرئاسي رقم 21-439.

⁴ - المادة 19 من المرسوم الرئاسي رقم 21-439.

⁵ - تنص المادة 14 من القانون 09 - 04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام

والإتصال ومكافحتها على أنه " تتولى الهيئة المذكورة في المادة 13 خصوصا المهام التالية :

- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته.

- مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية.

- تبادل المعلومات مع نظيرتها في الخارج قصد جمع المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وتحديد مكان تواجدهم.

بتكنولوجيا الإعلام والاتصال المؤرخ في 5 / 08 / 2009 مهام الهيئة، كما نصت المادة 04 من المرسوم الرئاسي 21-439 على المهام المنوطة بالهيئة، والتي تكون تحت رقابة السلطة القضائية طبقا لأحكام قانون الإجراءات الجزائية والقانون 09-04، وتتمثل هذه المهام في تحديد الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام ومكافحتها، وتنسيق وتنظيم عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، مساعدة السلطات القضائية المختصة ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال لاسيما من خلال جمع المعلومات والتزود بها من خلال الخبرات القضائية، ضمان المراقبة الوقائية للاتصالات الإلكترونية، تحت رقابة سلطة القاضي، قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والتي تمس بأمن الدولة، كما تضمن الهيئة بالتنسيق مع المصالح المختصة لوزارة الدفاع، المراقبة الإلكترونية عندما يتعلق الأمر بأمن الجيش، تجميع وتسجيل وحفظ المعطيات الرقمية للأنظمة المعلوماتية وتحديد مصادرها ومسارها من أجل استعمالها في الإجراءات القضائية، كما تسهر على تنفيذ طلبات المساعدة الصادرة من البلدان الأجنبية، وتطبيق تبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها، تعمل على تطوير التعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم الإلكترونية، والمساهمة في تكوين المحققين المتخصصين في مجال التحريات التقنية المتصلة بالجرائم الإلكترونية، وكذلك المساهمة في تعيين المعايير القانونية في مجال اختصاصها.

ومن خلال إستعراض لتشكيلة الهيئة والمهام المنوطة بها وإختصاصات كل جهاز، يتجلى لنا الدور الفعال للهيئة خاصة في مجال الوقاية من الجرائم الإلكترونية، فيما يتعلق بإجراءي المراقبة الإلكترونية والتفتيش نظم المعلوماتية، ولكن نحث المشرع الجزائري أن يستقر على تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال حتى تؤدي دورها على أكمل وجه وخاصة، أن إنتشار هذه الجرائم إزدادت وثيرتها في المجتمع الجزائري.

الفرع الثاني: السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي

تعد المعطيات ذات الطابع الشخصي جزء لا يتجزأ من الحق في الحياة الخاصة، التي كفل المشرع الجزائري حمايتها بإعتبارها حقا دستوريا أساسيا وهذا ما أكدته المادة 46 من دستور 2016 في الفقرة الرابعة حيث نصت "حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي حق

أساسي يضمنه القانون ويعاقب على إنتهاكه¹، وحماية لهذه المعطيات سن المشرع الجزائري القانون رقم 07/18 المؤرخ في 10 جوان 2018 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الذي يعد الإطار التشريعي المنظم للمسائل المتعلقة بحماية المعطيات الشخصية في الجزائر²، فأنشأ القانون رقم 07-18 آلية مؤسسية من أجل السهر على إحترام وحماية المعطيات ذات الطابع الشخصي، خول لها صلاحيات واسعة تسمى بالسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي³، ولتفصيل ذلك سوف نتطرق لنشأة وتشكيلية السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي (أولا) ثم لمهامها (ثانيا).

أولا: نشأة وتشكيلية السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي

سار المشرع الجزائري على نهج الدول التيا إلى إنشاء هيئات مستقلة مكلفة بالإشراف والرقابة لحماية المعطيات ذات الطابع الشخصي، كالتشريع الفرنسي الذي أنشأ اللجنة الوطنية للمعلومات والحريات (CNIL) بموجب القانون المتعلق بالمعلوماتية والحريات المؤرخ في 16/01/1978، والمشرع المغربي أحدث اللجنة الوطنية لمراقبة حماية المعطيات الشخصية بموجب القانون رقم 09-08 المؤرخ في 18/06/2009، المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، أما بالنسبة للمشرع الجزائري وذلك بموجب المادة 22 فقرة 01 من القانون 07-18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ثم إنشاء سلطة إدارية مستقلة لحماية المعطيات ذات الطابع الشخصي لدى رئيس الجمهورية وتسمى "السلطة الوطنية" مقرها الجزائر العاصمة، تتمتع بالشخصية المعنوية والإستقلال المالي والإداري⁴، رغم إختلاف المصطلحات المستعملة لمختلف التشريعات سواء الفرنسي أو المغربي، إلا أنهم إتفقوا على دورها في الإشراف والرقابة على معالجة المعطيات الشخصية.

¹ - القانون رقم 16 - 01 المؤرخ في 06/03/2016 يتضمن التعديل الدستوري، الجريدة الرسمية الجمهورية الجزائرية عدد 14 الصادرة بتاريخ 2016/03/07.

² - عائشة بن قارة مصطفى، آليات حماية المعطيات ذات الطابع الشخصي في التشريع الجزائري وفقا لأحكام القانون 07.18، المرجع السابق، ص 747.

³ - الفقرة 18 من المادة الثالثة من القانون 07-18 والتي تنص على " السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي النصوص عليها في هذا القانون. "

⁴ - المادة 22 من القانون رقم 07 - 18.

تتشكل السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي حسب المادة 23 من القانون 18-07 من ثلاث (3) شخصيات من بينهم الرئيس، يختارهم رئيس الجمهورية من بين ذوي الاختصاص في مجال عمل السلطة الوطنية، ثلاثة (3) قضاة يتم إقتراحهم من قبل المجلس الأعلى للقضاء من بين قضاة المحكمة العليا ومجلس الدولة، وعضو من كل غرفة من غرفتي البرلمان يتم إختيار كل منهما من قبل رئيس كل غرفة بعد التشاور مع رؤساء المجموعات البرلمانية، وكذا ممثل (01) عن المجلس الوطني لحقوق الإنسان وممثل (01) عن وزير الدفاع الوطني، وممثل (01) عن وزير الشؤون الخارجية، وممثل عن الوزير المكلف بالداخلية، وممثل (01) عن وزير العدل حافظ الأختام، وممثل (01) عن الوزير المكلف بالبريد والمواصلات السلكية واللاسلكية والتكنولوجية والرقمنة، وعضوين آخرين عن الوزير المكلف بالصحة، ووزير العمل والتشغيل والضمان الاجتماعي.

وما يلاحظ من خلال هذه التشكيلة تكاملها، وتأكيد المشرع على شرط الاختصاص القانوني والتقني في مجال المعطيات الشخصية، وهذا ما يؤكد إهتمام المشرع بهذا الجهاز، ودوره الفعال في حماية معالجة المعطيات ذات الطابع الشخصي.¹

كما يمكن للسلطة أن تستعين بأي شخص مؤهل من شأنه مساعدتها في أشغالها، يعين رئيس وأعضاء السلطة الوطنية، بموجب مرسوم رئاسي، لعهد مدتها خمس (5) سنوات قابلة للتجديد، وهو ما يعزز إستقلالية السلطة من الناحية العضوية، وتمكين الأعضاء من ممارسة وظيفتهم ضمن الأحكام المقررة، على الرغم من أن المشرع الجزائري لم يقيد قابلية التجديد مما يترتب عليه إمكانية تجديد عضوية الأعضاء لعدة عهديات²، وهذا ما أكدته الأستاذ jean louis autin الذي أعتبر أن الوقت أو المدة أمر ضروري بالنسبة لإستقلالية العضوية التي ترتبط بأداء السلطة لمهمتها المكلفة بها³، كما يثار إشكال بالنسبة لمسألة إختيار عضوين من البرلمان اللذين يتم إختيارهما من قبل رئيسا غرفتي البرلمان، فالإشكال يكمن في كيفية حساب عهدة الخمس سنوات، خاصة إذا تم تعيينهما في منتصف العهدة فهل يكملان

¹ - عبد الهادي الكحلوي، عبد الهادي بن زريطة، آليات حماية المعطيات ذات الطابع الشخصي، في ظل القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، مجلة القانون والعلوم السياسية، المجلد 07، عدد 02، 2021، ص 120.

² - حكيم تبينة، آليات الضبط الإداري لحماية المعطيات ذات الطابع الشخصي في التشريع الجزائري، المجلة الجزائرية للعلوم القانونية والسياسية، المجلد 58، العدد 01، 2021، ص 229.

³ - حكيم تبينة، المرجع نفسه، ص 229.

العهد في حالة حل البرلمان، أو في حالة انتهاء عهديهما؟ أم يتم إستبدالهما خاصة وأن رئيس السلطة الوطنية وأعضائها ملزمون بالحفاظ على الطابع السري للمعطيات ذات الطابع الشخصي والمعلومات، التي إطلعوا عليها بهذه الصفة ولو بعد إنتهاء مهامهم، وفي المقابل يحظون بحماية الدولة ضد أي تهديدات أو إهانات أو إعتداءات من أي طبيعة كانت بمناسبة أو أثناء تأدية مهامهم¹ ما لم يوجد نص قانوني يقضي بخلاف ذلك.²

ثانيا: مهام السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي

قبل التنصيب في الوظيفة يؤدي أعضاء السلطة الوطنية اليمين، أمام مجلس قضاء الجزائر العاصمة،³ وتعمل السلطة الوطنية على مراعاة مدى مطابقة معالجة المعطيات ذات الطابع الشخصي لأحكام القانون، وضمان عدم وجود أي أخطار قد تمس بحقوق الأشخاص والحريات العامة، وحرمة الحياة الخاصة، عند إستعمال تكنولوجيا الإعلام والاتصال، وقد حددت المادة 25 من القانون 18 - 07 المهام الموكلة إليهم والتي تتمثل فيما يلي:

- 1 - منح التراخيص⁴ وتلقي التصريحات المتعلقة⁵ بمعالجة المعطيات ذات الطابع الشخصي.
- 2 - إعلام الأشخاص المعنيين والمسؤولين عن المعالجة بحقوقهم وواجباتهم.
- 3 - تقديم الإستشارات للأشخاص والكيانات، التي تلجأ لمعالجة المعطيات ذات الطابع الشخصي، أو التي تقوم بتجارب أو خبرات من طبيعتها أن تؤدي إل مثل هذه المعالجة.⁶
- 4 - تلقي الإحتجاجات والطعون والشكاوى، بخصوص تنفيذ معالجة المعطيات ذات الطابع الشخصي وإعلام أصحابها بمالها.

¹ - خضرة شنتير، المرجع السابق، ص 173 .

² - المادة 26 من قانون 18 - 07 المتعلق بحماية المعطيات ذات الطابع الشخصي.

³ - يؤدي أعضاء السلطة الوطنية اليمين أمام مجلس قضاء الجزائر بالصيغة التالية " أقسم بالله العظيم أن أؤدي مهمتي كعضو في السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي بكل إستقلالية وحياء وشرف ونزاهة وأن أحافظ على سرية المداولات"

⁴ - المادة 17 من القانون 18 - 07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

⁵ - المادة 13 من القانون 18 - 07 المتعلق بحماية الأشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي.

⁶ - المادة 25 فقرة 02 و 03 من نفس القانون.

5 - الترخيص بنقل المعطيات ذات الطابع الشخصي نحو الخارج وفقا للشروط المنصوص عليها في هذا القانون.¹

7 - الأمر بإغلاق معطيات أو سحبها أو إتلافها.

8- تقديم أي اقتراح من شأنه تبسيط وتحسين الإطار التشريعي والتنظيمي لمعالجة المعطيات ذات الطابع الشخصي.

9 - نشر التراخيص الممنوحة والآراء المدلى بها في السجل الوطني المشار إليه في المادة 28 من هذا القانون.

10- تطوير علاقات التعاون مع السلطات الأجنبية الممثلة مع مراعاة المعاملة بالمثل .

11 -إصدار عقوبات إدارية وفقا لأحكام المادة 46 من هذا القانون.

12- وضع معايير في مجال حماية المعطيات ذات الطابع الشخصي.

13 - وضع قواعد السلوك والأخلاقيات التي تخضع لها معالجة المعطيات ذات الطابع الشخصي، كما تعد السلطة تقريرا سنويا حول نشاطها ترفعه إلى رئيس الجمهورية.

وللسير الحسن للمهام المنوطة بالسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، تزود بأمانة تنفيذية يسيرها أمين تنفيذي، يساعده في مهامه مستخدمون، وهم ملزمون بالحفاظ على سرية المعلومات التي يطلعون عليها أثناء، أو بمناسبة ممارسة مهامهم،² كما سيتم إنشاء سجل وطني لحماية المعطيات ذات الطابع الشخصي يمسك من طرف السلطة الوطنية وتفيد في:

¹ - تنص المادة 44 من ق 18 - 07 على " لا يجوز لمسؤول عن معالجة نقل المعطيات ذات طابعا شخصي إلى دولة أجنبية إلا بترخيص للسلطة الوطنية وفقا لأحكام هذا القانون، وإذا كانت هذه الدولة تضمن مستوى حماية كاف للحياة الخاصة والحريات والحقوق الأساسية للأشخاص إزاء المعالجة التي تخضع لها.

تقدر السلطة الوطنية المستوى الكافي من الحماية الذي تضمنه دولة معينة، لاسيما وفقا للمقتضيات القانونية المعمول بها في هذه الدولة ولإجراءات الأمن المطبقة فيها، وللخصائص المتعلقة بالمعالجة مثل غاياتها ومدتها وكذا طبيعة وأصل ووجهة المعطيات المعالجة.

وفي جميع الأحوال يمنع إرسال وتحويل معطيات ذات الطابع الشخصي إلى دولة أجنبية عند ما قد يؤدي ذلك إلى المساس بالأمن العمومي أو المصالح الحيوية للدولة . "أما المادة 45 فنصت على استثناءات على أحكام المادة 44.

² - المادة 27 من القانون 18 - 07.

- الملفات التي تكون السلطة العمومية مسؤولة عن معالجتها.
- الملفات التي يكون الخواص مسؤولين عن معالجتها.
- مراجع القوانين أو النصوص التنظيمية المنشورة المتضمنة إحداث ملفات عمومية.
- التصريحات المقدمة للسلطة الوطنية والتراخيص التي تسلمها.
- المعطيات المتعلقة بالملفات الضرورية للسماح للأشخاص المعنيين بممارسة حقوقهم المنصوص عليها في القانون 18-07.

وتعفى من التقييد في السجل الوطني الملفات، التي يكون الغرض الوحيد من معالجتها مسك سجل موجه بموجب مقتضيات تشريعية أو تنظيمية لإطلاع العموم، غير أنه تدرج بالسجل الوطني المذكور وجوبا هوية الشخص المسؤول عن المعالجة، حتى يتمكن الأشخاص المعنيون من ممارسة الحقوق المنصوص عليها في القانون 18-07.¹

الفرع الثالث الأجهزة المتخصصة التابعة للأمن والدرك الوطني

نظرا للانتشار السريع للجرائم الإلكترونية في كافة دول العالم، والجزائر ليست بمنأى عن هذه الظاهرة المستحدثة، فسارعت الدول إلى إنشاء مؤسسات وأجهزة متخصصة لمكافحة وتتبع مرتكبي هذه الجرائم، وقد قامت الجزائر بإتباع نفس الطريق، من خلال إستحداث أجهزة سواء كانت تابعة للدرك الوطني أو الأمن الوطني.

الفقرة الأولى: الوحدات التابعة للدرك الوطني

من أجل محاربة الجريمة بكافة أنواعها والجريمة الإلكترونية بصفة خاصة، تم إستحداث عدة هياكل للتصدي للإجرام المعلوماتي، من بينها الدرك الوطني الذي يلعب دورا كبيرا في مجال مكافحة من خلال الأجهزة التابعة له.

أولا: المعهد الوطني للأدلة الجنائية وعلم الإجرام

يمثل هذا المعهد مؤسسة عمومية ذات طابع إداري، تحت الوصاية المباشرة لوزير الدفاع الوطني

¹ - المادة 28 من القانون 18 - 07.

تتمتع بالشخصية المعنوية والاستقلال المالي، تم إنشاؤها بموجب المرسوم الرئاسي 04 - 183 المؤرخ في 26/06/2004 المتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي¹، مقره ببو شايو بالجزائر العاصمة، فهو يخضع لجميع الأحكام التشريعية والتنظيمية العسكرية، وقد صنف من بين المعاهد الكبرى في العالم.²

حيث يعد المعهد بمثابة هيئة مختصة في إجراء الخبرات والمعاينة، وذلك بمختلف دوائره³ بما فيها " دائرة الإعلام الآلي والإلكترونية" التي أوكلت لها مهام تحليل الأدلة المتعلقة بالجرائم الإلكترونية، وذلك بتحليل الدعامات الإلكترونية وإصلاح الدعامات التالفة، إنجاز المقاربات الهاتفية، تحسين التسجيلات الصوتية والفيديو والصورة وذلك لتسهيل استغلالها.⁴

وهو مكلف بالمهام التالية:⁵

- إجراء الخبرات بناء على طلب من القضاة والمحققين أو السلطات المؤهلة، والفحوص العلمية التي تخضع لاختصاص كل طرف في إطار التحريات الأولية والتحقيقات القضائية بغرض إقامة الأدلة التي تسمح بالتعرف على مرتكبي الجنايات والجنگ .

- تقديم مساعدة علمية أثناء القيام بالتحريات المعقدة باستخدام مناهج الشرطة العلمية والتقنية الرامية إلى تجميع وتحليل الأشياء والآثار والوثائق المأخوذة من مسرح الجريمة.

- المشاركة في الدراسات والتحليل المتعلقة بالوقاية والتقليل من كل أشكال الجريمة.

¹ - المرسوم الرئاسي رقم 04 - 183 المؤرخ في 26 يونيو 2004 المتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، الجريدة الرسمية للجمهورية الجزائرية، عدد 41، الصادرة بتاريخ 27 يونيو 2004.

² - مليكة بهلول، دور الشرطة العلمية والتقنية في الكشف عن الجريمة، أطروحة نيل شهادة دكتوراه، علوم، كلية الحقوق، جامعة الجزائر 01، الجزائر 2013، ص 144.

³ - يتكون المعهد الوطني للأدلة الجنائية وعلم الاجرام من إحدى عشر دائرة مختصة في مجالات مختلفة، جميعها تضمن الخبرة والتكوين والتعليم، تقديم المساعدات التقنية البحوث، الدراسات والتحليل في علم الجريمة، أنظر المعهد الوطني للأدلة الجنائية وعلم الإجرام مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية، وزارة الدفاع الوطني قيادة الدرك الوطني

⁴ - حسين ربيعي، المرجع السابق، ص 184

⁵ - المادة 04 من المرسوم الرئاسي رقم 04 - 183.

- تصميم بنوك معطيات وإنجازها طبقا للقانون بما في ذلك تلك الخاصة بالبصمات الجينية التي تكون في متناول المحققين والقضاة بغرض وضع المقاربات واستخلاص الروابط المحتملة بين المجرمين.
- المشاركة بصفته هيئة تضمن الفحوص والخبرات في مجال علم الإجرام في تحديد سياسة جنائية مثلى لمكافحة الإجرام.
- المبادرة بالبحوث المتعلقة بالإجرام وإجرائها باللجوء إلى التكنولوجيا الدقيقة.
- العمل على ترقية البحث التطبيقي وأساليب التحريات التي تثبت فعاليتها في ميادين علمي الإجرام والأدلة الجنائية على الصعيدين الوطني والدولي.
- المشاركة في كل الملتقيات والمحاضرات أو الندوات على الصعيدين الوطني والدولي.
- تصور الأبحاث الموكلة إلى الغير وضمان متابعتها وتقديرهما.

ثانيا: مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية

تم إنشاء مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية سنة 2008، ويعتبر الجهاز الوحيد المختص بهذا الصدد في الجزائر، يعمل على تأمين منظومة المعلومات لخدمة الأمن العمومي، وأعتبر بمثابة مركز توثيق، ويتواجد مقره ببئر مراد رابح¹، ويعتبر هذا المركز بمثابة نقطة وصل وطنية في مجال دعم أعمال البحث والتحقيق في الجرائم المعلوماتية، إذ يوفر المساعدة التقنية للمحققين ويساهم في توجيه التحقيقات المرتبطة بتكنولوجيا الإعلام والاتصال، فهو هيئة تقنية تعمل تحت وصاية مديرية الأمن العمومي والإستعمال تحت قيادة الدرك الوطني²، ويتولى مركز المراقبة من جرائم الإعلام الآلي والجرائم المعلوماتية ضمان المراقبة الدائمة والمستمرة على شبكة الأنترنت.

- القيام بمراقبة الإتصالات الإلكترونية، بما يسمح به القانون لفائدة وحدات الدرك الوطني والجهات القضائية.

¹ - سمير بارة، الدفاع الوطني والسياسات الوطنية للأمن السيبراني في الجزائر بالدور والتحديات، المجلة الجزائرية للأمن الإنساني، عدد 2، 2017/، ص 335.

² - حسين ربيعي، المرجع السابق، 185.

- مساعدة الوحدات الإقليمية للدرك الوطني في معاينة الجرائم المرتكبة بتكنولوجيا الإعلام، والبحث عن الأدلة في شبكة الأنترنت.

- المشاركة في عمليات التحري والتسرب عبر شبكة الأنترنت، لفائدة وحدات الدرك الوطني والسلطات القضائية.

إستطاع المركز معالجة أزيد من 100 جريمة إلكترونية سنة 2014، وما يفوق 500 قضية رقمية خلال سنة 2015، منها 300 جريمة تتعلق بمواقع التواصل الاجتماعي "فيسبوك" و 20 جريمة رقمية تتعلق باختراق مواقع رسمية لمؤسسات خاصة وعامة، استهدف مجرموها أنظمة المعالجة الآلية للمعطيات¹، في سنة 2019 ثم معالجة 1188 قضية بنجاح من مجموع 1515 قضية مسجلة مع توقيف 1512 متورط²، كما يقوم مكتب اليقظة والتحسيس التابع لهذا المركز بمهام اليقظة المعلوماتية التي تعد من أهم الطرق المعتمدة للوقاية من الجرائم الإلكترونية والإنذار المسبق الذي سمح بإتخاذ القرارات الكفيلة بمعالجتها ويعتمد في ذلك على عدة أنواع من اليقظة هي:³

-اليقظة الأمنية: والتي يمكن من خلالها متابعة مدى تطور الإجرام وأساليبه المختلفة والخطط العلمية التي ينتهجها المجرمون، الغرض من هذا العمل تحضير وتجديد أفضل الأفراد، والوسائل للتصدي لهذا النوع من الإجرام.

-اليقظة التكنولوجية والعلمية: وتتمثل في جمع مختلف المعطيات والمعلومات التي تسمح بمتابعة الابتكارات والتطورات الحاصلة في المجال التكنولوجي والعلمي.

-اليقظة الاجتماعية: تهتم بمتابعة مختلف التحاليل والدراسات التي تهتم بالمجتمع وتطورات.

-اليقظة القانونية: وتعنى بالتطورات الحاصلة في المجال القانوني والنصوص التشريعية، بمختلف المهام والنشاطات المتعلقة بالدرك الوطني لا سيما الحفاظ على الأمن العام.

-اليقظة الاقتصادية: تهتم بالجوانب الاقتصادية بهدف حماية المصالح الوطنية عند توقيع العقود ومعاهدات الشراكة الاقتصادية

¹ - سميرة بارة، المرجع السابق، ص435.

² - خضرة شنتير، المرجع السابق، ص201.

³ - عبد القادر عميمر، المرجع السابق، ص، ص 316-317.

الفقرة الثانية: الهيئات المتخصصة التابعة للأمن الوطني

جهاز الشرطة من الأجهزة الأمنية الفعالة والناشطة في مجال الوقاية من الجرائم بصفة عامة، والجرائم الإلكترونية بصفة خاصة، ويتمثل دور جهاز الشرطة من خلال قيام المديرية العامة للأمن الوطني إلى تحديث بنيتها الهيكلية، من أجل خلق أجهزة متخصصة في مكافحة الجرائم الإلكترونية تتمثل في:

أولا: المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني

إستجابة لمطلب الأمن المعلوماتي، ومحاربة التهديدات الأمنية الناتجة عن الجرائم الإلكترونية، أنشأت مصالح الأمن المصلحة المركزية للجريمة المعلوماتية، التي كانت عبارة عن فصيلة شكلت النواة الأولى لتشكيل أمني خاص لمواجهة الجريمة الإلكترونية، والتي أنشأت سنة 2011، ليتم بعدها إنشاء المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، بقرار المدير العام للأمن الوطني حيث أضيف للهيكل التنظيمي لمديرية الشرطة الفضائية في جانفي 2015.¹

ثانيا: المخابر الجهوية للشرطة العلمية

تضم المخابر الجهوية للشرطة العلمية دائرة خاصة، مهمتها البحث والتحقيق في التحقيق في الجريمة الإلكترونية تسمى " دائرة الأدلة الرقمية والآثار التكنولوجية "، تم إستحداثها في البداية كقسم تابع للمخبر الجهوي للشرطة العلمية، قبل ترقيتها في سنة 2004²، بسبب الإرتفاع الكبير لعدد القضايا الناتجة عن الجرائم الإلكترونية، وتضم هذه الدائرة ثلاثة أقسام: هي قسم إستغلال الأدلة الرقمية الناتجة عن الحواسيب والشبكات، قسم إستغلال الأدلة الناتجة عن الهواتف النقالة، وقسم تحليل الأصوات وتضم هذه الدائرة ثمانية أعضاء محققين، أربع منهم أعوان شرطة رسميين يتمتعون بصفة ضابط شرطة قضائية، والبقية أعوان شبيهيون يحوز كل منهم شهادة جامعية في تخصص الإعلام الآلي³، وفي سنة 2007 تم إستحداث أقسام متخصصة في تتبع الأدلة الرقمية بمخابر الشرطة العلمية، الكائن مقرها بالجزائر العاصمة، وهران وقسنطينة، وتقوم بإستغلال الأجهزة الإلكترونية، قصد إستغلال وتتبع كل ما من شأنه أن يساعد على

¹ - سمير بارة المرجع السابق، ص 437.

² - عبد القادر عمير، المرجع السابق ص 313.

³ - حسين ربيعي، المرجع السابق، ص 178.

اكتشاف الجريمة الإلكترونية، وضبط الأدلة.¹

ثالثا: الخلايا الولائية المختصة في مكافحة الجريمة الإلكترونية

تبلور دور الشرطة القضائية في مكافحة الجريمة الإلكترونية، في إستحداث ما يقارب 23 خلية لمكافحة الجريمة الإلكترونية سنة 2010 موزعة على ثمان خلايا على مستوى ولايات الشرق، ثمان خلايا على مستوى ولايات الغرب، ثمان خلايا على مستوى ولايات الوسط، خلية واحدة على مستوى ولايات الجنوب، لتقوم بعدها المديرية العامة للأمن الوطني، بتعميم هذه الخلايا على مستوى كل مصالح أمن ولايات الوطن.²

المبحث الثاني: التعاون الدولي لمكافحة الجريمة الإلكترونية

يعد التعاون الدولي اللبنة الأولى والركيزة الأساسية لمواجهة الجرائم الإلكترونية، نظرا لكونها تتم في أماكن مختلفة في العالم بإستخدام الإتصالات الحديثة، وباعتبار الجرائم الإلكترونية صورة من صور الجرائم العابرة للحدود، فإنه لا يمكن للدولة مهما بلغت من التطور مكافحتها، إلا بمساعدة بقية الدول الأخرى وتضافرها، لهذا يقتضي تحسين التعاون الدولي من خلال بناء سياسة جنائية مشتركة من أجل مكافحتها في جميع أنحاء العالم، ولا يكون ذلك إلا من خلال التعاون القضائي (المطلب الأول) والتعاون الشرطي (المطلب الثاني) والإهتمام بإجراءات تسليم المجرمين (المطلب الثالث).

المطلب الأول: المساعدة القضائية المتبادلة كآلية للتعاون الدولي

وتعد المساعدة القضائية المتبادلة في المسائل الجنائية، من الآليات الفعالة لمواجهة الإجرام بوجه عام والجرائم العابرة للحدود ومنها الجرائم الإلكترونية بوجه خاص، لما للتعاون في مجال الإجراءات الجنائية من دور في التوفيق بين حق الدولة في ممارسة إختصاصها داخل حدود إقليمها، وحققها في توقيع العقاب³، وقد أعطت الإتفاقيات الدولية¹ أهمية بموضوع المساعدة القانونية المتبادلة، ومنها الإتفاقية

¹ - عبد القادر عميمير، المرجع السابق، ص314.

² - حملاوي عبد الرحمان، دور المديرية العامة للأمن من الوطني في مكافحة الجريمة الإلكترونية، ورقة علمية مقدمة في إطار الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، مخبر الحقوق والحريات في الانظمة المقارنة، كلية الحقوق، جامعة بسكرة، المنعقد بين 16-17/11/2015، ص8.

³ - أحمد إبراهيم مصطفى سليمان، الإرهاب والجريمة المنظمة، دار الطلائع للنشر والتوزيع والتصدير القاهرة، د ط، 2006، ص394.

الأوروبية (بودابست) لمكافحة الجريمة الإلكترونية، التي نصت من خلال المادة 27 على ذلك، وأكدت عليها المادة 32 من الإتفاقية العربية لمكافحة تقنية المعلومات، وألزمت الدول الأعضاء بتبادل المساعدة فيما بين الدول لغايات التحقيقات، أو الإجراءات المتعلقة بالجرائم الإلكترونية، أو لجمع الأدلة الإلكترونية.... وغيرها، وكرس المشرع الجزائري مبدأ المساعدة القانونية، وذلك من خلال القانون رقم 04/09 المؤرخ في 05/08/2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، بموجب المادة 16 منه، فمن خلال هذا المطلب نتناول بالدراسة مفهوم المساعدة القضائية والشروط الواجب توافرها (الفرع الأول) وأهم صورها أو مظاهرها في (الفرع الثاني).

الفرع الأول: مفهوم المساعدة القضائية

للمساعدة القضائية دورا فعالا في مكافحة الجريمة الإلكترونية، وقد خصها المشرع بشروط وفقا لمبدأ سيادة الدولة والمعاملة بالمثل، سوف نقوم بتعريف المساعدة القضائية الدولية ثم نتطرق إلى الشروط والقيود الواردة عليها.

الفقرة الأولى: تعريف المساعدة القضائية

تعرف المساعدة القضائية المتبادلة بأنها " كل إجراء قضائي تقوم به دولة من شأنه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم".²، كما تعرف أيضا بأنها "ما تقدمه دولة لدولة أخرى من مساعدة وعون في سبيل ملاحقة الجناة بهدف عقابهم على جرائمهم وذلك من خلال تدابير وقائية تستهدف مواجهة الصبغة عبر الوطنية، وتستجمع الأدلة بمختلف الطرق وهو ما يستغرق وقتا تتطلب إمكانات لا تملكها سلطات قانونية لدولة واحدة مالم تدعمها وتساندها جهود السلطات القانونية في الدولة الأخرى".³

¹ - إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للحدود الوطنية (باليرمو 2000) المعتمدة من قبل الجمعية العامة لمنظمة الأمم المتحدة بتاريخ 15 نوفمبر 2000 والمصادق عليها بالمرسوم الرئاسي رقم 55/02 المؤرخ في 5 فيفري 2002.

² - غانم مرض الشمري، الجرائم المعلوماتية ماهيتها، خصائصها كيفية التصدي لها قانونيا، الدار العلمية للنشر، عمان، ط1، 2016، ص98.

³ - حسين بن سعيد بن سيف الغافري، الجهود الدولية في مواجهة جرائم الأنترنت، ص12، منشور على الموقع الإلكتروني <http://www.eastlaws.com> أطلع عليه يوم 03/09/2019 على الساعة 21h15.

والمساعدة القضائية لا تتحقق إلا بواسطة خطوات ثلاث هي¹:

أولاً: الطلب

وتقدمه الدولة صاحبة الاختصاص الجنائي بالمحاكمة، ويخضع هذا الطلب لقانون الدولة الطالبة وفي نطاق الإتفاقية، التي تعقدها مع الدولة التي ستقدم المساعدة ويتم تقديم الطلب بالطرق الدبلوماسية وبحسب الأصل، ومع ذلك فإن بعض الإتفاقيات الدولية تسمح بالإتصال المباشر بين جهات العدل الدولتين كسبا للوقت.

ثانياً: فحص الطلب

وتقوم به الدولة التي ستقدم المساعدة، ويتم ذلك عن طريق التحقق من إعتبار الواقعة المطلوب تحقيقها تعد جريمة وفقا لقانون الدولة الطالبة، وفي ضوء مدى إختصاص الدولة المطلوب منها بإجابة هذا الطلب وفقا لنصوص الإتفاقية التي تعقدها مع الدولة الطالبة.

ثالثاً: تنفيذ المساعدة القضائية

تتم المساعدة القضائية بمقتضى قواعد الدولة المطلوب منها تنفيذ الإجراء، ووفقا لقانون الدولة التي تنفذه، وتعد الإتفاقيات الدولية الأداة الوحيدة، التي يمكن لها أن تضع أو تفرض إلترامات بين الدول، ومن ثم فإنه بدون الإتفاقيات الدولية، وخارج الشروط التي تنص عليها لا يمكن أن تعتمد على مساعدة الدولة المطلوب منها.

الفقرة الثانية: شروط قبول المساعدة القضائية

قام المشرع الجزائري بموجب قانون 04/09 بتفعيل تبادل المساعدة القضائية الدولية فيما يخص الجرائم الإلكترونية، سواء تعلق الأمر بإجراء التحقيقات القضائية أو الترحيات، حيث نص المشرع من خلال المادة 1/16 من القانون نفسه على أنه "في إطار الترحيات أو التحقيقات القضائية الجارية لمعانة الجرائم المشمولة بهذا القانون وكشف مرتكبيها، يمكن السلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني".

¹ - عادل عبد العال إبراهيم خراشي، إشكالية التعاون الدولي وسبل التغلب عليها، دار الجامعة الجديدة الإسكندرية، د ط، 2015، ص 203.

يمكن في حالة الإستعجال، ومع مراعاة الإتفاقيات الدولية ومبدأ المعاملة بالمثل، قبول طلبات السريعة بما في ذلك أجهزة الفاكس أو البريد الإلكتروني وذلك بقدر ما توفر هذه الوسائل من شروط أمن كافية للتأكد من صحتها."

فمن خلال المادة السالفة الذكر، أقر المشرع للسلطات القضائية المختصة تبادل المساعدة القضائية على المستوى الدولي، قصد جمع الأدلة الخاصة بالجريمة الإلكترونية، ونظرا لتمييز هذه الأخيرة بسرعة إرتكابها ومحو أدلتها وصعوبة إكتشافها، مما يتطلب السرعة في إتخاذ الإجراءات الخاصة بجمع الأدلة والتحريات، ولتسهيل ذلك أورد المشرع إستثناء في المادة 2/16 من ق 04/09 لقبول طلبات المساعدة القضائية عن طريق وسائل الإتصال السريعة¹ كأجهزة الفاكس أو البريد الإلكتروني، وهاتين الوسيطتين جاءت على سبيل المثال لا الحصر مما يسمح بإستعمال مختلف وسائل الإتصال في حالة الاستعجال، مما يفتح المجال لاحتمال توافر وسائل اتصال جديدة في المستقبل²، لكنه إشتراط التأكد من صحتها، وعليه تتم المساعدة القضائية وفق شروط تتمثل في:

- تتم وفق الإتفاقيات الدولية

- تخضع لمبدأ المعاملة بالمثل احتراما لمبدأ سيادة الدولة.

وفي هذا المجال تبنى المشرع الجزائري قبول المساعدة القضائية بالطريقة الإلكترونية وذلك بموجب المادة 36 من الأمر رقم 06/05 المؤرخ في 23/08/2005 المتعلق بمكافحة التهريب تحت عنوان التعاون العملياتي" والتي جاءت نصها "مع مراعاة مبدأ المعاملة بالمثل وفي إطار الإتفاقيات الثنائية ذات الصلة، توجه طلبات المساعدة في مجال محاربة التهريب الصادرة عن السلطات الأجنبية كتابيا، أو بالطريقة الإلكترونية، إلى الجهات المختصة وتكون مصحوبة بكل المعلومات الضرورية إذا ما وجه الطلب إلكترونيا يمكن تأكيده بواسطة أي وسيلة تترك اثرا مكتوبا³..."

ومن القضايا التي لها بعد دولي، حيث تمكنت سلطات البحث والتحري وبالتعاون مع السلطات

¹ - فالأصل أن طلب المساعدة القضائية يكون بالشكل الخطي ويتم عن طريق الدبلوماسي وهو يتسم بالبطء وكثرة شكلياته، لذلك فإن هذه الطريقة لا يمكن إعتماها في مجال التحري في الجرائم الإلكترونية.

² - مريم أحمد مسعود، المرجع السابق، ص 63.

³ - المادة 36 من الأمر رقم 06/05 المؤرخ في 23/08/2005 تتعلق بمكافحة التهريب، الجريدة الرسمية للجمهورية الجزائرية، عدد 59 الصادرة بتاريخ 2005/08/28.

الألمانية وسفارة الولايات المتحدة الأمريكية بالجزائر، ومكتب الإنترنت فرع الجزائر من إلقاء القبض على شخص، هويته القيام بالقرصنة الإلكترونية، حيث قام هذا الأخير بإختراق قاعدة بيانات متواجدة بمدينة "ميونيخ" الألمانية، وقام بتحميل البيانات الرقمية الخاصة بـ 15000 بطاقة إئتمان بإستعمال العنوان الإلكتروني، وهذا ما مكنه من تحويل مبالغ مالية قدرت قيمتها بـ 100.000 دولار منذ عام 2005 من حساب زياث البنك الكندي (caisse populaire des jardins) فأدانت محكمة عنابة قسم الجنج الجاني، وفقا للمواد من 394 مكرر 1- 394 مكرر 2 من ق.ع.ج وهي جنحة تصميم وإدخال عن طريق الغش لمعطيات جنحة التقليد طبقا للمواد من 151 و 153 من القانون رقم 05/03 المتعلق بحقوق المؤلف والحقوق المجاورة¹، إلا أن قبول طلبات المساعدة القضائية ليست ملزمة بصفة مطلقة، يمكن أن ترد عليها بعض القيود.

الفقرة الثالثة: القيود الواردة على طلبات المساعدة القضائية الدولية

أورد القانون 04/09 المؤرخ في 05 أوت 2009 بعض القيود على تنفيذ طلبات المساعدة القضائية وهذا ما تضمنه المادة 18 من نفس القانون، والذي نص على "يرفض التنفيذ لطلبات المساعدة إذا كان من شأنها المساس بالسيادة الوطنية أو النظام العام، ويمكن أن تكون الإستجابة لطلبات المساعدة القضائية مقيدة بشرط المحافظة على سرية المعلومات المبلغة أو يشترط عدم إستعمالها في غير ما هو موضح في الطلب².

وعليه يمكن رفض طلبات المساعدة القضائية في الحالات التالية:

1- إذا كان الطلب فيه مساس بالسيادة الوطنية.

2- وإذا كانت ماسة بالنظام العام.

وهذا ما أكدت عليه إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للحدود الوطنية³، من خلال المادة 21/18 "ترفض طلب المساعدة القانونية المتبادلة في حالات معينة كأن ترى الدولة

¹ - أنظر الحكم رقم 10/073575 الصادر عن محكمة عنابة قسم الجنج بتاريخ 2010/06/28 مشار إليه لدى يزيد بوحليط، المرجع السابق، ص 362.

² - المادة 18 من القانون 04/09 المتضمن الرقابة من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

³ - إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية اعتمدت من طرف الجمعية العامة للأمم المتحدة بتاريخ 2000/11/15 بالقرار رقم 25/55 وعرض على التوقيع في مدينة باليرمو (إيطاليا) بتاريخ 12-15 ديسمبر 2000.

الطرف المطلوب منها المساعدة أن تنفيذ الطلب ينطوي على مساس بسيادتها وأمنها أو مصالحها الأساسية، أو أن يتعلق الطلب بجريمة سياسية... "

ويمكن الإستجابة لطلبات المساعدة القضائية في الحالات الآتية وذلك بشروط هي:

1- المحافظة على سرية المعلومات المبلغة لتلك الدولة.

2- عدم إستعمال المعلومات في غير الحالة الموضحة في طلب المساعدة القضائية.

وهذا بسبب حساسية أمن المعطيات والبيانات، التي قد تحتويها منظومة معلوماتية سواء تعلق الأمر بأمن الدولة أو الأشخاص.¹

الفرع الثاني: صور المساعدة القضائية الدولية

تأخذ المساعدة القضائية أكثر من صورة نذكر على سبيل المثال لا الحصر لأهم صورها وهي:

أولاً: تبادل المعلومات

ويشمل تقديم المعلومات والبيانات والوثائق والمواد الاستدلالية، التي تطلبها سلطة قضائية أو أمنية أجنبية، وهي بصدد النظر في جريمة ما عن الإتهامات التي وجهت إلى رعاياها في الخارج والإجراءات والتي إتخذت ضدهم²، كما أن هناك مظهرا آخر لتبادل المعلومات، يتعلق بالسوابق القضائية للجنة من خلالها يمكن للجهات القضائية التعرف وبدقة على الماضي الجنائي للفرد المحال إليها، وهي تساعد في تقرير الأحكام الخاص بالعود، ووفقا لتنفيذ العقوبة، وعدم الأهلية إلا أن تدويل الصحيفة الجنائية مازال في مراحل الأولى، وتقوم الدول بإعدادها بالنسبة لرعايا الدول التي ترتبط معها باتفاقيات تبادل المعلومات.³

إذ يوفر تبادل المعلومات أهمية في مكافحة الجريمة، ولما تقدمه المعلومات الصحيحة من مساعدة

¹ - يزيد بوحليط، المرجع السابق، ص363.

² - أحمد عبد اللاه المراغي، المرجع السابق، ص129.

³ -وردة شرف الدين، مجالات المساعدة القضائية الدولية المتبادلة فيما يخص جمع جميع الأدلة الرقمية وفقا للاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010، مجلة العلوم السياسية والقانون، المجلد3، العدد1، ماي 2019، ص 147.

لأجهزة تنفيذ القوانين، ومتابعة الأنشطة الإجرامية المختلفة ومصادر تمويلها.¹

لذلك فقد أوصى مؤتمر الأمم المتحدة السادس لمنع الجريمة ومعاملة المجرمين، بتطوير التبادل المنهجي للمعلومات بوصفه عنصر أساسيا من عناصر خطة العمل الدولية، لمنع الجريمة ومكافحتها، كما أوصى في مجال التعاون في المسائل المتعلقة بالجريمة الإلكترونية، بتوظيف نظم تبادل المعلومات بين الدول الأعضاء وتقديم المساعدة التقنية الثنائية المتعددة بين الأطراف إلى الدول الأعضاء.²

كما أكدت إتفاقية بودابست في مادتها 46/ب على ضرورة مشاوره الأطراف فيما بينهم حول تبادل المعلومات بشأن التطورات القانونية، السياسة أو التكنولوجيا ذات الصلة بالجريمة الإلكترونية وجمع الأدلة في الشكل الإلكتروني.³

وهذا ما اتجه إليه المشرع الجزائري وتضمنته المادة 17 من القانون 04/09 والتي نصت على أن الاستجابة لطلبات المساعدة الدولية الرامية لتبادل المعلومات أو اتخاذ إجراءات تحفظية وذلك وفقا للاتفاقيات الثنائية ومبدأ المعاملة بالمثل.

كذلك وبمقتضى المادتين 13 و 14 من القانون 04/09 تم إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، ومن مهامها تبادل المعلومات مع نظيرتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وتحديد مكان تواجدهم، وتسهر مديرية المراقبة الوقائية واليقظة الإلكترونية على تنفيذ طلبات المساعدة القضائية الأجنبية.⁴

¹ - الباشا فايزة يونس، الجريمة المنظمة في ظل الإتفاقيات الدولية والقوانين العربية، دار النهضة العربية، القاهرة، دط، 2002، ص، ص440- 441.

² - مؤتمر الأمم المتحدة السادس، لمنع الجريمة ومعاملة المجرمين. المنعقد في كاركاس سنة 1980.

³ - Art46 concertation des parties 1- les parties se concertent périodiquement au besoin afin de faciliter....

b- l'échange d'information sur les nouveautés juridiques politique ou techniques importants observes dans le domaine de la criminalité informatique et la collecte de preuves sous forme électronique. convention européenne de la criminalité .

⁴ - المادة 14 فقرة 2 من المرسوم الرئاسي 21-439، المرجع السابق، ص7.

ثانيا: نقل الإجراءات

يقصد بنقل الإجراءات، قيام دولة بناء على إتفاقية بإتخاذ إجراءات جنائية بصدد جريمة أرتكبت في إقليم دولة أخرى لمصلحة هذه الدولة، وذلك ضمن شروط معينة هي:

- أن يكون الفعل المنسوب إلى الشخص يشكل جريمة في الدولة الطالبة والدولة المطلوب عليها.
- أن تكون الإجراءات المطلوب إتخاذها، مقررة في قانون الدولة المطلوب إليها عن ذات الجريمة.
- أن تكون الإجراء المطلوب إتخاذها، يؤدي الوصول إلى الحقيقة كأن تكون أدلة الجريمة بالدولة المطلوب إليها.¹

فالعديد من الإتفاقيات الدولية والإقليمية، أقرت هذه الصورة كأحدى صور المساعدة القضائية الدولية كمعاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية²، وإتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية لسنة 2000 في المادة 21 منها، ذات الشيء نجده في معاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي لسنة 1999 في المادة 9 منها، أيضا المادة 16 من النموذج الإسترشادي لاتفاقية التعاون القانوني والقضائي الصادر عن مجلس التعاون الخليجي 2003³، كما أقر المجلس الأوروبي إتفاقية لنقل الإجراءات الجنائية، التي تعطي للأطراف المنظمة إمكانية محاكمة الجاني طبقا لقوانينها بناء على طلب دولة أخرى طرف في الإتفاقية بشرط أن يكون الفعل معاقبا عليه في الدولتين⁴، وهذا ما إتجه إليه المشرع في سياسته لمكافحة الجريمة بصفة عامة والإجرام المعلوماتي بصفة خاصة، حيث صادق على مجموعة من الإتفاقيات الدولية ومنها إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، كما قام بإبرام إتفاقيات ثنائية في مجال مكافحة الجرائم المستحدثة، كأبرام إتفاقيتين ثنائيتين مع فرنسا الأولى سنة 2007 في مجال التعاون القضائي في المجال الجنائي والمتعلقة بمكافحة الجريمة المنظمة⁵، والثانية أبرمت بتاريخ 2016/10/05 وتتعلق بالتعاون

¹ - أحمد عبد اللاه المراغي، المرجع السابق، ص130.

² - اعتمدت هذه الإتفاقية بواسطة الجمعية لعامة للأمم المتحدة بالقرار رقم 118/45 الصادر بتاريخ 14 ديسمبر 1990.

³ - حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الأنترنت، المرجع السابق، ص، ص510- 511.

⁴ - أحمد عبد اللاه المراغي، المرجع السابق، ص131.

⁵ - أبرمت الجزائر وفرنسا إتفاقية حول التعاون في مكافحة الجرائم المنظمة، وذلك بموجب المرسوم الرئاسي رقم 375/07 المؤرخ في 2007/12/10.

القضائي في المجال الجنائي الخاصة بمكافحة الجريمة المنظمة ومنها الجرائم الإلكترونية بكافة أشكالها.¹

ثالثا: الإنابة القضائية

يقصد بها طلب إتخاذ إجراء قضائي من إجراءات الدعوى الجنائية، تتقدم به الدولة الطالبة إلى الدولة المطلوب إليها، لضرورة ذلك عند الفصل في مسألة معروضة لدى السلطة القضائية في الدولة الطالبة لتعذر قيامها بهذا الإجراء بنفسها²، وتعرف أيضا بأنها "عمل بمقتضاه تفرض الجهة القضائية المختصة جهة أخرى للقيام مكانها، وفي دائرة اختصاصها بأحد أو بعض إجراءات التحقيق أو الإجراءات القضائية الأخرى، والتي تعذر عليها مباشرتها بنفسها بسبب بعد المسافة أو أي مانع آخر."³

وتهدف هذه الصورة إلى تسهيل الإجراءات الجنائية بين الدول، بما يكفل إجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة والتغلب على عقبة السيادة الإقليمية، التي تمنع الدولة الأجنبية من ممارسة بعض الأعمال القضائية داخل أقاليم الدول الأخرى، كسماع الشهود أو إجراء التفتيش وغيرها من الإجراءات الأخرى.⁴

وقد نظم المشرع على الإنابة القضائية الدولية⁵ وقسمها إلى قسمين بحسب ما جاء في نص المادة 721 و722 من قانون إجراءات جزائية.

1- الإنابة القضائية المرسلة إلى الخارج

ففي حالة المتابعات الجزائية غير السياسية في بلد أجنبي تسلم الإنابات القضائية من السلطة الأجنبية بالطريق الدبلوماسي، وترسل إلى وزارة العدل بالأوضاع المنصوص عليها في المادة 703، وتنفذ الإنابات القضائية إذا كان لها محل وفقا للقانون الجزائري وكل ذلك بشرط المعاملة بالمثل. "وما ورد في نص المادة 721 من ق.إ.ج.ج.

¹ - تهدف الإتفاقية إلى تعزيز فعالية التعاون القضائي في المجال لاسيما من خلال ترقية التقنيات الحديثة للتعاون بين البلدين في هذا المجال.

² - جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، المرجع السابق، ص83.

³ - كاشة محمد عبد العال، الإنابة القضائية في نطاق العلاقات الخاصة الدولية، دار الجامعية، بيروت، 1992، ص.

⁴ - خالد ممدوح إبراهيم، الجرائم المعلوماتية، مرجع سابق، ص409.

⁵ - أكد المشرع الجزائري على تكريسه لآلية الإنابة القضائية الدولية بموجب القانون رقم 01/05 المؤرخ في 06 فبراير 2005 الذي يتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتها، حيث نصت المادة 30 منه على "يمكن أن يتضمن التعاون القضائي طلبات التحقيق، والإنابة القضائية الدولية".

2- الإنابة القضائية الواردة من الخارج¹

تنص المادة 722 ق، ا، ج، ج على " في حالة المتابعات الجزائية الواقعة في الخارج إذا رأت حكومة أجنبية من الضروري تبليغ ورقة من أوراق الإجراءات، أو حكم إلى شخص مقيم في الأراضي الجزائرية فيرسل المستند وفقا للأوضاع المنصوص عليها في المادتين 702 و 703 مصحوبا بترجمة عند الاقتضاء ويحصل التبليغ إلى الشخص بناء على طلب النيابة العامة، وذلك بواسطة المندوب المختص ويعاد الأصل المثبت للتبليغ إلى الحكومة الطالبة بنفس الطريق وكل ذلك بشرط المعاملة بالمثل".

فالإنابة القضائية الدولية أساسها الاتفاقيات الدولية أو الثنائية، وكذا القوانين الداخلية للدول ومبدأ المعاملة بالمثل، حيث يرسل طلب الإنابة عبر الطريق الدبلوماسي، والتي تتميز عادة بالبطيء في سير الإجراءات، وهذا لا يتماشى مع الجرائم المستحدثة، التي تتصف بالسرعة والتعقيد ومنها الجريمة الإلكترونية، ولأجل ذلك إبرام إتفاقيات جديدة تساهم في تقصير الوقت واختصار الإجراءات كالإتفاقية المبرمة بين أمريكا وكندا التي نصت على إمكانية تبادل المعلومات شفويا في حالة الاستعجال²، وهو ما

¹ - رغم أن الجريمة الإلكترونية تعتمد كثيرا على التعاون الدولي من أجل مكافحتها، إلا أن هذا التعاون في مثل هذه الجرائم قليل جدا خصوصا في مجال الإنابة القضائية، لعدم وجود إتفاقيات ثنائية للتعاون في هذا المجال، والدليل على ضعف التعاون الدولي هو العدد القليل لحل لأنه ومن بين القضايا التي تبين حالة تنفيذ إنابة قضائية دولية الوحيدة، فصيلة الأبحاث للدرك الوطني بالجزائر وتتلخص القضية في يوم 13 أكتوبر 2011 بين الساعة 18:30 و 19:10 تعرض الموقع الحكومي الفرنسي [www. Ardenne. Pref gourv .fr](http://www.Ardenne.Pref.gouv.fr) التابعة لمنظمة La préfecture des Ardennes على شبكة الأنترنت الولوج باستعمال تقنية S O L وترك متحرك هذا الموقع توقيع باسم مستعار NOM DZ على صحة استقبال الصفحة بعد الاطلاع على الملفات المرفقة وعددها ثمانية مع الإنابة القضائية التي تتضمن معلومات حول تتبع الشخص المشتبه به على شبكة الأنترنت صاحب التوقيع NOM- DZ مع عناوين IP التي استعملها لذلك. حيث قام رئيس مصلحة الإعلام الآلي (LA Préfecture des Ardennes) بتزويد المحققين الفرنسيين بعناوين IP ومنها عناوين الاتصالات بالموقع تمت من الجزائر خلال الثلاثة أيام السابقة لاختراق الموقع يمكن للمشتبه به أن يكون قد استعملها هاته العناوين ملك لمزود خدمة الأنترنت الجزائري(س)

لدى تعريف هذا الشخص لإنشاء هذه المدونة مع تحديد البريد الإلكتروني الذي قام من خلاله بأنشائها وهو -dz hacker dz @ Hotmail Fr مع تعريف عناوين IP لاتصاله بهذا البريد، لدى Microsoft من بين عناوين IP من الجزائر لمزود خدمة الأنترنت (س)

يعد التفحص الجيد للعناوين الخاصة بالولوج للبريد الإلكتروني nom- dz @ hotmail.com وإجراء مقارنة شاملة تمكن المحققون من التعرف على هوية الهاكر nom -dz والذي تم توقيفه وتقديمه للعدالة. أنظر في ذلك دلال مولاي ملياني المرجع السابق، ص276.

² - جميل عبد الباقي الصغير، المرجع السابق، ص86.

تفطن إليه المشرع الجزائري واستدرك الأمر من خلال القانون 04/09 السابق الذكر من خلال المواد 16 و17 من نفس القانون والتي عبرت عنه باتخاذ إجراءات تحفظية، ولا يكون ذلك إلا بالإبادة القضائية.¹

المطلب الثاني: التعاون الأمني في مجال مكافحة الجريمة الإلكترونية

لا يقتصر التعاون الدولي في مجال مكافحة الجريمة الإلكترونية على المساعدة القضائية المتبادلة، فحسب وإنما يشمل التعاون الأمني، والذي تمخض عنه إيجاد آليات دولية وإقليمية التي لعبت دورا كبيرا في مجال التعاون الدولي في مكافحة الجريمة الإلكترونية، ومن بين هذه الهيئات الدولية المنظمة الدولية للشرطة الجنائية (الإنترپول)، (الفرع الأول)، وهيئات إقليمية تتمثل في مركز الشرطة الأوروبية (اليورو بول)، الأور جست، (الفرع الثاني) والأفريبول في (الفرع الثالث).

الفرع الأول: المنظمة الدولية للشرطة الجنائية (Interpol)

تقوم منظمة الشرطة الجنائية الدولية بدور فعال، في مجال التعاون الأمني بين الدول في مجال مكافحة الإجرام بشكل عام والجريمة الإلكترونية بشكل خاص، وذلك من خلال الاختصاصات الممنوحة لها بموجب قانونها الأساسي، سوف نتطرق إلى نشأة المنظمة (أولا) ومهامها أهدافها (ثانية) وإستراتيجيتها في مكافحة الجريمة الإلكترونية (ثالثا)

أولا: نشأة المنظمة الدولية للشرطة الجنائية

تعود البداية الفعلية لفكرة التعاون الدولي في المجال الشرطي إلى سنة 1904 تاريخ إبرام الإتفاقية الدولية الخاصة بمكافحة الرقيق بتاريخ 18/05/1904 بغرض مكافحة الدعارة واستغلال الفتيات²، وبعد ذلك أخذ التعاون الشرطي الدولي يأخذ صورة المؤتمرات الدولية، ومن أبرزها المؤتمر الثاني الذي أُنْصِفد بفينا وبفضل جهود مدير شرطة فينيا الدكتور جوهانز شوبر ويرجع له الفضل في إنشاء اللجنة الدولية للشرطة الجنائية³ وإختيار فينيا عاصمة لها، وكان نشاط هذه اللجنة يقتصر فقط على الدول الأوروبية غير

¹ - مريم أحمد مسعود، المرجع السابق، ص62.

² - جاء في المادة الأولى من الإتفاقية "تتعهد كل الحكومات المتعاقدة بإنشاء أو تعيين سلطة لجمع المعلومات الخاصة بإستخدام النساء والفتيات بغرض الدعارة في الخارج، ولهذه السلطة الحق في أن تخاطب مباشرة الإدارة والمماثلة لها في كل الأطراف المتعاقدة، فإستجابت سبع دول لهذه الإتفاقية وقامت بإنشاء أجهزة تتبادل من خلالها المعلومات والبيانات حول هذه الجريمة، أنظر عكروم عادل، المنظمة الدولية للشرطة الجنائية، والجريمة المنظمة كآلية لمكافحة الجريمة المنظمة، دار الجديدة، الإسكندرية، د ط، 2013، ص13.

³ - وهو الاسم الذي كان يطلق على المنظمة قبل عام 1956.

أن نشاطها تأثر بالأحداث السياسية، ما أدى إلى إختفاء نشاطها بسبب إندلاع الحرب العالمية الثانية، وبعد الحرب العالمية الثانية¹ عقد مؤتمر دولي بدعوة من المفتش العام للشرطة البلجيكية لوقاج (louvage) من تاريخ 03 إلى 07 جوان من عام 1946، حيث أعيد بعث اللجنة الدولية للشرطة الجنائية وتم نقلها إلى باريس، وفي هذا المؤتمر إستخدم لأول مرة مصطلح المنظمة الدولية للشرطة الجنائية، وفي سنة 1949 إعترفت الأمم المتحدة باللجنة الدولية للشرطة الجنائية بوضع إستشاري خاص بالمنظمات غير الحكومية.²

إلا أن نقطة التحول الدقيقة في تاريخ هذه المنظمة، يعود لسنة 1956 أين أعيد هيكلة المنظمة الدولية للشرطة الجنائية من الناحية التنظيمية، وكذلك وضع ميثاق لها والذي يحتوي على 50 مادة موزعة على أربعة أبواب، وإبتداء من تاريخ 1956/06/13 أصبحت المنظمة تعمل بشكل دائم ومستقر ويبلغ حاليا عدد الدول المنظمة اليها 195 دولة³، ويعمل الإنترنت على مدار الساعة بأربعة لغات الأكثر إستعمالا وهي العربية، الفرنسية، الإنجليزية، والإسبانية.⁴

وقد أنضمت الجزائر إلى المنظمة الدولية للشرطة الجنائية سنة 1963، أي بعد الإستقلال مباشرة ويمثلها الآن المكتب المركزي الذي يقع مقره بالجزائر العاصمة (شاطوناف)، وقد تولت الجزائر منصب رئاسة المنظمة من سنة 1974 إلى غاية سنة 1983⁵.

ثانيا: أهداف ومهام المنظمة الدولية للشرطة الجنائية

تتمثل مهمة المنظمة الدولية للشرطة الجنائية في تمكين أجهزة الشرطة حول العالم، من أجل العمل

¹ - محمد بوعبسة، المنظمة الدولية للشرطة الجنائية ودورها في مكافحة الجرائم، مجلة القانون، العدد 09، ديسمبر 2017، 04.

² - محمد رحموني، منظمة الشرطة الجنائية الدولية (الأنتربول) آلية لمكافحة الجريمة المنظمة، مجلة آفاق علمية، المجلد، 11، لعدد 04، 2019، ص 63.

³ - أنظر الموقع الرسمي للمنظمة الدولية للشرطة والإنتربول، المكتب الجامعي الحديث، القاهرة، ذ ط، 2018/06/27 على الساعة 14:30

⁴ - نسرین عبد الحمید نبیه، الجرائم الدولية والإنتربول، المكتب الجامعي الحديث، القاهرة، د ط، 2011، ص 255.

⁵ - رابح نهائي، دور المنظمات الدولية، في مكافحة الجريمة المنظمة (منظمة الأمم المتحدة، المنظمة الدولية للشرطة الجنائية نموذجا)، مجلة البحوث القانونية والاقتصادية، المجلد 04، العدد 02، 2021، ص 134.

لمنع الجريمة الدولية ومكافحتها من خلال تحقيق الأهداف التالية¹:

- الوصل بين أجهزة الشرطة حول العالم لجعلها أكثر أمنا لأجل منع الجريمة ومكافحتها عبر تعزيز التعاون الشرطي الدولي.

- أداء ودور مركز المعلومات العالمي للتعاون بين أجهزة إنفاذ القانون.

- توفير الإمكانيات الشرطية المتطورة التي تساعد البلدان الأعضاء على مكافحة الجرائم العابرة للحدود ومنعها.

- أداء دور طليعي في مجال النهج الابتكارية عالميا للعمل الشرطي.

- تعزيز دور الأنتربول إلى الحد الأقصى داخل البنية الأمنية العالمية.

- توحيد الموارد وبنى الإدارة لتحسين الأداء العملي.

ثالثا: إستراتيجية الإنتربول في مكافحة الجريمة الإلكترونية

تسهر منظمة الإنتربول على تحقيق وظيفتين لمكافحة الجرائم، تتمثل في قيامها بتجميع كافة البيانات والمعلومات المتعلقة بالجريمة والمجرم، وهذا من خلال عمل المكاتب المركزية الوطنية للشرطة الجنائية الدولية المتواجدة في أقاليم الدول الأعضاء، أما الثانية فتتمثل في التعاون في ضبط وملاحقة المجرمين وتسليمهم إلى الدولة التي تطلب تسليمهم، وهي في ذلك متخصصة بمكافحة الإجرام المنظم العابر للحدود بجميع صوره، بما هي ذلك المرتبط بجرائم الأنترنت وفي هذا السياق نجد دعوة سكرتيرها Raymound kendall في مؤتمر جرائم الأنترنت المنعقد في لندن في 2000/10/09 على ضرورة إيجاد تعاون دولي لمكافحة هذا النوع من الإجرام، وعلى ضرورة تقرير ذلك التعاون.

وقد إنعقدت عدة مؤتمرات تؤكد على ضرورة التعاون في مجال مكافحة الجرائم الإلكترونية، وهذا ما أكده المدير التنفيذي للخدمات الشرطية، السيد لوبوتان (le botane) في المؤتمر الدولي السادس بشأن الجرائم الإلكترونية المنعقد بالقاهرة في الفترة ما بين 13 إلى 15 /04/2005، وهذا ما أكدته الإنتربول كذلك في إحدى مؤتمراتها الدولية التي عقدتها في كوريا الجنوبية²، ولم تكتف الإنتربول بعقد المؤتمرات

¹ - المنظمة الدولية للشرطة الجنائية (الإنتربول) البيانات المالية 2016/2017، ص 11.

² - نبيلة هبة هروال، الجوانب الاجرائية، المرجع السابق، ص، ص-150، 151.

فقط بل قامت بإنشاء عام 2004 وحدة خاصة لمواجهة الإجرام المعلوماتي، وذلك بالتعاون مع المجموعة الثمانية G8 من خلال وضع إستراتيجيات لمواجهة الجريمة الإلكترونية، منها إنشاء مركز اتصالات أمني عبر الشبكة تعمل على مدار 24 ساعة 7 أيام في الأسبوع على مستوى مصالح الشرطة في الدول الأطراف، وتسمى المنظومة العالمية للاتصالات وتعرف بمنظومة 24/7، فهي تسمح بتبادل الرسائل بين المكاتب الوطنية للمنظمة في ظرف قصير، مما يسهل عملية ربط البيانات بين مختلف مكاتب العالم كما يسهل إجراء التحقيقات، وتتميز هذه المنظومة بأنها آمنة وتخضع للمعايير القانونية¹ بين مختلف مكاتب العالم كذلك تستعمل المنظمة الدولية للشرطة الجنائية وسائل لمكافحة الجريمة الإلكترونية كاستخدام منظومة قاعدة البيانات² وهي عبارة عن جملة من الملفات والقوائم تحتوي على معلومات تساعد في الكشف عن الجرائم ومرتكبيها.

إضافة إلى ذلك تقوم المنظمة الدولية بتزويد الدول الأطراف بكتيبات إرشادية حول الجرائم الإلكترونية وكيفية التدريب على مكافحتها والتحقيق فيها³، ومن المجهودات الجبارة المبذولة من أجل مكافحة الجريمة الإلكترونية، حيث تلقت النيابة العامة للجمهورية اللبنانية برقية من الإنتربول في ألمانيا، تم على إثرها توقيف أحد الطلبة الجامعيين من قبل القضاء اللبناني بتهمة إرسال صور إباحية لقاصر دون العاشرة من العمر من موقعه على شبكة الأنترنت⁴، وفي سنة 2016 قام الإنتربول والهيئة النيجيرية للجرائم الاقتصادية والمالية في إطار عملية مشتركة بالقبض على زعيم شبكة إجرامية دولية في نيجيريا اسمه "مايك" إشتراك معه ما لا يقل عن أربعين شخصا من نيجيريا وماليزيا وجنوب إفريقيا قاموا بآلاف

¹ - محمد رحموني، المرجع السابق، ص73.

² - ومن ضمن قواعد البيانات نذكر قاعدة البيانات الإسمية وتحتوي هذه القاعدة معلومات دقيقة عن المجرمين المعروفين دوليا، وأشخاص مفقودين، أو جنث غير متعرف عليها، والسجلات القضائية لهؤلاء المجرمين وصورهم وبصماتهم.

- قاعدة بيانات البصمة الجينية (A N D) توفر هذه القاعدة مقارنة البصمات الوراثية المتوفرة المتمثلة في جملة من البصمات الجينية الخاصة بكل فرد لإجراء المطابقات بين شخص وآخر، أو بين مسرح جريمة وشخص.

- قاعدة بيانات البصمات (p f) تمكن هذه القاعدة من الوصول إلى قاعدة المنظمة الدولية للشرطة الجنائية المتلفة بالمعلومات الآمنة لتحقيق بصمات الأصابع، وتتضمن هذه القاعدة معلومات أحييت بشكل مباشر بواسطة جلب الملفات الإلكترونية وتحتوي هذه القاعدة جملة من المعلومات الشخصية يستفاد منها بواسطة برنامجا خاصا يمكن من التعرف على المجرمين، أنظر محمد رحموني، المرجع نفسه، ص، ص 74-75.

³ - نبيلة هبه هروال، المرجع السابق، ص154.

⁴ - حسين بن سعيد بن سيف الغافري، المرجع السابق، ص238.

العمليات الخاصة بالإحتيال عبر شبكة الأنترنت، والتي إستهدفت مئات الضحايا في جميع أنحاء العالم مستعملين مخططات الاحتيال التجارية عبر البريد الإلكتروني.¹

ومن أهم العمليات وبالتنسيق بين منظمة الإنتربول والدول الأعضاء التي تستهدف الإجرام المعلوماتي، عملية انماسك (Anmask) لإستهداف قرصنة الحواسيب على المستوى الدولي والتي أسفرت عن إعتقال 25 شخصا في أمريكا اللاتينية وأروبا، وذلك بتظافر جهود كل من إسبانيا، الأرجنتين، شيلي، كولومبيا، وذلك عقب سلسلة الاعتداءات المعلوماتية المنسقة والتي انطلقت من هذه الدول ضد مواقع إلكترونية حكومية كولومبية.²

وفي الأخير يمكن القول أن المنظمة الدولية للشرطة الجنائية تقوم بعمل جبار من أجل الكشف عن الجريمة والمجرمين.

الفرع الثاني: مركز الشرطة الأوروبية (الأوروبول) Europol

إتجهت الدول الأوروبية إلى تعزيز التعاون الأمني، فيما بين أجهزتها الشرطة في مكافحة الجرائم ذات الخطورة الخاصة، والتي يدخل معظمها ضمن الجريمة المنظمة، بما فيها الجرائم الإلكترونية، فقامت بإنشاء العديد من الهيئات والمنظمات، ولعل أهمها التي لها علاقة بالتعاون بين هذه الدول في المسائل الأمنية المنظمة الأوروبية للشرطة الجنائية، التي تعد نموذجا فريدا في مكافحة الجريمة بصفة عامة والجرائم العابرة للحدود بصفة خاصة، ومنها الجريمة الإلكترونية.³

نتناول نشأتها ومهامها (أولا) وجهودها في مكافحة الجريمة الإلكترونية (ثانيا).

أولا: نشأة الأور بول

الأور وبول أحد الأجهزة المتواجدة على المستوى الأوروبي، وتعود فكرة إنشائها للمستشار الألماني Helmut Kohl أثناء إنعقاد قمة لكسمبورغ في 23/06/1991، بحيث يكون هذا الجهاز على نموذج

¹ - خضرة شنيخر، المرجع السابق، ص213.

² - حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، المرجع السابق، ص152.

³ - محمد حبيب عباسي، الجريمة المنظمة العابرة للحدود، أطروحة لنيل شهادة دكتوراه علوم، كلية الحقوق والعلوم السياسية، جامعة ابو بكر بلقايد، تلمسان، الجزائر، 2016/2017، ص583.

الشرطة الفدرالية الألمانية أي بمثابة "F B I" مكتب فيدرالي أوروبي للتحقيقات¹، تمت الموافقة على تأسيس وكالة الأور وبول على إثر معاهدة ماسترخت سنة 1992، وتم التوقيع على إتفاقية إنشاء جهاز الأوروبول في 1995/07/23، والتي دخلت حيز النفاذ في أول أكتوبر 1998 واتخذت من لاهاي بهولندا مقرها.

وتتمحور مهام الأوروبول حول تحسين التعاون الشرطي بين الدول الأعضاء في الإتحاد الأوروبي، في ميدان مكافحة كل الأشكال الخطيرة للإجرام الدولي، ومنها الجرائم الإلكترونية، حيث يقوم الجهاز بتسهيل تبادل المعلومات بين أجهزة الشرطة في الدول الأعضاء، وتجميع وتحليل المعلومات الأمنية المصالح المختصة في نفس الدول بالمعلومات، التي تهمها حول مختلف الأنشطة الإجرامية في الفضاء الأوروبي، كما تعمل على تسهيل جمع المعلومات، وإعادة نشرها في مختلف مصالح الشرطة للدول الأعضاء، وتقديم الخبرة والمساعدة الفنية تحت المسؤولية والرقابة القضائية للدول الأعضاء، وإعداد تقارير إستراتيجية في ميدان تقييم مخاطر الإجرام²، بما فيها المخاطر المتعلقة بالجرائم الإلكترونية، كما يتولى الأور بول تقديم النصيحة والتوجيهات والإرشادات المفيدة ومختلف أنواع الدعم (المادي واللوجستيكي) لهيئات التحقيق الوطنية لتنفيذ هذه المهام يضمن هذا الجهاز اتصالا دائما ومتوصلا مع السلطات المختصة³ في الدول الأعضاء عن طريق ما يسمى بنقاط إتصال.

ثانيا: جهود الأوروبول في مكافحة الجريمة الإلكترونية

للأور بول دورا فعالا في مجال مكافحة الجريمة الإلكترونية، حيث يختص بكل أشكال الإجرام التي ترتكب بواسطة التكنولوجيا الرقمية، تكون إحدى المنظمات الإجرامية الناشطة على الإقليم الأوروبي طرف فيها⁴، فقامت الأور بول بعدة عمليات في مجال الجرائم الإلكترونية، أهمها وأبرزها عملية أوديسيوس (odysseus) التي تمت في 26 فبراير 2004 بمبادرة من الأوروبول، حيث قامت قوات الشرطة بعمليات شملت عدة دول هي: إستراليا، بلجيكا، كندا، ألمانيا هولندا، بيلرو، إسبانيا، السويد، وبريطانيا،

¹ - جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالأنترنت، المرجع السابق، ص79.

² - خديجة مجاهد، آليات التعاون الدولي لمكافحة الجريمة المنظمة، أطروحة لنيل شهادة دكتوراه علوم، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، الجزائر، 2018، ص، ص، 410-411.

³ - جمال إبراهيمي، المرجع السابق، ص، ص، 303-304.

⁴ - Myriam quémener ,Joël ferry ,op,cit , p237.

كذلك عملية محطم الجليد (ice breaker) في 14 يونيو 2005، حيث تمكنت من مداهمة وتفتيش أماكن في ثلاثة عشرة دولة أوروبية وتوقيف العديد من الأفراد في كل من فرنسا، بلجيكا، المجر، السويد¹، كما قام بإستحداث جهاز على مستوى الأوروبي عام 2010 أطلق عليه إسم (internet crime reporting on line icros) مهمته توفير أكبر قدر ممكن من التعاون الأمني السريع في مجال مكافحة الجريمة الإلكترونية بين دول الإتحاد الأوروبي، وفي سنة 2017 تم تدعيم هذا الجهاز بهيئة متخصصة تدعى المركز الأوروبي للجريمة الإلكترونية، فهو همزة وصل بين الدول الأعضاء، وركز جهوده في تقديم الدعم الإستخباراتي والتشغيلي والقضائي للرد على الجرائم الإلكترونية.²

يقدم الأوروبي مجهودات جبارة من خلال دعمه للحكومات والأجهزة الأمنية ضد أخطار الجريمة الإلكترونية، لهذا فقد تم إختياره من قبل الإتحاد الدولي للأمن المعلوماتي، لإنجازه مختلف الدراسات الخاصة بالجريمة الإلكترونية، وذلك إلى غاية 2020 بهدف تحليل دوافع الجرائم الإلكترونية، ووضع تصور لتطورها.³

كما تعمل على بسط خبرتها وتجربتها في مجال مكافحة الجريمة الإلكترونية، وتقديم العون لمختلف الدول من خارج الإتحاد الأوروبي، كأستراليا وكندا والولايات المتحدة الأمريكية، أو في إطار الشراكة التي تبرمها آليات أخرى للتعاون الشرطي، كالشراكة التي دعا إليها المدير العام للأمن الوطني عبد الغاني هامل بإعتباره رئيسا لأفريبول بين أفريبول والأوروبول من أجل تأسيس شراكة عملياتية بينها تتدرج في إطار المشاورات الأمنية حول العديد من المسائل، لا سيما الجريمة العابرة للحدود الوطنية ومنها الجريمة الإلكترونية.⁴

¹ - جان فرانسو هروت، أهمية التعاون الدولي والتجربة البلجيكية في تبادل المعلومات بين عناصر الشرطة والتعاون القضائي، بحث مقدم إلى الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر ضمن برنامج تعزيز حكم القانون في بعض الدول العربية " مشروع تحديات النيابات العامة المملكة المغربية، المنعقدة ما بين 19-20 جوان 2007، ص 108.

² - جمال إبراهيمي، المرجع السابق، ص 306.

³ - حسين ربيعي، المرجع السابق، ص 153.

⁴ - مقال بعنوان هامل يدعو إلى شراكة عملياتية قوية بين أفريبول وأوروبول، منشور على الموقع : www.radio.algerie.dz/neus/ar/article/2018/02/27 أطلع عليه يوم 2018/10/25 الساعة 14:30.

ثالثا: الأور جست Eurojust

يتواجد هذا الجهاز على المستوى الأوروبي، يساعد على التعاون القضائي والشرطي في مواجهة ومكافحة جميع أنواع الجرائم بما فيها الجرائم الإلكترونية، وتم إنشائه سنة 2002 من قبل مجلس الاتحاد الأوروبي بتاريخ 22/02/2002¹، إن الميزة الأساسية لجهاز الأور جست هي البعد البين- حكومي la dimension intergouvernementale وهو جهاز يتمتع بالشخصية القانونية، يتكون من عضو وطني منتدب من كل دولة عضو في الاتحاد الأوروبي، بشرط أن يكون متمتعاً بصفة مدعى عام، قاضي أو ضابط شرطة، كما أن كل عضو وطني يخضع لقانون دولته فيما يخص نظامه الأساسي.²

وما تجدر الإشارة إليه، أن الأور جست يمثل دعامة في فعالية التحقيقات والمطاردات المتبعة من قبل السلطات القضائية الوطنية وخصوصا فيما يتعلق بالأنشطة المرتبطة بالجرائم الإلكترونية، وهو بذلك له علاقة وطيدة مع الأوروبيول يمدّها بالتحليلات اللازمة للقيام بالتحقيقات في الجرائم المنظمة³، وتتمثل أهداف جهاز الأور جست كما وضحتها المادة الثالثة من قرار تأسيسها وهي:

- ترقية وتحسين التنسيق بين السلطات المختصة للدول الأعضاء فيما يخص التحقيقات والمتابعات .
- تنفيذ طلبات التعاون القضائي والقرارات المرتبطة بهذا المجال، والمتعلقة خاصة بالأدوات المفعلة لمبدأ الاعتراف المتبادل .

- تدعيم السلطات المختصة بالدول الأعضاء على تقوية فعالية تحقيقها ومتابعتها.⁴

الفرع الثالث: شرطة الأفريبول

تعتبر الأفريبول أو ما يعرف بآلية الاتحاد الإفريقي للتعاون الشرطي، من بين الأجهزة الشرطية الحديثة، على مستوى القارة الإفريقية، التي تنشط في مكافحة الجريمة المنظمة العابرة للحدود الوطنية ومنها الجريمة الإلكترونية، وترجع فكرة إنشائها سنة 2013 بمناسبة إنعقاد المؤتمر الإقليمي الإفريقي

¹ - هبة نبيلة هروال، الجوانب الإجرائية، المرجع السابق، ص159.

² - سفيان كعرار، الآليات المؤسسية الأوروبية لمكافحة الجريمة المنظمة عبر الوطن، المجلة الأكاديمية، للبحوث القانونية والسياسية، المجلد الرابع، العدد الأول، 2020، ص581.

³ - هبة نبيلة هروال، المرجع السابق، ص160.

⁴ - سفيان كعرار، المرجع السابق، ص581.

الـ 22 للإنتربول والمنعقد في الفترة الممتدة من 10 إلى 12 سبتمبر 2013¹ بوهران، والتي شهدت حضور كافة قادة الشرطة الأفارقة الواحد والأربعون، وبمناسبة إنعقاد المؤتمر الإفريقي للمدراء والمفتشين العاملين للشرطة، الذي إنعقد بالجزائر يوم 10 فيفري 2014 وبدعوة من المدير العام للأمن الوطني السابق، الذي أكد على تعميم التعاون بين الشرطة الإفريقية، من خلال إستحداث آلية أفر يبول لمواجهة التحديات الأمنية التي تواجهها القارة الإفريقية، مجددا الدعم الدائم للجزائر من أجل تجسيد مشروع إنشاء الآلية²، وفي الدورة العادية الخامسة والعشرين للمجلس التنفيذي للاتحاد الإفريقي، المنعقد في يونيو 2014 في غينيا، تم إعتماد إعلان الجزائر بخصوص إنشاء الأفر يبول من قبل المجلس التنفيذي في الإتحاد بموجب القرار (xxv) EX cl/ dec. 820³، وفي سنة 2015 وبإنعقاد المؤتمر 39 الخاص بقيادة الأمن والشرطة العرب، تبنى المشاركون وبإجماع المبادرة التي تقدمت بها الجزائر حول إنشاء هذه الآلية، وذلك بإعتبار أن عشر دول تقع بالقارة الإفريقية ويكون مقرها الجزائر، وبتاريخ 13 ديسمبر 2015 تم الإفتتاح الرسمي لمقر الأفر يبول" الذي أقيم بالعاصمة الجزائرية بحضور ممثلي 41 بلدا إفريقيا، وبتاريخ 30 جانفي 2017 تم إعتماد النظام الأساسي لآلية الإتحاد الإفريقي للتعاون الشرطي "الأفر يبول" من قبل مؤتمر الإتحاد الإفريقي في دورته العادية رقم 28 المنعقدة بأديس أبابا- إثيوبيا ودخل حيز النفاذ بالتاريخ السالف الذكر⁴.

وترتكز مهام الأفر يبول في مضاعفة رصيد التعاون الشرطي الإقليمي والدولي، تحديد السياسة العامة للشرطة الجنائية، وتوفير التكوين وإعادة تأهيل أجهزة الشرطة الإفريقية التي تشهد تأخر أو ضعفا على مستوى الأداء⁵، وتطوير قدرات أجهزة الشرطة في الدول الأعضاء عن طريق العمل على إستحداث مراكز إمتياز إفريقية، تعتمد على برامج لتدريب الشرطة تتكيف مع واقع السياق الإفريقي، كما تقوم الشرطة الإفريقية على مكافحة الجريمة الإلكترونية، من خلال تبادل المعلومات والإستخبارات

¹ - خديجة خالدي، آلية الاتحاد الإفريقي للتعاون الشرطي، "أفر يبول"، مجلة العلوم الاجتماعية والإنسانية، العدد الخامس عشر، 20187، ص 67.

² - أحلام بوكربوعة، آلية الإتحاد الإفريقي للتعاون الشرطي "أفر يبول" ودورها في مكافحة ظاهرة الإرهاب، حوليات الجزائر 1، المجلد 34، العدد 04، ديسمبر 2020، ص 607.

³ - خديجة خالدي، المرجع السابق، ص 67.

⁴ - أحلام بوكربوعة، المرجع السابق، ص 608.

⁵ - جمال إبراهيمي، المرجع السابق، ص 313.

وفقا لما ورد في نص المادة 4 فقرة " من النظام الأساسي للأفريبول " تيسير تبادل وتقاسم المعلومات أو الإستخبارات لمنع ومكافحة الجرائم المنظمة العابرة للحدود الوطنية والإرهاب والجريمة الإلكترونية.

المطلب الثالث: تسليم المجرمين

يعد نظام تسليم المجرمين وسيلة ضرورية للتعاون القضائي الدولي، إذ يؤدي إلى وضع الشخص تحت أيدي السلطات المختصة في الدولة الطالبة، لإرتكابه جريمة أو صدور حكم ضده بالعقاب وتتخذ إجراءات تنفيذه¹، ويهدف التسليم إلى الحيلولة دون إفلات المجرم من العقاب، ولأهمية الموضوع سوف نتطرق إلى مفهوم التسليم (الفرع الأول) شروطه (الفرع الثاني) وإجراءاته (الفرع الثالث).

الفرع الأول: مفهوم التسليم

قبل الخوض في الأحكام المتعلقة بالتسليم خاصة شروطه وإجراءاته، يجب التطرق أولا إلى تعريفه ومصادره

الفقرة الأولى: تعريف نظام تسليم المجرمين² ومصادره

سوف نتناول أولا إلى تعريف التسليم، ثم إلى مصادره ثانيا.

أولا: تعريف التسليم

يعرف بأنه "إجراء من إجراءات التعاون القضائي الدولي، تقوم بموجبه إحدى الدول بتسليم شخص متواجد على إقليمها، إلى دولة أخرى أو إلى جهة قضائية دولية، إما بهدف محاكمته عن جريمة أتهم بإرتكابها، وإما لأجل تنفيذ حكم الإدانة الصادر ضده من محاكم هذه الدولة أو المحكمة الدولية.³"، كما يعرف أيضا بأنه "قيام دولة ما (الدولة المطلوب فيها التسليم بتسليم شخص، موجود في إقليمها إلى دولة أخرى(الدولة طالبة التسليم) بناء على طلبها، بغرض محاكمته عن جريمة معينة، نسبت إلى هذا المتهم

¹ - Philippe Richard, droit de l'extradition de terrorisme risques d'une pratique incertaine du droit a f d i vol 34, 1988,p654.

² - إن إصطلاح تسليم المجرمين يعد الترجمة العربية بكلمة « extradition » الفرنسية والتي أستعملت لأول مرة في مرسوم 19 فيفري 1971 في فرنسا وكلمة extradition التي أشتقت من الفرنسية، وإستعملت لأول مرة في قانون التسليم لسنة 1870 وتعني الترحيل، أنظر نادية دردار، الجهود الدولية لمكافحة الجريمة، المركز القومي للإصدارات القانونية، القاهرة ط 1، 2017، ص 102.

³ - عبد القادر عمير، المرجع السابق، ص361.

إرتكابها، وقد يكون التسليم بغرض تنفيذ حكم صدر ضده بالعقاب.¹، وعرف أيضا " وهو أن تتخلى دولة عن شخص موجود في إقليمها إلى دولة أخرى بناء على طلبها لتحاكمه عن جريمة يعاقب عليها القانون الدولي، أو لتنفيذ حكما صادرا عليه من محاكمتها.²

وقد نظم المشرع الجزائري تسليم المجرمين في الكتاب السابع من ق.إ.ج.ج تحت عنوان " العلاقات بين السلطات القضائية الأجنبية "، وخص الباب الأول منه لتسليم المجرمين ونصت عليه المادة 82 من دستور 2016.³

ثانيا: مصادر نظام تسليم المجرمين

تتعدد مصادر نظام التسليم، وقد إستقر الفقهاء على تصنيفها إلى ثلاث مصادر هي:

1- الإتفاقيات الدولية

وقد تكون هذه الإتفاقيات ثنائية⁴، وهي التي تتم بين دولتين وفقا لشروط وضوابط موضوعية من قبل الدولتين، وقد تكون اتفاقيات التسليم متعددة الأطراف، وقد وضعت الأمم المتحدة سنة 1990 معاهدة نموذجية لتسليم المجرمين، لتكون إطارا يساعد الدول على التفاوض إتفاقيات التسليم⁵، وإتفاقية التسليم بين دول جامعة الدول العربية الموقعة بالقاهرة 09/06/1953 والتي حلت محلها إتفاقية الرياض للتعاون القضائي 06/04/1983.

ولعل من أهم الإتفاقيات التي نصت على إجراء تسليم المجرمين في مجال الجريمة الإلكترونية، إتفاقية بودابست (الاتفاقية الأوروبية) من خلال المادة 24 منها والتي جاءت كما يلي " تطبق هذه المادة على تسليم المجرمين بين الدول الأطراف، بالنسبة للجرائم المنصوص عليها في المواد من 2 إلى 11 من

¹ - غانم مرضي الشمري، المرجع السابق، ص102.

² - عبد القادر البقيرات، العدالة الجنائية الدولية، ديوان المطبوعات الجامعية، الجزائر، حط، 2005، ص134.

³ - تنص المادة 82 من قانون 01/16 المؤرخ في 06 مارس 2016 المتضمن التعديل الدستوري بأنه " لا يسلم أحد خارج التراب الوطني إلا بناء على قانون تسليم المجرمين وتطبيقا له".

⁴ - تربط الجزائر بعدة إتفاقيات ثنائية في مجال التسليم نذكر منها : الإتفاقية المتعلقة بتنفيذ الأحكام وتسليم المجرمين مع فرنسا ج ز رقم 68 سنة 1965، الإتفاقية المتعلقة بتسليم المجرمين مع باكستان ج ر رقم 27 سنة 2002 وغيرها من الاتفاقيات الثنائية ...

⁵ - غانم مرضي الشمري، المرجع السابق، ص 103.

هذه الإتفاقية، شريطة أن يعاقب على هذه الجرائم بموجب قوانين كلا الطرفين، بعقوبة سالبة للحرية لمدة سنة على الأقل أو بعقوبة أشد، وهو نفس الإتجاه التي تبنته الإتفاقية العربية لمكافحة جرائم تقنية المعلومات على تسليم المجرمين بموجب المادة 31¹ منه، التي جاءت متطابقة مع المادة 24 من إتفاقية بودابست لسنة 2001.

2 - القوانين الداخلية

يعتبر التشريع الوطني في دول عديدة مصدرا أساسيا لأحكام التسليم، تلجأ إليه الدول لتنظيم كافة المسائل المتعلقة بتسليم المجرمين، أي حالة عدم وجود إتفاقية دولية ترتبط بها هذه الدولة²، ويكون ذلك عبر قانون مستقل كالتشريع الفرنسي، أو في شكل نصوص ممزوجة في قانون آخر كقانون الإجراءات الجزائية مثلا، كالمرشح الجزائري الذي عالج نظام تسليم المجرمين في المواد من 694 إلى 720 من قانون إجراءات جزائية³.

وعلى الرغم من دور التشريعات الوطنية المختلفة في إثراء وتطوير نظام تسليم المجرمين، لكن إختلاف هذه التشريعات تؤثر سلبا على وحدة و إنسجام النظام القانوني للتسليم⁴، وبذلك من شأن هذا التباين أن يعطي للاتفاقيات أهمية خاصة، لأن تكون المصدر الوحيد لتطوير وتحسين نظام وحدة إنسجام النظام القانوني للتسليم.

3 - المعاملة بالمثل

إن مبدأ المعاملة بالمثل، مبدأ دولي أساسه السابقة في التعامل، ففي حالة عدم وجود إتفاقية دولية

¹ - تنص المادة 31 من الإتفاقية العربية لمكافحة تقنية المعلومات على أنه " 1 . p هذه المادة تطبق على تبادل المجرمين بين الدول الأطراف على الجرائم المنصوص عليها في الفصل الثاني من هذه الإتفاقية بشرط أن تكون تلك الجرائم يعاقب عليها في قوانين الدول الأطراف المعنية بسلب الحرية لفترة أدناها واحدة أو بعقوبة أشد ..."

² - بالرغم من عدم وجود إتفاقية تسليم المجرمين بين الجزائر وبريطانيا، فقد أعلن القضاء البريطاني رسميا تسليم وفيق عبد المؤمن خليفة إلى السلطات الجزائرية في 25 جوان 2009 بعد تقديم الجزائر طلب تسليمه لها بسبب تورطه في قضية فساد، وصدور ضده حكم غيابيا من طرف السلطات الجزائرية بالسجن المؤبد.

³ - نظمت العديد من الدول نظام تسليم المجرمين بالنص عليه في قانون إجراءات جزائية منها التشريع التونسي في المواد من 308 إلى 335 ق.إ.ج. ت، التشريع اللبناني في المواد من 30 إلى 36، القانون الإيطالي من المواد 701 إلى 720 ق.إ.ج.إ.

⁴ - نادية دردار، المرجع السابق، ص 35.

تنظم إجراءات التسليم، فإن الكثير من الدول ونظرا للحتمية الدولية لنظام التسليم، توافق على طلب التسليم إستنادا لمبدأ المعاملة بالمثل، والذي يعني تطابق الحقوق والالتزامات أو على الأقل تكافؤها في مجال العلاقات الدولية، والذي يعد مصدرا توجيهيا في مجال تسليم المجرمين.¹

ثالثا: شروط التسليم

التسليم نظام له شروطه وإجراءات لا بد من توافرها، حتى يجد التسليم قبولا لدى سلطات دولة الملجأ، لذلك خص المشرع الجزائري بشيء من الدقة والتفصيل، في الفصل الثاني من الباب الأول من الكتاب السابع في المواد من 694 إلى 701 من ق.إ.ج.ج.

1- الشروط المتعلقة بالجريمة سبب التسليم

نص المشرع الجزائري على الأفعال التي يجوز التسليم من أجلها للدولة الطالبة، وذلك بموجب نص المادة 697 من ق.إ.ج.ج وهذا في حالة ارتكاب الشخص المطلوب تسليمه، لفعل يوصف بأنه جناية أو جنحة حتى تقبل الدولة الجزائرية التسليم، لا بد أن يكون هذا الفعل معاقبا عليه في قانون العقوبات الجزائري بعقوبة جناية أو جنحة على إعتبار أن الجزائر تأخذ بنظام التجريم المزدوج، وعليه سوف نبين الأفعال التي يجوز التسليم فيها:

أ- الجنائيات: يجوز تسليم الشخص الذي ارتكب فعل جنائية في كلا الدولتين الدولة الطالبة والمطلوب إليها، وهذا ما جاء في نص المادة 697 ق.إ.ج.ج على أن "جميع الأفعال التي يعاقب عليها قانون الدولة الطالبة بعقوبة جناية".

ب- الجنح: أجاز المشرع الجزائري طلب التسليم، إذا كان الفعل المترتب يأخذ صفة جنحة ولكن يكون بشروط وهي:

- إذا كانت الجنحة حدها الأقصى المقرر للعقوبة هي الحبس لمدة سنتين أو أقل.

- صدور حكم في حق مرتكب الجنحة بعقوبة تساوي أو تجاوز الحبس لمدة شهرين وفيما يخص الجرائم الإلكترونية، فهي ينطبق عليها نص المادة 697 من ق.إ.ج.ج، وذلك أن هذه الجرائم وصفها جنح في قانون العقوبات الجزائري ومعاقب عليها بالحبس من ثلاث أشهر إلى سنة طبقا لنص المادة 394

¹ - عبد القادر عمير، المرجع السابق، ص 363.

مكرر/1¹، فهي بذلك تمس أحد الشروط الأساسية لآلية تسليم المجرمين.

2 - الشروط المتعلقة بالشخص المطلوب تسليمه

لا تسلم الدولة الجزائرية مواطنيها الجزائريين الذين يتمتعون بالجنسية المكتسبة، سواء كانوا يتمتعون بها بصفة أصلية أو مكتسبة، طبقا لنص المادة 1/698 من ق.إ.ج.ج والتي تنص على "لا يقبل التسليم في الحالات الآتية:

-إذا كان الشخص المطلوب تسليمه جزائري الجنسية والعبرة في تقدير هذه الصفة بوقت وقوع الجريمة المطلوب التسليم لأجلها."

ولكن عدم تسليم المجرمين من مواطني الدولة، لا يعني إفلاتهم من العقاب إذ تنص الكثير من القوانين الوطنية والإتفاقيات الدولية ذات الصلة، على ضرورة محاكمتهم أمام القضاء الوطني، وهذا ما يعرف بمبدأ التسليم أو العقاب، إلا أن المشرع الجزائري لم يشر إلى هذا المبدأ، وكان عليه أن يحدد موقفه هذا بشأن رفضه التسليم.

الفرع الثاني: إجراءات التسليم

يتم تسليم المجرمين وفق إجراءات معينة منصوص عليها في قوانين الدولة.

أولا: إجراءات التسليم في الجزائر

نظم المشرع الجزائري إجراءات التسليم من بداية تقديم الطلب إلى غاية تنفيذه، وهذا بموجب المادة 702 وما يليها من ق.إ.ج.ج فنصت على "يوجه طلب التسليم إلى الحكومة الجزائرية بالطريق الدبلوماسي، ويرفق به الحكم بالعقوبة، حتى ولو كان غايابا وإما أوراق الإجراءات الجزائرية التي صدر بها الأمر رسميا بإحالة المتهم إلى جهة القضاء الجزائي أو التي تؤدي إلى ذلك بقوة القانون، وإما أمر القبض أو أية ورقة صادرة من السلطة القضائية ولها ذات القوة، على أن تتضمن هذه الأوراق الأخيرة بيانا دقيقا للفعل الذي صدرت من أجله وتاريخ هذا الفعل ويجب أن تقدم أصول الأوراق المبينة أعلاه أو نسخ رسمية فيها:" وهذا ما يدل على أن طلب التسليم يكون مكتوبا وهذا ما أكدته المادة السالفة الذكر.

¹ - تنص المادة 394 مكرر الفقرة الأولى من قانون 02/16 على أنه "يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50000 دج إلى 200000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعاينة الآلية للمعطيات أو يحاول ذلك."

يجب على الحكومة الطالبة أن تقدم في الوقت ذاته، نسخة من النصوص المطبقة على الفعل المكون للجريمة وأن ترفق بيانا بواقع الدعوى، بعد فحص المستندات يتولى وزير الخارجية تحويل طلب التسليم إلى وزير العدل، الذي يحقق من سلامة الطلب ثم يعطيه خط السير التي يتطلبه القانون.¹

يوجه الملف إلى النائب العام، حيث يتم استجواب الشخص الأجنبي للتحقق من شخصيته وهويته وبيلغه المستند الذي قبض عليه بموجبه وذلك خلال 24 ساعة التالية للقبض عليه ويحرر محضرا بذلك²، ثم يتم نقله إلى السجن بالعاصمة ويحول الملف والمستندات المرفقة، إلى النائب العام بالمحكمة العليا الذي يقوم باستجوابه أيضا في خلال 24 ساعة وتحرير محضر بذلك، ثم يحال الملف على الغرفة الجنائية بالمحكمة العليا لتقوم باستجوابه خلال ثمانية أيام بعد إستلامها للملف وتحرير محضر بذلك ثم تقوم بالنظر في الملف في جلسة علنية إلا إذا طلبت النيابة أو الشخص المطلوب أن تكون في جلسة سرية.

ويمكن للمطلوب التنازل عن المحاكمة والقبول بطلب التسليم فتثبت المحكمة هذا القرار وتحيل نسخة منه إلى وزير العدل عن طريق النائب العام بدون تأخير لاتخاذ ما يراه مناسبا بشأنه، وفي حالة العكس أي إذا تمسك المعني بالمحاكمة ففي هاته الحالة تقوم المحكمة العليا بالنظر في الملف بعد تقديم المعني أوجه دفاعه ويمكنه الاستعانة بمحام في ذلك، وبعدها تبدي المحكمة رأيها المعلن في الطلب بالرفض أو القبول، ويجب إعادة الملف خلال 8 أيام ابتداء من انقضاء الأجل السابق ذكره، وفي حالة رفض طلب التسليم يكون هذا الرأي نهائيا ولا يتم تسليم المطلوب، أما في حالة قبول الطلب يقوم وزير العدل بتوقيع مرسوم بالتسليم يبلغ للدولة طالبة التسليم، وفي حالة عدم قيام ممثلو الدولة طالبة التسليم بتسلم الشخص المعني خلاله مدة شهر من تاريخ تبليغ المرسوم يفرج عن هذا الأخير ولا يقبل أي طلب آخر في نفس الموضوع.

ويمكن في حالة الاستعجال يجوز لوكيل الجمهورية لدى المجلس القضائي وبناء على طلب مباشر من السلطات القضائية للدولة الطالبة أن يأمر بالقبض المؤقت على الأجنبي وذلك أن أرسل إليه مجرد إخطار سواء بالبريد أو بأي طريق من طرق الإرسال الأكثر سرعة التي يكون لها أثر مكتوب، ويجب على النائب العام أن يحيط وزير العدل والنائب العام لدى المحكمة العليا علما بهذا القبض، ولكن يجوز أن يفرج عن الشخص الذي قبض عليه مؤقتا وفقا للشروط المنصوص عليها بالمادة 705 من ق.إ.ج.ج

¹ - المادة 703 من قانون الإجراءات الجزائية الجزائري.

² - المادة 704 من قانون الإجراءات الجزائية الجزائري.

إذا لم تتلق الحكومة الجزائرية المستندات الواردة في المادة 702 خلال 45 يوما من تاريخ القبض عليه. ويتقرر الإفراج بناء على عريضة توجه إلى المحكمة العليا التي تفصل فيها خلال 8 أيام بقرار لا يقبل الطعن فيه، وإذا وصلت المستندات المشار إليها أعلاه بعد ذلك إلى الحكومة الجزائرية فتستأنف الإجراءات طبقا للمادة 703 وما بعدها.

وفي الأخير نقول أن الجريمة الإلكترونية لها طابع دولي، مما يلزم الدول على التعاون فيما بينها من خلال وضع آليات كتسليم المجرمين لمحاربتها، حتى لا يفلت المجرم المعلوماتي من العقاب، لهذا نجد المشرع الجزائري أولى أهمية كبيرة للتعاون الدولي وخاصة في مجال المساعدة القضائية، محاولا مواكبة ما أورده الإتفاقيات في هذا المجال، ولاسيما لإتفاقية بودابست لمكافحة الجريمة الإلكترونية، وكذا الاتفاقية العربية لمكافحة تقنية المعلومات والتي صادقت عليها الجزائر، وقد جسد المشرع أحكام التعاون الدولي في القانون 04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، وذلك تحقيقا للتحديات التي تفرضها الجريمة الإلكترونية، وبالرغم من حتمية التعاون القضائي في مجال مكافحة إلا أنه ثمة صعوبات تقف دون تحقيقه.

ثانيا: الصعوبات التي تواجه التعاون الدولي

إن التعاون الدولي بكافة صوره في مجال مكافحة الجريمة الإلكترونية، وإن كان مطلبا تسعى إلى تحقيقه أغلب الدول إن لم يكن كلها، إلا أنه ثمة صعوبات ومعوقات تقف دون تحقيقه.

1- تنوع واختلاف النظم القانونية الإجرائية

بسبب تنوع واختلاف النظم القانونية الإجرائية، قد تكون هناك طرق للتحري والتحقيق التي تثبت فعاليتها في دولة ما، قد تكون عديمة الفائدة في دولة أخرى أو قد لا يسمح بإجرائها، كما هو الحال بالنسبة للمراقبة الإلكترونية، فإذا اعتبرت طريقة من طرق جمع الإستدلالات أو التحقيق أنها قانونية في دول معينة قد تكون ذات الطريقة غير مشروعة في دول أخرى، بالإضافة إلى أنه قد لا تسمح دولة ما بإستخدام دليل إثبات جرى جمعه بطرق ترى هذه الدول أنها طرق غير مشروعة.¹

¹ - يوسف حسن يوسف، المرجع السابق، ص، ص 186 - 187.

2 - مشكلة تنازع الاختصاص القضائي

تشير مسألة الاختصاص القضائي في الجرائم الإلكترونية، سواء على المستوى الدولي حيث إختلاف التشريعات والنظم القانونية، والتي ينجم عنها تنازع بين الدول بالنسبة لهذا النوع من الجريمة، والتي تتميز بكونها عابرة للحدود، فقد يحدث أن ترتكب الجريمة في إقليم دولة معينة من قبل أجنبي، فهنا تكون الجريمة خاضعة للاختصاص الجنائي للدولة الأولى إستنادا إلى مبدأ الإقليمية، تخضع كذلك للاختصاص الدولة الثانية على أساس مبدأ الاختصاص الشخصي في جانبيه (السلبى والايجابى)، وقد تكون هذه الجريمة من الجرائم التي تهدد أمن وسلامة دولة أخرى، فتدخل في إختصاصها إستنادا إلى مبدأ العينية، كما تثار فكرة تنازع الاختصاص القضائي في حالة تأسيس الاختصاص على مبدأ الإقليمية، كما لو قام الجاني بعرض الصور ذات الطابع الإباحي، من إقليم دولة معينة وتم الإطلاع عليها في دولة أخرى، ففي هذه الحالة يثبت الاختصاص وفقا لمبدأ الإقليمية لكل دولة من الدول التي مستها الجريمة.¹

3 - الاشكاليات الخاصة بالإنبابة القضائية

وتتمثل هذه الاشكالات في:

أ - إشكالية فكرة السيادة

يقصد بفكرة السيادة أن الدولة هي السلطة العليا لا تعلوها سلطة في الداخل والخارج، بما يعنيه ذلك من إستئثار جهة الحكم في الدولة بكافة إختصاصات السلطة ومظاهرها، دون أن تخضع في ذلك لأي جهة أعلى، ودون أن تشارك معها في ذلك سلطة أو جهة مماثلة.

فعند ارتكاب شخص لجريمة من الجرائم الإلكترونية في إحدى الدول، وتجري محاكمته في دولة أخرى، فمن المنطق البحث عن كافة أدلة إثبات تلك الجريمة أو نفيها في البلد الذي وقعت فيه، بإعتبارها كانت مسرحا للجريمة، وهذا ما يعرف بالتعاون القضائي بين الدول، غير أن هذا التعاون قد يصطدم بفكرة سيادة كل دولة على إقليمها، بإعتبار أن كل دولة تقوم بنفسها بالفصل في المنازعات التي تقع على أراضيها، وعن طريق أجهزتها القضائية لإعتبارات ترتبط بالسيادة، وبالتالي إدخال فكرة السيادة قد يعوق التعاون القضائي بين الدول المختلفة في مكافحة الجرائم الإلكترونية.²

¹ - غانم مرضي الشمري، المرجع السابق، ص 126.

² - عبد العال خرشي، المرجع السابق، ص 244.

ب - إشكالية البطء في إجراءات الإنابة

الأصل بالنسبة لطلبات الإنابة القضائية الدولية، والتي تعد من صور المساعدة القضائية الدولية في المجال الجنائي أن تسلم بالطرق الدبلوماسية، وهذا ما يجعلها تتسم بالبطء والتعقيد، والذي يتعارض مع طبيعة الأنترنت وما تتميز به من سرعة، وهو الأمر الذي غنعكس على الجرائم الإلكترونية¹، كذلك من الصعوبات التباطؤ في الرد، حيث أن الدولة متلقية الطلب غالبا ما تكون متباطئة في الرد على الطلب، سواء بسبب نقص الموظفين المدربين أو نتيجة الصعوبات اللغوية أو الفوارق في الإجراءات التي تعقد الإستجابة وغيرها من الأسباب².

4 - الإشكالات المتعلقة بتسليم المجرمين

وتتمثل أهم الإشكالات في إشكاليتين إزدواجية التجريم والتزام في طلبات التسليم.

أ - إزدواجية التجريم

التجريم المزدوج من أهم شروط نظام تسليم المجرمين، تتضمن القوانين الوطنية والإتفاقيات الدولية المتعلقة بتسليم المجرمين، لهذا الشرط واعتباره كشرط أساسي للاستجابة لطلبات التسليم، وبالرغم من أهميته، نجده عقبة أمام التعاون الدولي في مجال تسليم المجرمين بالنسبة للجرائم الإلكترونية، لا سيما وأن معظم الدول لا تجرم هذه الجرائم، بالإضافة إلى أنه من الصعوبة تحديد فيما إذا كانت النصوص التقليدية لدى الدولة المطلوب منها التسليم يمكن أن تنطبق على الجرائم الإلكترونية أو لا الأمر الذي يعيق تطبيق الإتفاقيات الدولية في مجال تسليم المجرمين، يحول جمع الأدلة ومحاكمة المجرمين³.

ب - التزام في طلبات التسليم

ويقصد بالتزام في طلبات التسليم أو تنازع الطلبات، تلك الحالة التي يصل فيها إلى الدول المطلوب منها التسليم أكثر من طلب عدة دول تطلب ذات الشخص، سواء كان الطلب متعلق بنفس الجريمة أو بجرائم أخرى⁴.

¹ - يوسف حسن يوسف، المرجع السابق، ص 188.

² - غانم مرضي الشمري، المرجع السابق، ص 127.

³ - يونس حسن يوسف، المرجع السابق، ص 188.

⁴ - عادل عبد العال خراشي، المرجع السابق، ص 247.

فالإشكالية المتعلقة في الجرائم الإلكترونية، أن الشخص المطلوب تسليمه قد يرتكب جريمة أو أكثر من الجرائم الإلكترونية، تمس في نفس الوقت مصالح أساسية لأكثر من دولة، ففي هذه الحالة قد تتزاحم طلبات التسليم المقدمة من الدول المتضررة إلى الدولة المطلوب إليها.

وحتى يمكن القول بتزاحم في طلبات التسليم ينبغي أن تقدم الدولة الطالبة الأدلة، التي تثبت قيام الشخص المطلوب بإرتكاب الجريمة مع القيام بإرسالها في الطلب بالفعل، حيث لا تكفي التصريحات الشفوية أو إبداء الرغبة في استلام الشخص.¹

5- عدم وجود نموذج موجود للنشاط الإجرامي

لم تتفق الأنظمة القانونية في دول العالم، على صورة محددة ونماذج معينة يتم الاتفاق المشترك بين الدول حولها تتدرج في إطار الجريمة الإلكترونية، فما يكون مجرما في بعض الأنظمة، قد لا يكون في أخرى، ولعل عدم الاتفاق بين الأنظمة القانونية المختلفة على صور موحدة للسلوك الإجرامي في الجريمة الإلكترونية يغري مجرمو المعلوماتية على إرتكاب جرائمهم دون تقييد بالحدود الجغرافية.²

تمت بحمد الله

¹ - عادل عبد العال، المرجع نفسه، ص 247.

² - صورة بوربابة، التعاون الدولي في مكافحة الجرائم المعلوماتية، مجلة القانون الدولي للدراسات البحثية، العدد 1، 2019، ص 100.

خاتمة

في ختام دراستنا نقول أن الغاية الأساسية للسياسة الجنائية هي حماية المصلحة الاجتماعية في مواجهة مخاطر الظاهرة الإجرامية، ويكون بإتباع نظام فعال للتجريم، ونظام عقابي ملائم، وقانون إجرائي يوفر الضمانات لمحاكمة عادلة، كما يجب أن توافق السياسة الجنائية الوطنية مع نظيرتها الدولية.

وقد تعامل المشرع الجزائري مع المستجدات التي طرحتها الجريمة الإلكترونية، من خلال إنتهاج سياسة تشريعية أهم مظاهرها سن تعديلات سواء على مستوى التجريم، أو تعديل قانون الإجراءات الجزائية بإستحداث أساليب خاصة بالبحث والتحري تتوافق مع خصوصية الجريمة، دون أن ينسى الجانب الوقائي من خلال ما تضمنه القانون 04-09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الذي يحوي نصوصا تجمع بين القواعد الإجرائية المكملة لقانون الإجراءات الجزائية من جهة، والقواعد الوقائية التي تسمح بالترصد المبكر للاعتداءات المحتملة.

و بذلك نخلص لجملة من النتائج والتي تتمثل فيما يلي:

- عدم وجود إتفاق بين فقهاء القانون على مصطلح للدلالة على الجريمة الإلكترونية، مما أدى إلى عدم الإتفاق على إيجاد تعريف موحد لها.
- تتميز الجريمة الإلكترونية بخصائص تجعلها تختلف عن الجرائم التقليدية، وهذه الخصوصية كان لها الأثر في تميز مرتكب الجريمة الذي يطلق عليه المجرم المعلوماتي المتصف بالذكاء والخبرة، ولا يلجأ للعنف عرفت جرائمه بالجرائم الناعمة، يرتكب جريمته بضغطة زر على الحاسوب.
- لا تختلف الجريمة الإلكترونية من حيث الأركان العامة للجريمة التقليدية، إلا أن الإختلاف يكمن في محل الجريمة، الذي هو عبارة عن معلومات وبيانات ذات طابع معنوي لا ترى بالعين المجردة، أو هي عبارة عن ذبذبات كهرومغناطيسية لا يمكن قراءتها إلا عبر الحاسب الآلي، فالركن المادي للجريمة يدخل الوسيلة إعتبارها جزء من النشاط التقني، لأن هذه الوسيلة في حد ذاتها عرضة للسلوك الإجرامي جديد، وضم إلى ذلك النتيجة المحتملة التي تتحقق مع النتيجة التي يريدها الجاني.
- قصور النصوص التقليدية في مواجهة التحديات التي تثيرها الجريمة الإلكترونية، مما سبب في أضرار إقتصادية وإجتماعية ونفسية وعسكرية، لذا كان من الضروري على الدول التدخل عن طريق إبرام إتفاقيات وعقد المؤتمرات من أجل التصدي لهذه الجرائم، وأهم الاتفاقيات المبرمة اتفاقية بودابست التي أرسى قواعد قانونية، بانتهاء سياسة جنائية مشتركة بين جميع الدول لمكافحة الجريمة

الإلكترونية وكانت لها الأثر الكبير في تأثر المشرع الجزائري بهذه الاتفاقية، وكذا بالاتفاقية العربية حيث استقى منها منظومته التشريعية لمكافحة الجريمة الإلكترونية.

- فأول مبادرة قام بها المشرع الجزائري إدراج برامج الحاسب الآلي وقواعد البيانات ضمن المؤلفات التي يحميها القانون بموجب الأمر رقم 03-05 المؤرخ في 2003/07/19 المتعلق بحقوق المؤلف والحقوق المجاورة، وأعتبر هما من القيم المالية المستحدثة مما أضفى حماية جزائية عليها من التقليد.
- انتهج المشرع في سياسته من حيث التجريم والعقاب إلى تعديل قانون العقوبات بموجب القانون رقم 04-15 المؤرخ في 2004/11/10، الذي كان له الأثر الكبير في مواجهة الجريمة الإلكترونية من خلال النص على جرائم المساس بأنظمة المعالجة الآلية للمعطيات من المواد 394 مكرر إلى 394 مكرر 7، بالرغم أن المشرع وفق في تناوله لهذه الجرائم، إلا أنه يعاب عليه عدم تجريمه لبعض الجرائم التي يمكن أن تمس بالنظام المعلوماتي كالإعتراض لنظم المعالجة الآلية للمعطيات، بل اكتفى بالجمع بين فعلي الدخول والبقاء غير المشروعين، على خلاف بعض التشريعات التي نصت عليه بنص خاص، ومن جهة أخرى لم ينص على جريمة إعاقة أو إفساد نظام المعالجة الآلية للمعطيات كجريمة مستقلة وإنما إعتبرها ظرف مشدد لجريمة الدخول أو البقاء غير المصرح بهما، على عكس المشرع الفرنسي الذي تناولها في نص خاص، كذلك لم يتناول جريمة التزوير الإلكتروني التي تعتبر من أهم الجرائم المنتشرة حاليا.
- وسع المشرع من نطاق العقوبة، من خلال تجريم الشروع في جميع الجرائم الماسة بالنظام المعلوماتي وإعتبارها جنح، وذلك أن الشروع لا يقرر إلا في الجنح الخطيرة.
- إقرار المشرع مسؤولية الشخص المعنوي في حالة إرتكابه لهذه الجرائم وشدد من العقوبة المقررة له.
- إقرار المسؤولية الجنائية لمقدمي الخدمة طبقا للمادة 394 مكرر 8 من قانون العقوبات.
- خطورة الجريمة الإلكترونية على الحياة الخاصة للأفراد، ما دعا المشرع إلى بسط حماية جزائية للحق في الخصوصية بموجب المواد 303 مكرر-303 مكرر 3 من قانون العقوبات، إلى جانب إضفاء حماية جزائية لإستغلال الأطفال في المواد الإباحية من خلال تعديل قانون العقوبات لسنة 2014 حيث أضاف المادة 333 مكرر 1، بالإضافة إلى سن نصوصا لتجريم الإرهاب الإلكتروني بموجب المادتان 87 مكرر 11 و 87 مكرر 12 بموجب القانون 06-16.

- واجه المشرع الجريمة الإلكترونية بنصوص خاصة، فأصدر العديد من القوانين هدفها إصباح الحماية الجزائية فسن القانون 04-15 الخاص بالتوقيع والتصديق الإلكترونيين، القانون 04-18 المتعلق القواعد العامة بالبريد والاتصالات الإلكترونية، الذي أكد على سرية المراسلات والاتصالات الإلكترونية، القانون 05-18 المتعلق بالتجارة الإلكترونية الذي أصبح حماية للمستهلك الإلكتروني وكذا الإهتمام بوسائل الدفع الإلكتروني بإعتبارها الوسيلة الفعالة للمعاملات الإلكترونية، إلا أنه لم يدرج نصوص تجريبية في حالة الإعتداء عليها.
- إصباح الحماية الجزائية لبطاقة الشفاء الخاص بالضمان الإجتماعي بموجب القانون 01-08.
- صدور القانون رقم 07-18 المتعلق بحماية الأشخاص الطبيعيين في معالجة المعطيات ذات الطابع الشخصي فنص على الاعتداءات التي تقع عليها.
- أما من الناحية الإجرائية أهم النتائج المستخلصة هي:
- يمكن لأي شخص متضرر من الجريمة الإلكترونية تقديم شكوى أو بلاغ أمام الجهات المختصة إما بالطرق التقليدية، أو عن طريق تقديم الشكاوى والبلاغات عبر المواقع الإلكترونية، سواء على مستوى جهاز الشرطة أو الدرك الوطني، كما يمكن تقديم الشكاوى والعرائض عن بعد وذلك للولوج عبر أرضية تسمى " النيابة الإلكترونية".
- توسيع الإختصاص القضائي لكل من الشرطة القضائية، ووكيل الجمهورية، قاضي التحقيق، بموجب المواد 37 و42 ومن قانون إجراءات جزائية.
- إنشاء هيئة قضائية تختص بالمتابعة والتحقيق والحكم في النظر في الجرائم الإلكترونية تسمى بالقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.
- ولقصور الأساليب التقليدية للبحث والتحري في إثبات ومكافحة الجريمة الإلكترونية، قام المشرع بتعديل قانون الإجراءات الجزائية بموجب القانون 06-22 المؤرخ في 20/12/2006، وسن إجراءات خاصة للبحث والتحري لملاءمتها للطبيعة الخاصة الجريمة الإلكترونية كاعتراض المراسلات وتسجيل الأصوات والنقاط الصور، وكذا عملية التسرب وذلك بموجب المواد من 65 مكرر 5 الى 65 مكرر 18 من قانون إجراءات جزائية.
- إصدار قانون للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بموجب القانون 04-09 المؤرخ في 5/8/2009 و المكمل لقانون العقوبات في مجال الوقاية و مكافحة الجريمة الإلكترونية،

عن طريق إيجاد إجراءات للرصد المبكر للجرائم قبل وقوعها، من أهمها إجراء المراقبة الإلكترونية، كما نظم إجراء التفتيش عن بعد وحجز المعطيات الذي يتلاءم مع الطبيعة الخاصة للجرائم الإلكترونية، وفرض التزامات على مقدمي الخدمات، بتقديم المساعدة للسلطات القضائية المختصة بالبحث والتحري لدورهم الفعال في الكشف عن هذه الجرائم الخطيرة.

- إنشاء هيئة وطنية مهمتها الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، وحدد المرسوم الرئاسي رقم 21-439 إعادة تنظيم الهيئة الوطنية، ونصت على مهامها المادة 14 من القانون 04-09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.
- كما إستحدثت هيئات ووحدات مكلفة بالبحث والتحري عن هذه الجرائم فهناك وحدات تابعة للدرك الوطني، وأخرى تابعة للأمن الوطني التي تعتمد في تكوينها على الطرق العلمية والتكنولوجيا لأفرادها.
- أقر المشرع الجزائري بالإثبات الإلكتروني ومسالة قبوله يخضع لتقدير القاضي الجزائري، الذي يتمتع بدور إيجابي في مناقشة الدليل وموازنة القيمة القانونية له قبل أن يطمئن إليه، كباقي الأدلة الأخرى
- كما إهتم بالتعاون الدولي في مجال مكافحة الجريمة الإلكترونية بإعتبارها عابرة للحدود الوطنية، من خلال الإعتماد على المساعدة القضائية أو الأمنية وتفعيل تسليم المجرمين حتى لا يفلت المجرم المعلوماتي من العقاب عن طريق إبرام الاتفاقيات الثنائية.
- وفي ضوء النتائج المستخلصة من الدراسة يمكن إقتراح بعض التوصيات أهمها:
- ندعو المشرع الجزائري الاسراع إلى الانضمام إلى الإتفاقية المتعلقة بمكافحة الجرائم المعلوماتية إتفاقية بودابست ذات الطابع الدولي.
- ضرورة تشديد العقوبات الخاصة بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، خاصة في مواجهة الأشخاص المنوط بهم التعامل مع هذه الأنظمة، كالموظفين مثلا الذين يملكون صلاحية ذلك.
- إدراج مسؤولية مقدم الخدمات بنص قانوني في حالة أن يكون شريكا في ترويج المواد الإباحية واستغلال الأطفال عبر الأنترنت، مع فرض الرقابة على مقاهي الأنترنت.
- وضع نصوص خاصة تتعلق بحماية جزائية في حالة الإعتداء على وسائل الدفع الإلكتروني بإعتبارها أساس المعاملات التجارة الإلكترونية.

- توفير الوسائل الحديثة في مجال تكنولوجيا الإعلام و الإتصال للسلطات القضائية المكلفة بالبحث والتحري و العمل على تحديثه، إلى جانب تأهيل و تدريب الجهات الأمنية و القضائية في المجال المعلوماتي ، لرفع مستوى الكفاءة و التعاون و التنسيق و الإستعانة بالخبرات و التجارب الأجنبية الناجحة في سبيل مكافحة الجريمة الإلكترونية.
 - ضرورة تكوين متخصصين في مجال مكافحة الجريمة الإلكترونية للكشف السريع لها.
 - تعزيز آليات الوقاية من آفة الجريمة الإلكترونية، وتأمين البرامج وحماية المحتويات تحسبا لتطوير التجارة الإلكترونية في الجزائر.
 - إطلاق حملات للتحسيس عبر وسائل الإعلام بخطورة هذه الجرائم من أجل رفع درجة الوعي الإجتماعي.
 - عقد مؤتمر دولي تحت إشراف الأمم المتحدة، لإبرام إتفاقية شارعة تتضمن إجماع دولي لمكافحة الجرائم الإلكترونية، مع إيجاد قانون جنائي موحد يتجاوز مبدأ سيادة الدولة.
 - ضرورة التأكيد على التعاون الدولي بإعتباره ضرورة حتمية في مجال مكافحة الجريمة الإلكترونية .
- في الأخير نقول أن المشرع الجزائري رغم الترسانة القانونية التي خصها في سياسته الجنائية لمكافحة الجريمة الإلكترونية، ونثنى المجهودات التي قام بها، إلا أنها غير كافية لمواجهة الإجرام المعلوماتي لخصوصية وتميز هذه الأخيرة بالتطور السريع، والقانون لا يتطور بنفس الوتيرة التي تتطور بها التكنولوجيا الحديثة.

قائمة المصادر

والمراجع

قائمة المصادر والمراجع

أولاً: قائمة المصادر

-دستور 2016

-المؤتمرات والإتفاقيات الدولية

- 1- إتفاقية الجريمة المنظمة العابرة للحدود الوطنية الصادرة عن الأمم المتحدة بتاريخ 2000/11/15.
- 2- إتفاقية مكافحة إستعمال تكنولوجيا المعلومات لأغراض إجرامية، رقم 63-55، الصادرة عن هيئة الأمم المتحدة ، الجمعية العامة، 81، ديسمبر 2000.
- 3- إتفاقية بودابست المتعلقة بالجريمة الإلكترونية، المنبثقة عن اجتماع المجلس الأوروبي ببودابست، المجر تحت رقم 185 بتاريخ 23 نوفمبر 2003.
- 4- مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة و العدالة الجنائية، البند الثامن من جدول الأعمال المؤقت، التطورات الأخيرة في إستخدام العلم والتكنولوجيا من جانب المجرمين و السلطات المختصة في مكافحة الجرائم الإلكترونية، المنعقد بالبرازيل 12-19 أبريل 2010، رقم A/conf213/09.

-القوانين

- 1- القانون رقم 89-02 المؤرخ في 07/02/1989 المتعلق بالقواعد العامة لحماية المستهلك، الجريدة الرسمية للجمهورية الجزائرية عدد 06 ن الصادرة بتاريخ 08/02/1989.
- 2- القانون رقم 83 لسنة 2000 المؤرخ في 09/08/2000 ن المتعلق بالمبادلات التجريبية الإلكترونية، الرائد الرسمي للجمهورية التونسية عدد 64 الصادرة بتاريخ 11/08/2000.
- 3- القانون رقم 03-11 المؤرخ في 26/08/2003 المتعلق بالنقد والقرض المعدل والمتمم، الجريدة الرسمية للجمهورية الجزائرية، عدد 52 الصادرة بتاريخ 26/08/2003.
- 4- القانون 04-02 المؤرخ في 23/06/2004 يحدد القواعد المطبقة على الممارسات التجارية، الجريدة الرسمية للجمهورية الجزائرية، عدد 41 الصادرة بتاريخ 27/06/2004.
- 5- القانون رقم 04-15 المؤرخ في 10/11/2004 المعدل و المتمم لقانون الإجراءات الجزائية ، الجريدة الرسمية للجمهورية الجزائرية ، عدد 71 الصادرة بتاريخ 10/11/2004.
- 5- القانون 15-04 المؤرخ في 10/11/2004، المعدل والمتمم للأمر 66/156 المتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، عدد 71 الصادرة بتاريخ 15/11/2004.

- 6- القانون رقم 05-11 المؤرخ في 17/07/2005 المتعلق بالتنظيم القضائي، الجريدة الرسمية للجمهورية الجزائرية، عدد 51 الصادرة بتاريخ 20/07/2005.
- 7- القانون رقم 06-01 المؤرخ في 20/02/2006 المتعلق بالوقاية من الفساد و مكافحته، الجريدة الرسمية للجمهورية الجزائرية، عدد 14 الصادرة بتاريخ 08/03/2006.
- 8- القانون رقم 06-22 المؤرخ في 20/12/2006 المعدل والمتمم للأمر 66-156 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية، عدد 84 الصادرة بتاريخ 20/12/2006.
- 9- القانون رقم 06-23 المؤرخ في 23/12/2006 المعدل والمتمم للأمر 66-156 المؤرخ في 08/06/1966، المتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، عدد 84 الصادرة بتاريخ 24/12/2006.
- 10- القانون رقم 08-01 المؤرخ في 20/01/2008 المعدل و المتمم للقانون رقم 83-11 المؤرخ في 02/07/1983، المتعلق بالتأمينات الإجتماعية، الجريدة الرسمية للجمهورية الجزائرية، عدد 04 الصادرة بتاريخ 27/01/2008.
- 11- القانون رقم 09-01 المؤرخ في 25/02/2009 المعدل والمتمم للأمر رقم 66/156 المؤرخ في 08/06/1966 المتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، عدد 15 الصادرة بتاريخ 08/03/2009.
- 12- القانون 09-03 المؤرخ في 25/02/2009 المتعلق بحماية المستهلك وقمع الغش، الجريدة الرسمية للجمهورية الجزائرية، عدد 15 الصادرة بتاريخ 08/03/2009.
- 13- القانون المغربي رقم 08-09 يتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية، عدد 5711 الصادرة بتاريخ 23/02/2009.
- 14- القانون رقم 10-06 المؤرخ في 15/08/2010 المعدل والمتمم للقانون 04-02 يحدد القواعد المطبقة على الممارسات التجارية، الجريدة الرسمية للجمهورية الجزائرية، عدد 46 الصادرة بتاريخ 18/08/2010.
- 15- القانون رقم 14-01 المؤرخ في 04/02/2014، المعدل و المتمم للأمر 66-156 المتضمن قانون العقوبات ، الجريدة الرسمية للجمهورية الجزائرية، عدد 7 الصادرة بتاريخ 16/02/2014.
- 16- القانون رقم 14-04 المؤرخ في 24/02/2014 المتعلق بالنشاط السمعي البصري، الجريدة الرسمية للجمهورية الجزائرية، عدد 16 الصادرة بتاريخ 16/03/2014.

- 17- القانون رقم 15-04 المؤرخ في 2015/02/01، يحدد القواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين، الجريدة الرسمية للجمهورية الجزائرية، عدد06 الصادرة بتاريخ 2015/02/10.
- 18- القانون رقم 15-06 المؤرخ في 2015/02/15 المعدل والمتمم للقانون رقم 05-01 المؤرخ في 2006/02/06 المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتها.
- 19- القانون رقم 15-12 المؤرخ في 2015//15 المتعلق بحماية الطفل، الجريدة الرسمية للجمهورية الجزائرية، عدد39 الصادرة بتاريخ 2015/07/19.
- 20- القانون رقم 94 المتعلق بمكافحة الإرهاب، الجريدة الرسمية، عدد 33مكرر، الصادرة بتاريخ 2015/08/10.
- 21- القانون 16-01 المؤرخ في 2016/03/06 المتضمن التعديل الدستوري، الجريدة الرسمية للجمهورية الجزائرية، عدد14 ألسادرة بتاريخ 2016/03/07.
- 22- القانون رقم 16-02 المؤرخ في 2016/06/19 المعدل و المتمم للأمر 66-156 المتضمن لقانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، عدد37 الصادرة بتاريخ 2016/06/22.
- 23- القانون رقم 18-04 المؤرخ في 2018/05/10، المعد والمتمم للقانون رقم 200-03 المؤرخ في 2000/08/05، يحدد القواعد العامة المتعلقة بالبريد و الإتصالات الإلكترونية ، الجريدة الرسمية للجمهورية الجزائرية، عدد27، الصادرة بتاريخ 2018/135.
- 24- القانون رقم 18-05 المؤرخ في 2018/05/10، يتعلق بالتجارة الإلكترونية، الجريدة للجمهورية الجزائرية، عدد28، الصادرة بتاريخ 2018/05/16.
- 25- القانون رقم 18-07 المؤرخ في 2018/06/10، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية للجمهورية الجزائرية، عدد34، الصادرة بتاريخ 2018/06/10.
- 26- القانون 18-09 المؤرخ في 2018/06/10 المتعلق بحماية المستهلك وقمع الغش المعدل والمتمم، الجريدة الرسمية للجمهورية الجزائرية، عدد 35، الصادرة بتاريخ 2018/06/13.
- 27- القانون رقم 175-2018 بشأن مكافحة جرائم تقنية المعلومات المصري ، الجريدة الرسمية للجمهورية المصرية، عدد32 مكرر(ج) الصادرة بتاريخ 2018/07/14.

الأوامر

- 1-الأمر رقم 03-05 المؤرخ في 19/07/2003، يتعلق بحقوق المؤلف و الحقوق المجاورة، الجريدة الرسمية للجمهورية الجزائرية، عدد44، الصادرة بتاريخ2003/07/23.
- 2-الأمر رقم 03-07 المؤرخ في 19/07/2003،يتعلق ببراءة الاختراع، الجريدة الرسمية للجمهورية الجزائرية،عدد44، الصادرة بتاريخ 2003/07/23.
- 3-الأمر رقم 03-08 المؤرخ في 19/07/2003، يتعلق بحماية التصميم الشكليه للدوائر المتكاملة، الجريدة الرسمية للجمهورية الجزائرية، عدد 44، الصادرة بتاريخ 2003/07/23.
- 4- الأمر 05-06 المؤرخفي 23/08/2005، يتعلق بمكافحة التهريب، الجريدة الرسمية للجمهورية الجزائرية،عدد55 الصادرة بتاريخ 2005/08/28.

المراسيم

المراسيم الرئاسية

- 1-المرسوم الرئاسي رقم 92-461 المؤرخ في19/12/1992 يتضمن التصديق على إتفاقية الطفل،الجريدة الرسمية للجمهورية الجزائرية، عدد 91 الصادرة بتاريخ 1992.
- 2-المرسوم الرئاسي رقم 97-431 المتضمن إنضمام الجزائر بتحفظ إلى إتفاقية برن لحماية المصنفات الأدبية و الفنية،الجريدة الرسمية للجمهورية الجزائرية، عدد61 الصادرة بتاريخ14/09/1997.
- 3-المرسوم الرئاسي98-413 المؤرخ في 27/12/1998 يتضمن التصديق على الإتفاقية العربية لمكافحة الإرهاب، الجريدة الرسمية للجمهورية الجزائرية عدد 93 الصادرة بتاريخ 09/03/1999.
- 4-المرسوم الرئاسي رقم 04-183 المؤرخ في 26 يونيو2004 المتضمن المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، الجريدة الرسمية للجمهورية الجزائرية، عدد 41 الصادرة بتاريخ 27 يونيو2004.
- 5-المرسوم الرئاسي رقم 06-299 المؤرخ في 02/09/2006 يتضمن التصديق على البرتوكول الإختياري لإتفاقية حقوق الطفل، الجريدة الرسمية للجمهورية الجزائرية، عدد55 ألسادرة بتاريخ 06/09/2006.
- 6-المرسوم الرئاسي رقم 06-299 المؤرخ في 02/09/2006 يتضمن التصديق على البرتوكول الإختياري الملحق بإتفاقية حقوق الطفل المتعلق بشأن بيع الأطفال وإستغلالهم في البغاء وفي المواد الإباحية، الجريدة الرسمية للجمهورية الجزائرية، عدد55 الصادرة بتاريخ 06/09/2006.

- 7- المرسوم الرئاسي رقم 14-252 المؤرخ في 08/09/2014 يتضمن التصديق على الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، الجريدة الرسمية للجمهورية الجزائرية، عدد 57 الصادرة بتاريخ 2014.
- 8- المرسوم الرئاسي رقم 15-261 المؤرخ في 18/10/2015 المحدد لتشكيلة و تنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، عدد 53 الصادرة بتاريخ 08/10/2015.
- 9- المرسوم الرئاسي رقم 19-172 المؤرخ في 06/06/2019 يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال و مكافحتها، الجريدة الرسمية للجمهورية الجزائرية، عدد 37 الصادرة بتاريخ 06/06/2019.
- 10- المرسوم الرئاسي رقم 20-183 المؤرخ في 13/07/2020 يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، عدد 40 الصادرة بتاريخ 18/07/2020.

المراسيم التنفيذية

- 1- المرسوم التنفيذي رقم 98-257 المؤرخ في 25/08/1998 المتعلق بضبط شروط إقامة خدمات الأنترنت وإستغلالها، الجريدة الرسمية للجمهورية الجزائرية، عدد 63 الصادرة بتاريخ 26/08/1998.
- 2- المرسوم التنفيذي رقم 16-267 المؤرخ في 17/10/2016 المتضمن تمديد الإختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، الجريدة الرسمية للجمهورية الجزائرية، عدد 62 الصادرة بتاريخ 23/10/2016.

القرارات الوزارية

- 1- القرار الوزاري المشترك المؤرخ في 17/12/2017 يحدد التنظيم الداخلي لهياكل الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال و مكافحتها، الجريدة الرسمية للجمهورية الجزائرية، عدد 14 الصادرة بتاريخ 04/03/2017.

ثانيا: قائمة المراجع

1- الكتب العامة

- 1- أبو عمرو مصطفى أحمد، الإلتزام بالإعلام في عقود الإستهلاك -دراسة في القانون الفرنسي والتشريعات العربية-، دار الجامعة الجديدة، الإسكندرية، د ط، 2010.
- 2- أحسن بوسقيعة، الوجيز في القانون الجزائري العام، دار هومة، الجزائر، ط3، 2006.

- 3- أحسن بوسقيعة، التحقيق القضائي، دار هومة، الجزائر، دط، 2008.
- 4- أحسن بوسقيعة، الوجيز في القانون الجزائري العام، دار هومة، الجزائر، ط8، 2009.
- 5- أحسن بوسقيعة، الوجيز في القانون الخاص، الجزء الأول، دار هومة، ط17، 2014.
- 6- أحمد إبراهيم، مصطفى سليمان، الإرهاب والجريمة المنظمة، دارالطلائع للنشر والتوزيع، القاهرة، دط، 2006.
- 7- أحمد فتحي سرور، الوسيط في قانون العقوبات، الجزء الأول، القسم الأول، دار النهضة العربية، القاهرة 1981.
- 8- الباشا فايزة يونس، الجريمة المنظمة في ظل الإتفاقيات الدولية والقوانين العربية، دار النهضة العربية، القاهرة د ط، 2002.
- 9- بغدادي مولاي ملياني، الإجراءات الجزائية في التشريع الجزائري، المؤسسة الوطنية للكتاب، الجزائر، د ط، 1992.
- 10- بن عيسى بن كثير، الإجراءات الخاصة المطبقة على الإجرام الخطير، نشرة القضاة، العدد 63، وزارة العدل، الديوان الوطني للاستغلال التربوية، الجزائر، 2008.
- 11- جلال ثروت، قانون العقوبات القسم العام، الدار الجامعية، بيروت، ط1، دس ن.
- 12- جميل عبد الباقي الصغير، قانون العقوبات -القسم الخاص-، دار النهضة العربية، القاهرة، دط، 1998.
- 13- جندي عبد المالك، الموسوعة الجنائية، الجزء 4، مركز الابحاث والدراسات د م ن، دط، 2006.
- 14- خالد لعلاوي، جرائم الصحافة المكتوبة في القانون الجزائري -دراسة قانونية بنظرة إعلامية-، دار بلقيس، الجزائر، دط، 2012.
- 15- سالم روضان الموسمي، فعل الارهاب والجريمة الارهابية، منشورات الحلبي الحقوقية، بيروت، ط1، 2010.
- 16- سامي حارب المنذري، معاينة مسرح الجريمة والحصول على الادلة المادية، موسوعة العلوم الجنائية تقنية الحصول على الادلة المادية- الجزء الأول-، شرطة الشارقة، مركز بحوث الشرطة، ط1، 2007.
- 17- سامي حسين الحسيني، النظرية العامة للتفتيش، دار النهضة العربية، القاهرة، 1972.

- 18-سيد محمد حسن الشريف، النظرية العامة للإثبات الجنائي، دار النهضة العربية، القاهرة، د ط، 2002.
- 19-شريفة هنية، الحقوق المعنوية وحمايتها في القانون الجزائري حق المؤلف، العلامات الرسوم والنماذج الصناعية، براءة الاختراع، دار الجامعة الجديدة، الاسكندرية، دط، 2018.
- 20-عادل عبد العال إبراهيم خراشي، إشكاليات التعاون الدولي وسبل التغلب عليها، دار الجامعة الجديدة، الإسكندرية، د ط، ..
- 21-عبد الرحمان خلفي، محاضرات في القانون الجنائي العام، دار الهدى، الجزائر، ط1، 2012.
- 22-عبد الرحمان خلفي، الإجراءات الجزائية في التشريع الجزائري والمقارن، د د ن، ط3، 2017.
- 23-عبد الرحيم عبد الصادق شكر، جرائم الإرهاب في القانون الجنائي المصري والمقارن، -دراسة موضوعية وإجرائية-، دار النهضة العربية القاهرة، ط1، 2012.
- 24-عبد العزيز توفيق، شرح قانون المسطرة المدنية والتنظيم القضائي، دار النجاح الجديدة، الدار البيضاء، 1995.
- 25-عبد القادر البقيرات، العدالة الجنائية الدولية، ديوان المطبوعات الجماعية، الجزائر، د ط، 2005.
- 26-عبد الله سليمان، شرح قانون العقوبات الجزائري -القسم العام -الجزء الأول -"الجريمة"، ديوان المطبوعات الجامعية، الجزائر، 1995.
- 27-عبد المجيد جباري، دراسات قانونية في المادة الجزائية على ضوء أهم التعديلات الجديدة، دار هومة، الجزائر، ط2، 2013.
- 28-عكاشة محمد عبد العال، الإنابة القضائية في نطاق العلاقات الخاصة الدولية، دار الجامعية، بيروت، 1992.
- 29-عكروم عادل، المنظمة الدولية للشرطة الجنائية والجريمة المنظمة كألية لمكافحة الجريمة المنظمة، دار الجامعة الجديدة، الاسكندرية، دط، 2013.
- 30-علي القهوجي، قانون العقوبات -القسم العام-الدار الجامعة للطباعة، بيروت، دط، 2000.
- 31-عوض محمد عوض، المبادئ العامة في قانون الاجراءات الجنائية، دار الطباعة الجامعية، الاسكندرية، مصر، د ط، 1999.
- 32-غازي الذنبيات، الخبرة الفنية في إثبات التزوير، دار الثقافة، عمان، د ط، 2010.

- 33- فاروق عبد الرحمان مراد، معاينة مسرح الجريمة -الجزء الأول- دار النشر بالمركز العربي للدراسات الامنية والتدريب، الرياض، ط1، 1991.
- 34- مامون محمد سلامة، قانون الإجراءات الجنائية معلقا عليه بالفقه والقضاء، دار الفكر العربي، القاهرة، د ط، 1981.
- 35- محمد أبو العلا عقيدة، مراقبة المحدثات التكنولوجية -دراسة مقارنة-، دار النهضة العربية، القاهرة، ط2، 2008.
- 36- محمد زكي أبو عامر، الإجراءات الجنائية، منشأة المعارف، الاسكندرية، ط2، د س ن.
- 37- محمد صبحي نجم، شرح قانون العقوبات -القسم الخاص- ديوان المطبوعات الجامعية الجزائر، د ط، 2000.
- 38- محمد صبحي نجم، قانون العقوبات -القسم العام- النظرية العامة للجريمة، دار الثقافة للنشر والتوزيع ط4، 2012.
- 39- محمد عبد المطلب، تعريف الإرهاب الدولي بين الإعتبارات السياسية والإعتبارات الموضوعية، دار الجامعة الجديدة، الاسكندرية، ط1، 200.
- 40- محمد علي فارس الزعبي، الحماية القانونية لقواعد البيانات وفقا لقانون حق المؤلف، منشأة المعارف، الاسكندرية، دط، 2003.
- 41- محمد محدة، ضمانات المشتبه فيه اثناء التحريات الدولية-الجزء 2- دار الهدى، الجزائر، ط1، 1991.
- 42- محمد مروان، نظام الإثبات في المواد الجنائية في القانون الوضعي الجزائري، الجزء الثاني، ديوان المطبوعات الجامعية الجزائر، ط1999.
- 43- محمد نجيب حسني، شرح قانون العقوبات -القسم العام- دار النهضة العربية، القاهرة، ط6، 1986.
- 44- محمود محمود مصطفى، الاثبات في المواد الجنائية في القانون المقارن، الجزء الأول، مطبعة جامعة القاهرة، ط2، 1977.
- 45 -محمود نجيب حسن، النظرية العامة للقصد الجنائي -دراسة تأصيلية مقارنة في الجرائم العمدية، دار النهضة العربية، القاهرة، ط2، 1971.
- 46 -محمود نجيب حسني، شرح قانون الإجراءات الجنائية، د د ن، ط2، 1988.

- 47 -مصطفى محمد الدغدي، التحريات والإثبات الجنائي، دار الكتب القانونية، المحلى الكبرى، دط، 2006.
- 48 -معز أحمد محمد الحيارى، الركن المادي في الجريمة، منشورات الحلبي الحقوقية، لبنان، ط1، 2010.
- 49 -منى أبو بكر الصديق، الإلتزام بالإعلام المستهلك عن المنتجات، دار الجامعة الجديدة، دط، د س ن.
- 50 -نادية درادار، الجهود الدولية لمكافحة الجريمة، المركز القومي للإصدارات القانونية، القاهرة، ط1، 2017.
- 51 -نسرین عبد الحمید نبیه، الجرائم الدولية والإنترنت، المكتب الجامعي الحديث، القاهرة، د ط، 2011.
- 52 -نصر الدين مروك، محاضرات في الإثبات الجنائي، النظرية العامة للإثبات الجنائي-الجزء الأول-، دار هومة، الجزائر، 2003.
- 2- الكتب المتخصصة**
- 1-إبراهيم احمد عبد الخالق الدوي، التجارة الالكترونية-دراسة تطبيقية على المكتبات-، مكتبة الملك فهد الوطنية، الرياض، ط2، 2010.
- 2-أحمد حسام طه تمام، الجرائم الناشئة عن إستخدام الحاسب الآلي الحماية الجنائية للحاسب الآلي - دراسة مقارنة-، دار النهضة العربية، القاهرة، دط، 2000.
- 3-أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، الاسكندرية، د ط، 2005.
- 4-أحمد عبد الخالق، التجارة الإلكترونية والعولمة، منشورات المنظمة العربية للتنمية الإدارية، مصر، دط، 2008.
- 5-أحمد عبد اللاه المراغي، الجريمة الإلكترونية ودور القانون الجنائي في الحد منها -دراسة تحليلية تأصيلية مقارنة- المركز القومي للإصدارات القانونية، القاهرة،
- 6-أحمد محمد عبد الرؤوف المنيفي، فيروسات الحاسب الآلي، مكتبة نور، د س ن، دون ترقيم.
- 7- أسامة عبد الله قايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دار النهضة العربية، القاهرة، دط، 1994.

- 8- أشرف عبد القادر قنديل، الإثبات في الجريمة الإلكترونية، دار الجامعة الجديدة، الإسكندرية، دط، 2015.
- 9- آمال بن قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة، الجزائر، ط2، 2007.
- 10- أمير فرج، التوقيع الإلكتروني، دار المطبوعات الجامعية الاسكندرية، دط، 2008.
- 10- أمير فرج يوسف، الجرائم الدولية للإنترنت، المركز القومي للإصدارات القانونية، القاهرة، ط1، 2011.
- 11- إيمان بن سالم، جريمة التجنيد الإلكتروني للإرهاب وفقا لقانون العقوبات الجزائري، المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، برلين ط1 2018.
- 14- أيمن عبد الحفيظ، الإتجاهات الفنية والامنية لمواجهة الجرائم المعلوماتية، مطابع الشرطة، د م ن، د ط، 2005.
- 15- أيمن عبد الله فكري، جرائم نظم المعلومات -دراسة مقارنة- دار الجامعة الجديدة، الاسكندرية، د ط، 2007.
- 16- إيهاب فوزي السقا، جريمة التزوير في المحررات الإلكترونية، دار الجامعة الجديدة، الإسكندرية، دط، 2008.
- 17- بلال أمين زيد الدين، جرائم نظم المعالجة الآلية للبيانات في التشريع المقارن والشريعة الإسلامية، دار الفكر الجامعي، الإسكندرية، ط1، 2008.
- 18- بولين أنطونيوس أيوب، الحماية القانونية للحياة الشخصية في مجال المعلوماتية-دراسة مقارنة-، منشورات الحلبي الحقوقية، ط1، 2009.
- 19- ثرون عبد الحميد، التوقيع الإلكتروني ماهيته، مخاطره وكيفية مواجهتها مدى حجية في الإثبات، دار الجامعة الجديدة، الإسكندرية، د ط، 2007.
- 20- جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، ط1، 1992.
- 21- جميل عبد الباقي الصغير، الأنترنت القانون الجنائي، دار النهضة العربية، القاهرة، د ط، 2012.
- 22- جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالأنترنت، دار النهضة العربية، القاهرة، د س ن.

- 23- حسام محمد عيسى، نقل التكنولوجيا -دراسة من الآليات القانونية للتبعية الدولية، دار المستقبل العربي، القاهرة، د ط، 1987.
- 24- حسن طاهر داود، جرائم نظم المعلومات، أكاديمية نايف العربية للعلوم الأمنية، الرياض، ط1، 2000.
- 25- حسين الغافري، محمد الألفي، جرائم الأنترنت بين الشريعة الإسلامية والقانون دار النهضة العربية، القاهرة، د ط، 2008.
- 26- حسنين المحمدي بوادي، إرهاب الأنترنت الخاطر القادم، دار الفكر الجامعي، الإسكندرية ط1، 2006.
- 27- حسين بن سعيد الغافري، السياسة الجنائية في مواجهة الأنترنت -دراسة مقارنة- دار النهضة العربية، القاهرة، د ط، 2009.
- 28- خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنت، دار الثقافة، عمان، ط1، 2011.
- 30- خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، دار الجامعة الجديدة، الاسكندرية، د ط، 2008.
- 31- خالد ممدوح إبراهيم، أمن المستهلك الإلكتروني، دار الفكر الجامعي، الإسكندرية، ط1، 2008.
- 32- خالد ممدوح إبراهيم، حماية المستهلك في العقد الإلكتروني، دار الفكر الجامعي، الاسكندرية، ط1، 2008.
- 33- خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، الاسكندرية، ط1، 2009.
- 34- خالد ممدوح إبراهيم، فن التحقيق في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية، ط1، 2009.
- 35- خليفة محمد، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الإسكندرية، د ط، 2007.
- 37- رشا مصطفى، الحماية القانونية للكيانات المنطقية، دار الفكر الجامعي، الإسكندرية، د ط، 2006.
- 38- رشاد خالد عمر، المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية -دراسة تحليلية مقارنة-، المكتب الجامعي الحديث، د ط، 2013.

- 39-رشيدة بوكري، جرائم الإعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن منشورات الحلبي الحقوقية، بيروت، ط1، 2012.
- 40-رفد عيادة الهاشمي، الإرهاب الإلكتروني، د د للنشر، د ط، د س ن.
- 41-زيدان زبيحة، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، الجزائر د ط، 2011.
- 42-سالم روضان الموسوي، جرائم القذف والسب عبر القنوات الفضائية-دراسة مقارنة معززة بتطبيقات قانونية، منشورات الحلبي، بيروت، ط1، 2012.
- 43-سامي جلال فقي حسين، التفتيش في الجرائم المعلوماتية-دراسة تحليلية- دار الكتب القانونية-، الإسكندرية، 2011.
- 44-سامي علي حامد عيان، الجريمة المعلوماتية وإجرام الأنترنت، دار الفكر الجامعي، الإسكندرية، دط، 2007.
- 45-سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الأنترنت، دار النهضة العربية، القاهرة، ط1، 1999.
- 46-شمسان ناجي صالح الخيلي، الجرائم المستخدمة بطرق غير مشروعة لشبكة الأنترنت-دراسة مقارنة-، دار النهضة العربية، القاهرة، دط، 2009.
- 47-شيماء عبد الغني محمد عطاء الله، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، الاسكندرية، دط، 2007.
- 48-ضياء علي احمد نعمان، الغش المعلوماتي الظاهرة والتطبيقات سلسلة الدراسات القانونية في المجال المعلوماتي، المطبعة والوراقة الوطنية، مراكش، ط1، 2011.
- 49-طارق عبد الحق، برمجيات الأنترنت الملاحقة والإستكشاف، قصر الكتاب، الجزائر، ط1، 2005.
- 50-عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي-دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية، 2010.
- 52-عادل يحي، السياسة الجنائية في مواجهة الجريمة الإلكترونية، دار النهضة العربية، القاهرة، ط1، 2014.
- 54-عبد الرحمان جلهم حمزة، الأنترنت من منظور شرعي قانوني، ظافر للتصميم والطباعة، بغداد، دط، د س ن .

- 55- عبد الرحمان خلفي، الحماية الجزائية لحقوق المؤلف والحقوق المجاورة، منشورات الحلبي الحقوقية، ط1، 2007.
- 56- عبد الصبور عبد القوي علي المصري، التنظيم القانوني للتجارة الإلكترونية، د د ن، ط1، 2012.
- 57- عبد الصبور عبد القوي علي مصيري، الجريمة الإلكترونية، دار العلوم للنشر والتوزيع، ط1، د س ن.
- 58- عبد العال الديري، محمد صادق إسماعيل، الجرائم الإلكترونية -دراسة قانونية قضائية مقارنة- المركز القومي للإصدارات القانونية، القاهرة، ط1، 2012.
- 59- عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، دار الفكر الجامعي، الاسكندرية، دط، 2004.
- 60- عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجزائية في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، المحلة الكبرى، دط، 2007.
- 60- عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية- دراسة مقارنة- في ضوء الضوابط العامة للإجراءات الجنائية، دار النهضة العربية، القاهرة، ط5، 2009.
- 61- عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت -دراسة معمقة في جرائم الحاسب الالي والانترنت، بهجات للطباعة والتجليد، مصر دط، 2009.
- 62- عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، دار النهضة العربية، القاهرة، ط1، 2009.
- 63- عبد القادر الفنتوخ، الانترنت للمستخدم العربي، مكتبة العبيكان، الرياض، دط، 2000.
- 64- عبد الكريم رشيد توبة، جرائم تكنولوجيا المعلومات، دار المستقبل، ط1، 2008.
- 65- عبد الله عبد الكريم عبد الله، جرائم المعلومات والانترنت (الجرائم الإلكترونية) منشورات الحلبي الحقوقية، بيروت، ط1، 2007.
- 66- عبد الله عبد الكريم عبد الله، الحماية القانونية لحقوق الملكية الفكرية على شبكة الانترنت دراسة في الأطر القانونية للحماية مع شرح النظام القانوني للملكية الفكرية في التشريعات المصرية والأردنية والأوروبية والأمريكية ومعاهد في الانترنت، دار الجامعة الجديدة، الاسكندرية، دط، 2008.

- 67- عبد اللاه أحمد هلال، حجية المخرجات الكمبيوترية في المواد الجنائية -دراسة مقارنة- دار النهضة العربية، القاهرة، ط1، 1999.
- 68- عبد اللاه أحمد هلال، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء إتفاقية بودابست، دار النهضة العربية، القاهرة، ط1، 2003.
- 69- عبد اللاه أحمد هلال، إتفاقية بودابست معلقا عليها، دار النهضة العربية، القاهرة، ط1، 2008.
- 70- عبد اللاه أحمد هلال، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، دار النهضة العربية، القاهرة، ط2، 2008.
- 72- عبد الهادي بن زيطة، حماية برامج الحاسوب في التشريع الجزائري وفقا لأحكام قانون المؤلف الجديد الأمر 03-05، دار الخلدونية، الجزائر، ط1، 2007.
- 73- عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون - دراسة مقارنة-، منشأة المعارف، الاسكندرية، ط1، د س ن.
- 74- علي بن عبد الله عسيري، الآثار الأمنية لإستخدام الشباب للإنترنت، جامعة نايف العربية للعلوم الامنية، الرياض، 2004.
- 75- علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والإنترنت-دراسة مقارنة-عالم الكتب الحديث، عمان، ط1، 2004.
- 76- علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة، الاسكندرية، ط1، 1997.
- 77- علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، المكتبة القانونية، القاهرة، ط1، 1999.
- 78- علي عبود جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الاشخاص والحكومة، منشورات زين الحقوقية بيروت، ط1، 2013.
- 79- علي عدنان الفيل، إجراءات التحري وجمع الادلة والتحقيق الابتدائي في الجريمة المعلوماتية-دراسة مقارنة- المكتب الجامعي الحديث، د ط، 2011.
- 80- علي عدنان الفيل، الإجرام المعلوماتي-دراسة مقارنة-منشورات الحلبي الحقوقية، بيروت ط1، 2011.

- 81- علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة الإلكترونية-دراسة مقارنة-دار الكتاب الجامعي، الإسكندرية، دط، 2009.
- 81- عمر عبد الفتاح، علي يونس، جوانب قانونية للتعاقد الإلكتروني في إطار القانون المدني، دار نشر، ط1، 2009.
- 82- عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الأنترنت، دار النهضة العربية، القاهرة، دط، 2004.
- 83- عمر محمد أبو بكر بن يونس، الإتفاقية الأوروبية حول الجريمة الافتراضية (المذكرة التفسيرية)، مؤسسة ادم للنشر والتوزيع، مالطا، ط2، 2008.
- 84- عيسى غسان ريضي، القواعد الخاصة بالتوقيع الإلكتروني، دار الثقافة، عمان، ط1، 2009.
- 85- غانم مرضي الشمري، الجرائم المعلوماتية ماهيتها، خصائصها كيفية التصدي لها قانونيا، الدار العلمية للنشر والتوزيع، عمان، ط1، 2016.
- 86- غنية باطل، الجريمة الإلكترونية -دراسة مقارنة-الدار الجزائرية، الجزائر، 2015.
- 87- فتحي محمد انور عزت، الحماية الجنائية الموضوعية والإجرائية الإعتداء على المصنفات والحق في الخصوصية والكمبيوتر والأنترنت في نطاق التشريعات الوطنية والتعاون الدولي، دار النهضة العربية، القاهرة، ط1، 2007.
- 88- لينا محمد الأسدي، مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية -دراسة مقارنة-دار حامد للنشر، عمان، ط1، 2015.
- 89- محمد الأمين البشري، التحقيق في الجرائم المستحدثة، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الامنية، الرياض، ط1، 2004.
- 90- محمد امين الشوابكة، جرائم الحاسوب والأنترنت (الجريمة المعلوماتية)، مكتبة دار الثقافة، عمان، ط1، 2004.
- 91- محمد أمين الرومي، جرائم الكمبيوتر والأنترنت، دار المطبوعات الجامعية، عمان، دط، 2004.
- 92- محمد حجازي، الحسابات والأنترنت (الجرائم المعلوماتية)، المركز المصري للملكية الفكرية، 2005.
- 93- محمد حسين منصور، المسؤولية الإلكترونية، دار الجامعة الجديدة، الإسكندرية، د ط، 2003.

- 94-محمد سامي الشوا، ثورة المعلومات وإنعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، دط، د س ن.
- 95-محمد طارق عبد الرؤوف الخن، جريمة الاحتيال عبر الانترنت، الاحكام الموضوعية والاحكام الاجرائية، منشورات الحلبي الحقوقية، بيروت، ط1، 2012.
- 96-محمد عبد الظاهر حسين، المسؤولية القانونية في مجال شبكة الانترنت، د د ن، د ط، 2004.
- 97-محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت -دراسة مقارنة-، دار النهضة العربية، ط2، 2009.
- 98-محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة الإسكندرية، دط، 2004.
- 99-محمد محمد حسن الحسني، حماية المستهلك الإلكتروني في القانون الدولي الخاص، دار النهضة العربية، القاهرة، ط2، 2012.
- 100-محمد محمد شتا، فكرة الحماية الجنائية لبرامج الكمبيوتر، دار الجامعة الجديدة، الاسكندرية، دط، 2001.
- 102-محمود أحمد عابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة، عمان، دط، 2005.
- 103-محمود محمد محمود جابر، الجرائم الناشئة عن استخدام الهواتف النقالة لجرائم نظم الاتصالات والمعلومات، المكتب الجامعي الحديث، الإسكندرية، د ط، 2017.
- 104-مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الالكترونية، دار النهضة العربية، القاهرة، دط، 2001.
- 105-مدحت رمضان، الحماية الجنائية للتجارة الإلكترونية -دراسة مقارنة-، دار النهضة العربية، ط1، 2001.
- 106-مريم محمد ال علي، واقع الجرائم الإلكترونية المتعلقة بالآداب العامة عبر الانترنت-دراسة ميدانية-، مركز البحوث الشارقة، الشارقة، دط، 2009.
- 107-مسعود خثير، الحماية الجنائية لبرامج الكمبيوتر أساليب وثغرات، دار الهدى، الجزائر، 2010.
- 109-مصطفى محمد موسى، اساليب اجرامية بالتقنية الرقمية ماهيتها ومكافحتها، دار الكتب القانونية، مصر، دط، 2005.

- 110-مصطفى محمد موسى، السيرة الذاتية للفيروسات الإلكترونية بين الوقاية والمكافحة والعلاج، دار الكتب القانونية، المحلى، مصر، دط، 2008.
- 111-مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، مطابع الشرطة، القاهرة، ط1، 2009.
- 112-ممدوح خليل بحر، حماية الحياة الخاصة في القانون الجنائي-دراسة مقارنة-، دار النهضة العربية، القاهرة، دط، دس ن.
- 113-ممدوح عبد الحميد عبد المطلب، البحث والتحقيق والجنائي الرقمي في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، المجلة الكبرى، د ط، 2006.
- 114-منير محمد الجنبهي، ممدوح محمد الجنبهي، امن المعلومات الالكترونية، دار الفكر الجامعي، الاسكندرية، 2006.
- 115-منير محمد الجنبهي، ممدوح محمد الجنبهي، جرائم الأنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الاسكندرية، دط، 2006.
- 116-نانة عادل محمد فريد قورة ن جرائم الحاسب الاقتصادية-دراسة نظرية تطبيقية-، دار النهضة العربية، القاهرة، ط1 2004.
- 117-نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، دار الفكر الجامعي، الاسكندرية، ط1، 2007.
- 118-نجاه بن مكي، السياسة الجنائية لمكافحة جرائم المعلوماتية، دار الخلدونية، الجزائر، دط، 2017.
- 119-نسرین عبد الحمید نبیه، الجريمة المعلوماتية والمجرم المعلوماتي، منشأة المعارف، الاسكندرية، دط، 2008.
- 120-نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة، عمان، 2010.
- 121-هدى قشقوش، جرائم الحاسب الالكتروني، دار النهضة العربية، القاهرة، دط، 1992.
- 122-هدى قشقوش، الحماية الجنائية للتجارة الالكترونية عبر الانترنت، دار النهضة العربية، القاهرة، دط، 2000.
- 123-هلال بن محمد بن حارب البورسعيدى، الحماية القانونية والفنية لقواعد المعلومات المحوسبة-دراسة قانونية وفنية مقارنة-، دار النهضة العربية، القاهرة، ط1، 2009.

- 124-وليد الزيدي، القرصنة على الأنترنت والحاسوب، دار اسامة للنشر، عمان، ط1، 2003.
- 125-يوسف حسن يوسف، الجرائم الدولية للأنترنت، المركز القومي للإصدارات القانونية، القاهرة، ط1، 2011.

الأطروحات

- 1-إبراهيم بن سطم بن خلف الغنزي، التوقيع الإلكتروني وحمايته الجنائية، رسالة مقدمة لنيل شهادة دكتوراه، قسم العلوم الشرطية، جامعة نايف للعلوم الأمنية، الرياض، 2009.
- 2-الداودي مجراب، الأساليب الخاصة للبحث والتحري في الجريمة المنظمة، أطروحة لنيل شهادة دكتوراه علوم، كلية الحقوق، جامعة الجزائر 01، 2016.
- 3-الربيع السعدي، حجية التوقيع الإلكتروني في التشريع الجزائري، أطروحة لنيل شهادة دكتوراه علوم، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2016.
- 4-أمنية علالي، الجرائم العابرة للحدود المرتكبة بتقنية الأنترنت، أطروحة لنيل شهادة دكتوراه علوم، كلية الحقوق والعلوم السياسية، جامعة باجي مختار، عنابة، الجزائر، 2018.
- 5-تركي بن عبد الرحمان المويشير، بناء نموذج أمني لمكافحة الجرائم المعلوماتية وقياس فاعليته، أطروحة لنيل شهادة دكتوراه الفلسفة، كلية الدراسات العليا، قسم العلوم الشرطية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2009.
- 6-جمال إبراهيمي، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة لنيل شهادة الدكتوراه في العلوم، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، الجزائر، 2018.
- 7-خديجة مجاهدي، آليات التعاون الدولي لمكافحة الجريمة المنظمة، أطروحة لنيل شهادة دكتوراه علوم، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، الجزائر، 2018.
- 8-خضرة شنتير، الآليات القانونية لمكافحة الجريمة الإلكترونية، أطروحة لنيل شهادة الدكتوراه الطور الثالث (ل.م.د)، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية، ادرار، الجزائر، 2021.
- 9-دلال مولاي ملياني، إشكالية الإثبات في جرائم الأنترنت في التشريع الجزائري، أطروحة لنيل شهادة الدكتوراه في القانون، كلية الحقوق والعلوم السياسية، جامعة أبوبكر بلقايد، تلمسان، الجزائر، 2017-2018.
- 10-رابح لهوي، الشرعية الإجرائية للأدلة المعلوماتية المستمدة من التفتيش، أطروحة لنيل شهادة دكتوراه علوم، كلية الحقوق والعلوم السياسية، جامعة باتنة 01، 2020-2021.

- 11- راضية زرقيني، الحماية الجزائية للمعطيات الشخصية، أطروحة لنيل شهادة دكتوراه علوم، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر، الوادي، 2021-2022.
- 12- رشيدة أكسوم عيلام، المركز القانون للمستهلك الإلكتروني، أطروحة لنيل شهادة الطور الثالث، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2018.
- 13- شريفة سوماتي، السياسة الجنائية للمشرع الجزائري في مواجهة الجريمة المستحدثة، أطروحة لنيل شهادة دكتوراه علوم، كلية الحقوق، جامعة الجزائر 01، 2017-2018.
- 14- عبد العزيز نويري، الحماية الجزائية للحياة الخاصة-دراسة مقارنة-أطروحة لنيل شهادة دكتوراه علوم، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، الجزائر، 2010-2011.
- 15- عبد الوهاب ملياني، أمن المعلومات في بيئة الأعمال الإلكترونية، أطروحة لنيل شهادة الدكتوراه في القانون العام، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، الجزائر، 2016-2017.
- 16- فاتح بهلول، النظام القانوني للتجارة الإلكترونية في ظل التشريع الجزائري، أطروحة لنيل شهادة دكتوراه علوم، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2017.
- 17- فاطمة الزهراء عكو، المسؤولية المدنية لمقدمي الخدمة الوسيطة في الأنترنت، أطروحة لنيل شهادة دكتوراه في القانون، كلية الحقوق، جامعة الجزائر 01، الجزائر، 2014-2015.
- 18- فتيحة حواس، حماية المصنفات الرقمية وأسماء النطاق على شبكة الانترنت، أطروحة لنيل شهادة الدكتوراه في القانون، كلية الحقوق، جامعة الجزائر 01، 2016.
- 19- فيصل بدري، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، أطروحة لنيل شهادة دكتوراه علوم، كلية الحقوق بن يوسف بن خدة جامعة الجزائر 01، 2017-2018.
- 20- محمد التوجي، الحماية الجنائية من الجرائم المرتكبة بواسطة الهاتف النقال، أطروحة لنيل شهادة الدكتوراه، كلية الحقوق والعلوم السياسية، جامعة احمد دراية، ادرار، الجزائر، 2018-2019.
- 21- محمد حبيب عباسي، الجريمة المنظمة العابرة للحدود، أطروحة لنيل شهادة دكتوراه علوم، كلية الحقوق والعلوم السياسية، جامعة ابو بكر بلقايد، تلمسان، 2016-2017.
- 22- محمد خليفة، جريمة التواجد غير المشروع في الانظمة المعلوماتية-دراسة مقارنة-، أطروحة لنيل شهادة دكتوراه، كلية الحقوق، جامعة باجي مختار، عنابة، الجزائر، 2011.
- 23- محمد خميخم، الحماية الجنائية للمستهلك في عقود التجارة الالكترونية، أطروحة لنيل شهادة دكتوراه علوم، كلية الحقوق والعلوم السياسية، جامعة ابي بكر بلقايد، تلمسان، 2017-2018.

- 24- محمد رشاد إبراهيم مفتاح، الحماية الجنائية للحق في حرمة الاتصالات الشخصية، أطروحة لنيل شهادة دكتوراه في الحقوق، جامعة الاسكندرية، 2009.
- 25- مصطفى هنشور وسيمة، النظام القانوني للتجارة الإلكترونية في التشريع الجزائري، أطروحة لنيل شهادة دكتوراه ل.م.د، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس، مستغانم، الجزائر، 2017.
- 26- مليكة بهلول، دور الشرطة العلمية والتقنية في الكشف عن الجريمة، أطروحة لنيل شهادة دكتوراه علوم، كلية الحقوق، جامعة الجزائر 01، الجزائر، 2013.
- 27- منيرة بن جدو، الحماية الجنائية لتعاملات التجارة الإلكترونية، أطروحة لنيل شهادة دكتوراه في الطور الثالث، كلية الحقوق والعلوم السياسية، جامعة محمد لمين دباغين، سطيف 2، 2021-2022.
- 28- نبيلة هبة هروال، جرائم الأنترنت -دراسة مقارنة-، أطروحة لنيل شهادة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة ابي بكر بلقايد، تلمسان، 2013-2014.
- 29- نعيم سعيدي، الحماية النائية للحق في الخصوصية في مجال المعلوماتية، كلية الحقوق والعلوم السياسية، جامعة الحج لخضر، باتنة، 2020-2021.
- 30- يزيد بوحليط، السياسة الجنائية في مجال مكافحة الجرائم الإلكترونية في الجزائر، أطروحة لنيل شهادة دكتوراه علوم، كلية الحقوق، جامعة باجي مختار، عنابة، 2016.

رسائل الماجستير

- 1- أسامة بن بطو، حماية برامج الحاسب الآلي بين نظامي حقوق المؤلف وبراءة الاختراع، مذكرة لنيل شهادة الماجستير في الحقوق، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2015.
- 2- راضية لالوش، من التوقيع الإلكتروني، مذكرة لنيل شهادة الماجستير في القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2012.
- 3- زكريا لدغم شيكوش، النظام القانوني للتسرب في القانون الجزائري، مذكرة لنيل شهادة الماجستير في العلوم القانونية والادارية، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، 2013.
- 4- سليمان غازي العتيجي، درجة توافر كفايات البحث والدليل الرقمي في الجرائم المعلوماتية لدى ضباط شرطة العاصمة المقدسة، رسالة لنيل شهادة ماجستير في العلوم الشرطية، كلية الدراسات العليا، قسم العلوم الشرطية، جامعة نايف للعلوم الأمنية، الرياض، 2010.

- 5- سليمان مهج الغنزي، وسائل التحقيق في جرائم نظم المعلومات، رسالة لنيل شهادة الماجستير في العلوم الشرطية، كلية الدراسات العليا، أكاديمية نايف العربية للعلوم الامنية، الرياض، 2003.
- 6- عالية بوياح، دور الانترنت في مجال التسويق، مذكرة لنيل شهادة الماجستير، جامعة منتوري، قسنطينة، 2010-2011.
- 7- عبد الله دغش العجمي، المشكلات العملية والقانونية للجرائم الإلكترونية -دراسة مقارنة-رسالة لنيل الماجستير في القانون، جامعة الشرق الأوسط، 2014.
- 8- عبد المالك بن ذياب، حق الخصوصية في التشريع العقابي الجزائري، مذكرة لنيل شهادة الماجستير في العلوم القانونية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2013.
- 9- فتيحة رصاع، الحماية الجنائية للمعلومات على شبكة الأنترنت، مذكرة لنيل شهادة الماجستير، كلية الحقوق والعلوم السياسية، جامعة ابي بكر بلقايد، تلمسان، الجزائر، 2011-2012.
- 10- محمد بن نصير محمد السرحاني، مهارات التحقيق الجنائي الفني في جرائم الحاسوب والانترنت -دراسة مسيحية- على ضباط الشرطة بالمنطقة الشرقية، رسالة لنيل شهادة الماجستير.
- 11- مريم أحمد مسعود، آليات مكافحة جرائم تكنولوجيا الإعلام والاتصال في ضوء القانون رقم 04-09، مذكرة لنيل شهادة الماجستير، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، 2013.
- 12- نداء نائل فايز المصري، خصوصية الجرائم المعلوماتية، مذكرة لنيل شهادة الماجستير في الحقوق، كلية الدراسات العليا، جامعة النجاح، نابلس، فلسطين، 2017.
- 13- نسيم دردور، جرائم المعلوماتية على ضوء القانون الجزائري والمقارن، مذكرة لنيل شهادة الماجستير في الحقوق، كلية الحقوق والعلوم السياسية، جامعة قسنطينة، 2012-2013.
- 14- نسيم جدي، جرائم المساس بأنظمة المعالجة الآلية للمعطيات، مذكرة لنيل شهادة الماجستير في الحقوق، كلية الحقوق، جامعة وهران، الجزائر، 2013-2014.
- 15- نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة لنيل شهادة الماجستير في العلوم القانونية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، الجزائر.
- 16- يوسف صغير، الجريمة المرتكبة عبر الأنترنت، مذكرة لنيل شهادة الماجستير في القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، الجزائر، 2013.

- 1- أحلام بوكربوعة، آليات الإتحاد الإفريقي للتعاون الشرطي "أفريبول" ودورها في مكافحة ظاهرة الإرهاب، حوليات الجزائر، 1، المجلد 34، العدد 04، ديسمبر 2020.
- 02- أحمد أسامة حسينة، الجريمة الإلكترونية بين الشرعية الجنائية الإجرائية، مجلة جامعة الأزهر، غزة، المجلد 19، عدد خاص بمؤتمر كلية الحقوق الخامس المحكم، 2017.
- 03- أحمد بن خليفة، حفوطة عبد القادر، الجريمة الإلكترونية واليات التصدي لها، مجلة الإمتياز لبحوث والادارة، المجلد 01، العدد 01، 2017.
- 04- أحمد بن مالك، أثر الاثبات بالأدلة العلمية الحديثة على الاقتناع الشخصي للقاضي الجزائري بها، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد 10، العدد 01، 2021.
- 05- أحمد غلاب، زهية كيسي، إجراءات إعتراض المكالمات السلكية واللاسلكية كالية لمتابعة جرائم المخدرات، مجلة تحولات، جامعة ورقلة، المجلد الثاني، العدد الأول، يناير 2019.
- 06- إسمهان بوضياف، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الاستاذ الباحث للدراسات القانونية والسياسية، العدد الحادي عشر، سبتمبر 2018.
- 07- إلهام خرشي، النظام القانوني للهيئة الوطنية للوقاية منالجرائم المتصلة بتكنولوجيا الإعلام والاتصال، مجلة البحوث القانونية والسياسية، المجلد 04، عدد 01، 2022.
- 07- الزهرة جقريف، التوقيع الالكتروني، مجلة الدراسات القانونية، المجلد 1، العدد 3، ديسمبر 2017.
- 08- الطيبي البركة، إشكالية الإثبات في الجرائم الإلكترونية، مجلة افاق علمية، المجلد 11، العدد 01، 2019.
- 09- أمال مشتي، التجارة الالكترونية في الجزائر، مجلة البحوث والدراسات القانونية والسياسية، العدد 03، 2017.
- 10- أمينة معزير، التسرب في قانون الإجراءات الجزائية الجزائري، مجلة القانون والمجتمع، المجلد 3، العدد 1، د س ن.
- 11- أمينة بن عميور، إلهام بوحلايس، القطب الجزائري الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، مجلة البحوث في العقود وقانون الأعمال، المجلد 07، عدد 01، 2022.
- 12- انسام سمير طاهر الحجامي، جريمتي القذف والسب عن طريق الأنترنت، مجلة رسالة الحقوق، العدد 02، 2015.

- 13- بدره عمارة، فتحة عمارة، الحماية الجنائية للمعلومات الإلكترونية في إطار قانون الملكية الفكرية، مجلة الحقيقة، المجلد 13، العدد 4، ديسمبر 2014.
- 14- بوراس بودالية، واقع التجارة الإلكترونية في الجزائر، مجلة البصائر للدراسات القانونية والاقتصادية، المجلد 01، عدد 01، 2021.
- 15- جمال الدين بوقرة، جمال الدين عنان، القطب الجزائري الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، مجلة الأستاذ الباحث للعلوم القانونية والسياسية، المجلد 07، عدد 01، 2022.
- 16- جاسم خريبط خلف، التفتيش في الجرائم المعلوماتية، مجلة الخليج العربي، المجلد 41، العدد 3-4، 2013.
- 17- جميلة محلق، إعتراض المراسلات، تسجيل الاصوات والتقاط الصور في قانون الاجراءات الجزائية الجزائري، مجلة التواصل في الاقتصاد والادارة والقانون، عدد 42، جوان 2015.
- 18- جورج لبكي، المعاهدات الدولية للانترنت حقائق وتحديات، مجلة الدفاع الوطني اللبناني، عدد 83، بيروت، 2014.
- 19- حسين جفالي، الطاهر دلول، الحماية الجنائية للمستهلك من الإشهار الإلكتروني غير المرغوب فيه في التشريع الجزائري، المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد 02، العدد 04، د س ن .
- 20- حسين جفالي، الحماية الجنائية لحق المستهلك الإلكتروني في الاعلام في التشريع الجزائري، المجلة الاكاديمية للبحوث القانونية والسياسية، المجلد الثالث، العدد الأول، 2019.
- 21- حسين ربيعي، المراقبة الإلكترونية وحقوق الفرد في الخصوصية داخل الفضاء الرقمي، المجلة الاكاديمية للبحث القانوني، المجلد 13، العدد 01، 2016.
- 22- حفيظ نقادي، أساليب البحث والتحري الخاصة، المجلة الجزائرية للعلوم القانونية والسياسية، المجلد 5، عدد 4، د س ن.
- 23- حكيم تبينة، اليات الضبط الاداري لحماية المعطيات ذات الطابع الشخصي في التشريع الجزائري، المجلة الجزائرية للعلوم القانونية والسياسية المجلد 58، العدد 01، 2021.
- 24- حنان مناصرية، الحماية القانونية لبرامج الحاسب الالي بين التشريع الجزائري والاتفاقيات الدولية، مجلة الباحث للدراسات الاكاديمية، المجلد 06، عدد 01، 2019.
- 25- خالد بن سامي، واقع التجارة الإلكترونية والإمداد في الجزائر، مجلة أداء المؤسسات الجزائرية، العدد 12، 2017.

- 26-خديجة خالدي، آلية الاتحاد الإفريقي للتعاون الشرطي "افريبول" مجلة العلوم الاجتماعية والانسانية، العدد15، 2018.
- 27- دلال مولاي ملياني، شهادة الشهود في جرائم تكنولوجيا الإعلام والاتصال، مجلة البحوث القانونية والسياسية، عدد 06، 2016.
- 28-دنيا زاد ثابت، مراقبة الإتصالات الإلكترونية الحق في حرمة الحياة الخاصة في القانون الجزائري، مجلة العلوم الاجتماعية والسياسية، المجلد5، العدد1، 2014.
- 29-رابح نهائي، دور المنظمات الدولية في مكافحة الجريمة المنظمة(منظمة الامم المتحدة، المنظمة الدولية للشرطة الجنائية نموذجاً)، مجلة البحوث القانونية والاقتصادية، المجلد04، العدد02، 2021.
- 30-راضية مشري، الحماية الجزائية للمصنفات الرقمية في ظل قانون حق المؤلف، مجلة التواصل في العلوم الانسانية والاجتماعية، عدد34، جوان 2013.
- 31-رامي حليم، جرائم الاعتداء على أنظمة المعالجة الآلية للمعلومات، مجلة دراسات وابحاث، كلية الحقوق والعلوم السياسية، جامعة زياني عاشور، الجلفة، العدد01، 2009.
- 32-رشا خليل عيد، جرائم الاستغلال الجنسي لأطفال عبر الانترنت، مجلة الفتح، العدد27، 2006.
- 33-رضا هميسي، تفتيش المنظومات المعلوماتية في القانون الجزائري، مجلة العلوم القانونية والسياسية، عدد5، جوان 2012.
- 34-سامية آية مولود، الضمانات المقررة لمشروعية اعتراض المراسلات وتسجيل الاصوات والنقاط الصور في الجرائم الاقتصادية، المجلة النقدية، المجلد10، عدد2، ديسمبر 2015.
- 35-سامية بلجراف، سلطة القاضي الجزائي في قبول وتقدير الدليل الرقمي، مجلة الدراسات القانونية المقارنة، المجلد07، العدد01، 2021.
- 36-سامية عبد الرزاق خلف، جريمة اختراق أنظمة المعلومات -دراسة مقارنة-مجلة كلية القانون، جامعة البصرة، د ت ن.
- 37-سعيد سالم المزروعى، عبد الرحمان عزمان، اجراءات التحقيق في جرائم تقنية المعلومات وفقا للتشريع الاماراتي، مجلة العلوم الاقتصادية والادارية والقانونية، المجلد الثاني، العدد الثالث عشر، اكتوبر. 2018.
- 38-سفيان كعرار، الآليات المؤسسية الاوربية لمكافحة الجريمة المنظمة عبر الوطن، المجلة الاكاديمية للبحوث القانونية والسياسية، المجلد الرابع، العدد الأول، 2020.

- 39-سمير بارة، الدفاع الوطني والسياسات الوطنية للأمن السيبراني في الجزائر، الدور والتحديات، المجلة الجزائرية للأمن الانساني، عدد2، 2017.
- 40-سمير شعبان، الجريمة الإلكترونية -مقاربة تحليلية لتحديد مفهوم الجريمة والمجرم، مجلة دراسات وأبحاث، المجلد1، عدد1، سبتمبر 2009.
- 41-سميرة معاشي، الجريمة المعلوماتية دراسة تحليلية لمفهوم الجريمة المعلوماتية، مجلة المفكر، العدد السابع عشر، جوان2018.
- 42-شريعة كلاع، ظاهرة تجنيد الشباب في الجماعات الارهابية من خلال استخدام شبكات التواصل الاجتماعي، مجلة مدرات سياسية، المجلد2، العدد6، 2018.
- 43- شريعة سوماتي، القطب الجزائري الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال كآلية جديدة ضمن الجهاز القضائي المتخصص، مجلة الدراسات القانوني، المجلد08، عدد02، 2022.
- 44-صورية بورابة، التعاون الدولي في مكافحة الجرائم المعلوماتية، مجلة القانون الدولي للدراسات البحثية، العدد الأول، 2019.
- 45-عائشة بن قارة مصطفى، اليات حماية المعطيات ذات الطابع الشخصي في التشريع الجزائري وفقا لاحكام القانون رقم 18-07، مجلة العلوم القانونية والسياسية، المجلد10، العدد1، افريل 2019.
- 46-عادل بوزيدة، دور الشهادة الالكترونية في الاثبات الجزائي على ضوء قانون الاجراءات الجزائية الجزائري، النبراس للدراسات القانونية، المجلد الأول، العدد الأول، سبتمبر2016.
- 47-عادل بوزيدة، الاطار القانوني لمكافحة جريمة الاساءة لرئيس الجمهورية عبر المواقع الالكترونية في التشريع الجزائري، اسم المجلة، العدد06جوان 2016.
- 48-عادل عبد الله خميس المعمري، التفتيش في الجرائم المعلوماتية، الفكر الشرطي، المجلد22، العدد56، 2013.
- 49-عبد الرحمان خلفي، الحق في الحياة الخاصة في التشريع العقابي الجزائري، مجلة البحوث والدراسات، العدد12، 2011.
- 50-عبد الرزاق احمد الشيبان، إجراءات الخبرة القضائية ودورها في الإثبات، مجلة كلية القانون للعلوم القانونية والسياسية، د ع، د س ن.
- 51-عبد المالك صاولي، تشريعات الجريمة الإلكترونية في البيئة الإعلامية العالمية، مجلة الحقوق والعلوم السياسية، العدد 10، جوان 2018.

- 52- عبد الهادي الكحلوي، عبد الهادي بن زيطة، آليات حماية المعطيات ذات الطابع الشخصي في ظل القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، مجلة القانون والعلوم السياسية، المجلد 07، عدد 02، 2021.
- 53- عثمان طارق، حماية الأطفال من الإستغلال الجنسي في المواد الإباحية عبر الانترنت في التشريع الجزائري، مجلة المفكر، المجلد 11، عدد 1، فيفيري 2016.
- 54- عيدة بلعابد، الدليل الرقمي بين حتمية الإثبات الجنائي والحق في الخصوصية المعلوماتية، مجلة افاق علمية، المجلد 11، العدد 01، 2019.
- 55- عز الدين طباش، الحماية الجزائية للمعطيات الشخصية في التشريع الجزائري-دراسة في ظل قانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في معالجة ذات الطابع الشخصي، المجلة الاكاديمية للباحث القانوني، العدد 02، 2018.
- 56- عز الدين وداعي، التسرب كأسلوب من أساليب البحث والتحري الخاصة على ضوء قانون الاجراءات الجزائية والمقارن، المجلة الاكاديمية للبحث القانوني، المجلد 16، عدد 02، 2017.
- 57- عزيزة لرقط، الحماية الجنائية للتوقيع الإلكتروني التصديق الإلكتروني في التشريع الجزائري، مجلة الاجتهاد للدراسات القانونية والاقتصادية، العدد 11، 2017.
- 58- عمر طه خليل، عفاف بديع جميل، التكييف الفقهي والقانوني لجرائم الانترنت، مجلة كلية التراث الجامعة، العدد السابع عشر، د س ن.
- 59- فاطمة الزهراء عربوز، التفتيش الإلكتروني كاجراء للتحقيق في الجرائم المعلوماتية، مجلة جيل الابحاث القانونية المعمقة، مركز جيل الابحاث العلمي، العدد 34، جويلية 2019.
- 60- فتح الله لفقير، كريمة كريم، الحماية الجزائية لقانون الملكية الفكرية للمصنف الالكتروني في بيئة الانترنت ومدى استفادة المصنف الصحفي من هذه الحماية، مجلة الصورة والاتصال، العدد 22، فبراير 2018.
- 61- فوزي عمارة، اعتراض المراسلات وتسجيل الاصوات والتقاط الصور والتسرب كاجراءات تحقيق قضائي في المواد الجزائية، مجلة العلوم الانسانية، عدد 33، جوان 2010.
- 62- لورانس سعيد الحوامدة، الجرائم المعلوماتية أركانها وآلية مكافحتها-دراسة تحليلية مقارنة-مجلة الميزان للدراسات الاسلامية والقانونية، المجلد الرابع، العدد الأول، 2017.

- 63- ليندا شرايشة، السياسة الدولية والإقليمية في مجال مكافحة الجريمة الإلكترونية الاتجاهات الدولية في مكافحة الجريمة الإلكترونية، مجلة دراسات وأبحاث، المجلد 1، عدد 1، سبتمبر 2009.
- 64- مبارك بن الطيبي، محمد رحموني، شروط قبول الدليل الرقمي كدليل إثبات في الجريمة الإلكترونية، مجلة القانون والعلوم السياسية، المجلد 05، العدد 02، 2019.
- 65- محمد أحمد عيسى، حماية حقوق الملكية الفكرية للمصنفات الرقمية في ظل القانون الدولي، مجلة جامعة الملك عبد العزيز، عدد 7، 2002.
- 66- محمد السعيد زناتي، الجريمة الإلكترونية في ظل التشريع الجزائري والاتفاقيات الدولية، مجلة اليزي للبحوث والدراسات، العدد 2، 2017.
- 67- محمد الطاهر عديلة، استخدام مواقع التواصل الاجتماعي في عمليات التجنيد الإرهابي قراءة في الآليات، المضمون وسبل الوقاية، مجلة الاستاذ الباحث القانونية والسياسية، المجلد 1، العدد 01، سبتمبر 2017.
- 68- محمد أمين الخرشة، إبراهيم سليمان القطاونة، الحماية الجنائية لحرمة الحياة الخاصة في قانون العقوبات الاماراتي، جامعة الشارقة للعلوم الشرعية والقانونية، المجلد 13، العدد 1، 2016.
- 69- محمد بن فردية، الدليل الجنائي الرقمي وحجتيه أمام القضاء الجزائري-دراسة مقارنة- المجلة الأكاديمية للباحث القانوني، المجلد 5، العدد 2، 2014.
- 70- محمد بعجي، التزامات مقدمي الخدمة عبر الأنترنت، مجلة الاستاذ الباحث للدراسات القانونية والسياسية، المجلد 4، العدد 1، 2019.
- 71- محمد بوكبسة، المنظمة الدولية الشرطة الجنائية ودورها في مكافحة الجرائم، مجلة القانون، العدد 09، ديسمبر 2017.
- 72- محمد حماد مرهج الهيتي، نطاق الحماية الجنائية للمصنفات الرقمية-دراسة مقارنة بين القوانين العربية لحماية حق المؤلف، مجلة الشريعة والقانون، جامعة الإمارات العربية، العدد 48، أكتوبر 2011.
- 73- محمد خليفة، دراسة نقدية لنصوص جرائم أنظمة المعالجة الآلية للمعطيات في قانون العقوبات الجزائري، المجلة النقدية، المجلد 13، عدد 1، جوان 2018.
- 74- محمد رحموني، منظمة الشرطة الجنائية الدولية (الأنتربول) آلية لمكافحة الجريمة المنظمة، مجلة افاق علمية، المجلد 11، العدد 04، 2019.

- 75-مشتاق طالب وهيب، مفهوم الجريمة الالكترونية ودور الحاسوب بارتكابها مجلة العلوم القانونية والسياسية، كلية القانون والعلوم السياسية، جامعة دالي العراق المجلد الثالث، العدد الأول، 2014.
- 76-مريم خليفي، الحماية الجنائية لمواقع التجارة الإلكترونية عبرالأنترنت، مجلة العلوم القانونية، عدد02، جانفي2011.
- 77-مريم خليفي، الالتزام بالإعلام الإلكتروني وشفافية التعامل في مجال التجارة الالكترونية، مجلة دفاتر السياسة والقانون، العدد04، جانفي2011.
- 78-مريم لوكال، الآليات القانونية المستحدثة لحماية الشهود والخبراء الضحايا بموجب الأمر 15-02 المعدل والمتمم لقانون الإجراءات الجزائية -دراسة مقارنة-، مجلة حوليات الجزائر1، الجزء الثاني، المجلد31، عدد2، جوان 2017.
- 79-مريم لوكال، الحماية القانونية الدولية والوطنية للمعطيات ذات الطابع الشخصي في الفضاء الرقمي في ضوء قانون حماية المعطيات رقم 07/18، مجلة العلوم القانونية والسياسية، المجلد 31، العدد01، أبريل 2019.
- 80-مفيدة مباركية، الحماية الجنائية للحق في الخصوصية الرقمية في القانون الجزائري، مجلة الشريعة والاقتصاد، المجلد السابع، العدد13، جوان 2018.
- 81-نادية ضريفي، عبد الوهاب دراج، سلطات القاضي الجنائي في تقدير الدليل الإلكتروني المستمد من التفتيش الجنائي، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد04، العدد02، 2019.
- 82-ناصر حمودي، الحماية الجنائية لنظم المعالجة الآلية للمعطيات في التشريع الجزائري، المجلة الأكاديمية للبحث القانوني، المجلد 14، العدد2، 2016.
- 83-نبيل محمد احمد صبيح، حماية المستهلك في التعاملات الإلكترونية، مجلة الحقوق، جامعة الكويت، العدد02، جوان 2008.
- 84-نبيلة هبة هروال، ماهية جرائم الأنترنت، مجلة المعيار، المجلد03، العدد05، جوان2012.
- 85-نجا عبوي، الحماية الجزائية لبطاقة الشفاء الإلكترونية، مجلة الحقيقة، العدد41، 2017.
- 86-نجية شيخ، اساليب البحث والتحري المستخدمة في القانون رقم22/06 المعدل والمتمم لقانون الاجراءات الجزائية الجزائري، المجلة النقدية، المجلد8، عدد01، جوان2013.
- 87-نجية شيخ، اجراء التسرب في القانون الجزائري وسيلة لمكافحة الجرائم المستحدثة، مجلة المعارف، العدد22، ديسمبر2018.

- 88-نزيمه مكاري، وسائل الاثبات في جرائم الإعتداء على حق المؤلف عبر الانترنت، مجلة المناهج القانونية، العدد13-14.
- 89-نسرين مشتة، إخلاص بن عبيد، الحماية القانونية للمعطيات الشخصية في ظل القانون 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، المجلة الجزائرية للحقوق والعلوم السياسية، المجلد 6، العدد01، 2021.
- 90-نصير بن تركية، إستغلال الطفل في المواد الإباحية ما بين الحظر الدولي والتجريم الوطني المجلة الجزائرية للحقوق والعلوم السياسية، العدد4، ديسمبر2017.
- 91-نعيمه إزديري، التفتيش في الجرائم الإلكترونية، مجلة المتوسط للدراسات القانونية والقضائية، العدد4، 2014.
- 93-نور الدين بن حميدوش، مكانة الدليل الإلكتروني في الإثبات الجزائي، مجلة الدراسات والبحوث القانونية، المجلد04، العدد02، جانفي2020.
- 94-نور الدين محرز، نظام الدفع الإلكتروني ودوره في تفعيل التجارة الإلكترونية مع الاشارة لحالة الجزائر، مجلة الاقتصاد الجديد، العدد02، جانفي2010.
- 95-نور الهدى محمودي، حجية الدليل الرقمي في اثبات الجريمة المعلوماتية، مجلة الباحث للدراسات الاكاديمية، العدد11، جوان 2017.
- 96-وردة شرف الدين، مجالات المساعدة القضائية الدولية المتبادلة فيما يخص جمع جميع الادلة الرقمية وفقا للاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة2010، مجلة العلوم السياسية والقانون، المجلد3، العدد15، ماي2019.
- 97-ياسمينه بونعارة، الجريمة الالكترونية، مجلة المعيار، كلية اصول الدين، جامعة الامير عبد القادر للعلوم الاسلامية، قسنطينة، العدد 39، جوان 2005.
- 98-ياسين جبيري، الحماية الجنائية للتصديق والتوقيع الإلكتروني-دراسة مقارنة-، مجلة جامعة الأمير عبد القادر الإسلامية، العدد01، 2008.
- 99-يحي الشديدي، الشهادة في الجريمة الإلكترونية، مجلة البعث، المجلد38، العدد50، 2016.
- 100-يحي تومي، الحماية القانونية، للمعطيات ذات الطابع الشخصي على ضوء القانون رقم07/18 دراسة تحليلية، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 4، العدد2، 2019.

101- بليمان يمينه، الإشهار الكاذب والمضلل، مجلة العلوم الانسانية، المجلد ب، عدد32، ديسمبر.2009

102-يوسف مسعودي، النظام القانوني لحماية المصنفات الرقمية، مجلة الدراسات القانونية عدد4، 2009.

103-يوسف شويفر، التسرب كألية للتحري والتحقيق والإثبات، مجلة المستقبل، مدرسة الشرطة سيدي بلعباس، عدد01، 2007.

المؤتمرات والملتقيات والندوات

01-آمنة محمدي بوزينة، إجراءات التحري الخاصة في مجال الجرائم المعلوماتية-دراسة تحليلية لأحكام قانون الاجراءات الجزائية وقانون الوقاية من الجرائم الإعلام، ورقة علمية مقدمة في إطار الملتقى الوطني حول اليات مكافحة الجرائم الالكترونية في التشريع الجزائري، مركز جيل البحث العلمي، الجزائر، المنعقد في 2017/03/29.

03-أمين أعزان، الجريمة المعلوماتية، ورقة علمية قدمت للمؤتمر العلمي المغاربي حول المعلوماتية والقانون، اكااديمية الدراسات العليا، طرابلس، ليبيا، المنعقد في الفترة من 2009/10/29/28.

04-ايسر محمد عطية، دور الآليات الحديثة للحد من الجرائم المستحدثة الارهاب الالكتروني وطرق مواجهته، ورقة علمية مقدمة الملتقى العلمي حول الجرائم المستحدثة في ظل التغيرات والتحولات الاقليمية والدولية، كلية العلوم الإستراتيجية، المنعقد في الفترة بين 2014/11/9-7.

05-جان فرانسوا هاروت، أهمية التعاون الدولي والتجربة البلجيكية في تبادل المعلومات بين عناصر الشرطة والتعاون القضائي، ورقة علمية مقدمة في اطار الندوة الاقليمية حول الجرائم المتصلة بالكمبيوتر ضمن برنامج تعزيز حكم القانون في بعض الدول العربية" مشروع تحديات النيابة العامة" المملكة المغربية، المنعقد بين 2007/06/20-19.

06-ذياب موسى البداينة، الجرائم الالكترونية المفهوم والاسباب، ورقة علمية مقدمة في اطار الملتقى العلمي الجرائم المستحدثة في ظل التغيرات والتحولات الاقليمية والدولية، كلية العلوم الاستراتيجية الاردن المنعقد خلال الفترة من 2014./09/4-2

07-رحاب عميش، الجرائم المعلوماتية، بحث مقدم إلى المؤتمر الأول حول المعلوماتية والقانون، اكااديمية الدراسات العليا، طرابلس، ليبيا، المنعقد في الفترة بين 2009/10/29-28.

- 08-رحيمة نمديلي، خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة، ورقة علمية مقدمة في اطار اعمال المؤتمر الدولي الرابع عشر للجرائم الالكترونية، المنعقد في طرابلس، لبنان، الفترة 24-25 مارس 2017.
- 09-رضا هميسي، أحكام الشاهد في الجريمة المعلوماتية، ورقة علمية مقدمة في إطار المؤتمر الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، مخبر الحقوق والحريات في الانظمة المقارنة، كلية الحقوق، جامعة بسكرة، المنعقد بين 16-17/11/2015.
- 10-زوليخة بلعطار، مديحة بن عميرش، اليات حماية المستهلك الالكتروني من مخاطر الاحتيال والاختراق، ورقة علمية مقدمة في اطار الملتقى الوطني الثالث حول المستهلك والاقتصاد الرقمي، المركز الجامعي عبد الحفيظ بوصوف، ميلة، المنعقد بين 23-24/04/2018.
- 11-صالح شتين، الحماية الجنائية للمصنفات الرقمية في اطار قانون حق المؤلف الجزائري ورقة علمية مقدمة لملتقى الملكية الفكرية بين مقتضيات العولمة وتحديات التنمية، كلية الحقوق والعلوم السياسية، جامعة بجاية، المنعقد يومي 28-29/04/2013.
- 12-عبد الرحمان اللمتوني، الإجرام المعلوماتي بين ثبات النص وتطور الجريمة، سلسلة ندوات محكمة الاستئناف بالرباط، العدد 7، 2017.
- 13-عبد الرحمان حملاوي، دور المديرية العامة للامن الوطني في مكافحة الجريمة الالكترونية ورقة علمية مقدمة في اطار الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة مخبر الحقوق والحريات في الانظمة المقارنة، كلية الحقوق، جامعة بسكرة، المنعقد بين 16-17/11/2015.
- 14-عبد المؤمن بن صغير، الطبيعة الخاصة للجريمة المرتكبة عبر الانترنت في التشريع الجزائري المقارن، بحث مقدم في اطار الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة المنعقد في الفترة 16-17 نوفمبر 2015، كلية الحقوق، جامعة بسكرة، الجزائر.
- 15-عبد الناصر محمد محمود فرغلي، محمد عبيد سيف المسماري، الاثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية-دراسة تطبيقية مقارنة- ورقة علمية مقدمة في اطار المؤتمر العربي الأول لعلوم الادلة الجنائية والطب الشرعي، الرياض، المنعقد بين 12-14/11/2007.
- 16-فاروق خلف، الاليات القانونية لمكافحة الجريمة المعلوماتية، ورقة علمية مقدمة في إطار الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، مخبر الحقوق والحريات في الانظمة المقارنة، جامعة بسكرة، المنعقد بين 16 و17/11/2015.

- 17-فضيلة عاقل، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، ورقة علمية مقدمة في إطار المؤتمر الدولي الرابع عشر حول الجرائم الإلكترونية، طرابلس، لبنان المنعقد بين 24-25 مارس 2017.
- 18-محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي والأنترنت، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت، المجلد الثاني، جامعة الإمارات العربية المتحدة، ابوظبي، 2000.
- 19-موسى مسعود أرحومة، الإشكاليات التي تنبثها الجريمة المعلوماتية عبر الوطنية، ورقة علمية مقدمة في إطار المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، لبنان، المنعقد بين 28-29/10/20.
- 20-ما شائ الله الزوي، المواجهة الجنائية للبريد الإلكتروني الدعائي المزعج أو المضلل، ورقة علمية مقدمة في إطار المؤتمر الدولي الرابع للجرائم الإلكترونية، مركز جيل البحث العلمي، طرابلس، المنعقد بين 24-25 مارس 2017.
- 21-نسمة بطيحي، الجرائم المتعلقة بانتهاك الأحكام الإجرائية المقررة لحماية الحق في الخصوصية الرقمية في التشريع الجزائري، ورقة علمية مقدمة في إطار الملتقى الدولي حول الخصوصية في مجتمع المعلوماتية، مركز جيل الباحث العلمي، طرابلس، لبنان، المنعقد بين 19 و20/07/2019.
- 22-هارون بحرية، دور الدليل الرقمي في إثبات الجريمة المعلوماتية في التشريع الجزائري، ورقة علمية مقدمة في إطار الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، مخبر الحقوق والحريات في الأنظمة المقارنة، كلية الحقوق، جامعة بسكرة، المنعقد بين 16-17/11/2015.
- 23-هشام ملاطي، خصوصية القواعد الإجرائية المعلوماتية، محاولة المقاربة مدى ملائمة القانون الوطني مع المعايير الدولية، سلسلة ندوات محكمة الاستئناف بالرباط، العدد السابع، 2014.
- 22-يونس عرب، جرائم الكمبيوتر والأنترنت، ورقة مقدمة لمؤتمر الأمن العربي، مركز العربي للدراسات والبحوث الجنائية، المنعقد يومي 10-12/02/2002.

مواقع الأنترنت

- 01-محمد عبد الله المنشاوي، جرائم الانترنت من منظور شرعي وقانوني، د س ن
www.minshawi.com
- 02-محمد علي قطب، الجرائم المعلوماتية ومواجهتها الجزء الثاني، الأكاديمية الملكية للشرطة، وزارة الداخلية، البحرين منشور على موقع www.policemv.crim.bh/reports.

- 03-وزارة الاتصالات وتقنية المعلومات، تقرير الجرائم الالكترونية تكبد الاقتصاد العالمي خسائر بقيمة 445 مليار دولار سنويا منشور على الموقع www.gov.mcit.gov.sa/news.
- 04-مقال بعنوان هل المجتمع الدولي بحاجة إلى تشريع جديد بخصوص الجرائم السيبرانية، جريدة العين الاخبارية منشور على الموقع al-ain.com.article.united-mat..
- 05-مركز معلومات G8 متاح على الموقع الالكتروني <http://www.cybercrime-law.net/G8.html>.
- 06-قرار اعتماد قانون الإمارات العربي الإسترشادي لمكافحة جرائم تقنية المعلومات متاح على الموقع الالكتروني <http://arabic.justice.dz/ligue-arabe/loi-emur-ar-crintech-inf.pdf>.
- 07-تقرير الانترنت حول الجريمة الإلكترونية في افريقيا منشور على الموقع www.interpol.int/or/1/11/2020/36.
- 08-محمد صغري، شرح جريمة السب في القانون الجزائري، الموسوعة الجزائرية للدراسات السياسية والاستراتيجية، منشور على الموقع الالكتروني <http://www.politis-dz.com>.
- 09-عبد الرحمان بن عبد الله السند، وسائل الارهاب الالكتروني حكمها وطرق مكافحتها مقال منشور على الموقع الالكتروني السكينة الالكترونية [www.assikima.com\(fils\)books/book8pdf](http://www.assikima.com(fils)books/book8pdf)
- 10-غادة الحلايقة، بحث حول تكنولوجيا الإعلام والاتصال، منشور على الموقع <https://mawdoo3.com>
- 11-طوني عيسى، حماية برامج الكمبيوتر وقواعد البيانات بحث منشور على الموقع <http://www.lipa-ib.org/my-file/it-ens-file-computer-2program.pdf>.
- 12-حسين بن سعيد الغافري، الجرائم الواقعة على التجارة الإلكترونية، منشور على الموقع <http://www.eastlaw.com>.
- 13-فادي سالم، مقال بعنوان موقعك في ويب، في مهب الاختراق منشور على الموقع <http://www.ahewar.org/debat/show>.
- 14-نضال ياسين الحاج حمو، دور الدليل الالكتروني في الاثبات الجنائي-دراسة تحليلية-مجلة جامعة تكريت للعلوم القانونية والسياسية، المجلد 1، العدد 19، 2013 منشور على الموقع www.iasji.net.iasj-article.

- 15- ميسون خلف حمد الحمداني، مشروعية الأدلة الإلكترونية في الإثبات الجنائي، مجلة كلية الحقوق، المجلد 18، العدد 2، كانون الثاني، جامعة النهرين منشور على الموقع <http://www.mlaw.nahrain.org/issue.php> ?-58.
- 16- علي حسن الطوالة، مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي -دراسة مقارنة- مركز الاعلام الامني منشور على الموقع www.policenc.gov.bh.
- 17- حسين بن سعيد الغافري، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الانترنت بحث منشور على الموقع <http://www.eastlaws.com>.
- 18- حكيمة ذهبي، خبراء يشرحون أسباب التغيرات التي طرأت على الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، مقال منشور على الموقع <http://m.elbilad.net/art...>
- 19- الموقع الرسمي للمنظمة الدولية للشرطة الجنائية (الإنترپول) www.interpol.intr/or.
- 20- مقال بعنوان هامل يدعو إلى شراكة عملياتيه بين أفريبول وأوروبول، منشور على الموقع algerie.dz/news/ar/article/2018.
- 21- مقال بعنوان إرضية النيابة الإلكترونية e-nyaba منشور على الموقع www.mjjustice.dz/ar/...

المراجع بالفرنسية

Les ouvrages en français

- 1- Ali azzouzi, la cybercriminalité au Maroc, bishoop solution ,casablanca,maroc, 1^{er} édition, 2010.
- 2- Caprioli eric, règlement des litiges internationaux et droit applicable dans le commerce électronique ,édition, du juris-classeur, litec, paris 2002.
- 3- Faral –schuhl chritiane, cyber droit ,le droit à l'épreuve de l'internet, 3e édition, Dunod, paris, 2002.
- 4- John arquí, David ronfledt, networks and netware, the future of terror ,crime and militany, usa, rand publication, 2001.
- 5- kayser ,la protection de la vie privée par le droit du secret de la vie privée, puam, paris ,2009.
- 6- Myriam quémener, Joël ferry, cybercriminalité, défi mondial, 2em édition , economica, paris, 2009.
- 7- Myriam quémener Yves, la cybercriminalité, édition, economica, paris, France, 2010.

- 8- Pierre Catala, les transformations de droit par l'informatique, émergences du droit de l'information, 1983.
- 9- Rose Phillippe, la criminalité informatique, que sais-je, 1^{er} édition, puf, 1988.
- 10- Sieber Ulrich, the international handbook on computer crime computer related economic crime and the infringement privacy, 1986.
- 11- Tafforeau Patrick, droit de la propriété intellectuelle, 2^{em} édition, édition gualino, France, 2007.

-les thèses

- 12- Boos Romain, la lutte contre la cybercriminalité au regard de l'action des états, thèse de doctorat de droit privé et sciences criminelles, université de Lorraine, France, 2017.
- 13- Ibrahim Coulibaly, la protection des données à caractère personnel dans le domaine de recherche scientifique, thèse de doctorant, université de Grenoble, 2011.

Master

- 14- Emmanuelle Matignon, la cybercriminalité un focus dans le monde des télécoms, mémoire de master en droit numérique administrations, école de droit de Sorbonne université, Paris 1, 2011-2012.

Revue

- 15- Bainbridge David, hacking the unauthorized access of computer system, the legal implication, ML, rev 1989, vol 52
- 16- Mohrenschlager (Manfred), computer crimes and other crimes against information technology in Germany, R.I.D.P, 1993..
- 17- Jacques Francillon, les crimes informatiques et d'autres crimes dans le domaine de la technologie informatique en France, rev.int.pen, 1990, vol 64.
- 18- Olivier Decima, les investigations numériques en procédure pénale française du piratage informatique aux réquisitions et sais numériques ? revue la faculté de droit, n°1, 2017.
- 19- Harvé Bonnard, la répression de la criminalité, J.C.P, cahiers de droit de l'entreprise, 2002, n°4.
- 20- Mohamed Bouzabar, la criminalité informatique sur internet, journal law, n°20, 2002.
- 21- Michael D. Roster, Robert H. Rines, computer jurisprudence legal responses to the information revolution, New York, N.Y: Oceana publication, 1986.
- 22- Philippe Richard, droit de l'extradition de terrorisme risques d'une pratique incertaine: du droit vers le non droit, AFDI, vol 34, 1988.

Site

- 23- cass.crim 27 octobre 2009, disponible en ligne à l'adresse suivante:[http://www.globe-net.org/FMG/cour de cassation full disclosure criminelle, chambre criminelle](http://www.globe-net.org/FMG/cour-de-cassation-full-disclosure-criminelle-chambre-criminelle),27 octobre 2009.
- 24- convention sur la criminalité (boudapest 2001)disponible sur le site:[http://www.europol.eu/meets docs/19/2/2014/documents /libre/du 7conv budapest7/cov budapestfr.pdf](http://www.europol.eu/meets-docs/19/2/2014/documents-libre/du-7conv-budapest7/cov-budapestfr.pdf)
- 25- Lerbrun(M) et M boutcha (e),évolution de la responsabilité des intermédiaires technique en Italie, in [http://www.juriscom.net/variations/responsabilité des intermédiaires. technique en Italie](http://www.juriscom.net/variations/responsabilite-des-intermediaires-technique-en-italie) ,atrul.
- 26- Mohamed chawki ,essai sur la cybercriminalité ,site ichei.org ,2006.
- 27- M.robert Del piccha, rapport de la loi autorisant l'approbation de convention sur la criminalité et du protocole additionnel à cette convention relatif à l'incrimination d'actes de nature raciste et xénophole commis par le biais de système informatique sénat, session ordinaire de2004-2005,annexe au procès verbale de la séance du 4 mai 2005,sp. Publier sur le site [www.senat .fr](http://www.senat.fr)

Projet

- 28- Devez(J), les qualifications pénales applicables au fraudes informatique, acte du viii de IAFDP,Grenoble28-30 novembre 1985,economica,1986.
- 29- Philippe Guillot et Daniel ventre, capacités d'interception et surveillance ,projet utic, université paris8,vincennes-saint Denis, paris ,France,2017.

Loi

- 30- loi n°88-19,5janv.1988, relative à la fraude informatique,jo6janv
- 31- Rap j .thyrand doc, sénat 1987,n°3.

قنفود نبيهة

السياسة الجنائية في مكافحة الجريمة الإلكترونية في التشريع الجزائري

أطروحة لنيل شهادة الدكتوراه ل م د
شعبة الحقوق، تخصص: قانون العقوبات والعلوم الجنائية

الملخص

إن التقدم التكنولوجي المذهل الذي شهدته البشرية في الآونة الأخيرة، أدى إلى ظهور ما يعرف بالجريمة الإلكترونية، ذات الطبيعة الخاصة والمعقدة التي تثير العديد من الإشكاليات سواء من ناحية اكتشافها أو صعوبة إثباتها، وتبعاً لذلك تطلب الأمر جهوداً لمكافحتها .

لقد واكب المشرع الجزائري التشريعات الدولية في مواجهة الجريمة الإلكترونية، وذلك بانتهاج سياسة جنائية متكاملة، من خلا إرساء تدابير مستحدثة، فمن الناحية الموضوعية سن قواعد قانونية متضمنة التجريم والعقاب خاصة في مجال المساس بأنظمة المعالجة الآلية للمعطيات، الحق في الخصوصية، استغلال الأطفال في الإباحية... إلخ، باعتبار عدم كفاية الإجراءات التقليدية في مكافحة الجريمة الإلكترونية بادر المشرع بإقرار إجراءات مستحدثة ملائمة لكشف خبايا هذه الجريمة، بعد التعديلات الماسة بقانون الإجراءات الجزائية كإجراء أساليب التحري الخاصة، إنشاء قطب جزائي متخصص، و نتيجة لخطورة هذه الجريمة أصدر قانون يختص بالوقاية منها قبل وقوعها و يتمثل في القانون 04-09 المتعلق بالقواعد الخاصة للوقاية الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وأقر المراقبة الإلكترونية والتفتيش عن بعد، وإنشاء هيئة وطنية مختصة بمكافحتها و الوقاية منها.

الكلمات المفتاحية: الجريمة الإلكترونية، السياسة الجنائية، المشرع الجزائري، التجريم والعقاب، إجراءات مستحدثة، الهيئة الوطنية.

الأستاذ المشرف: فوزي عمارة جامعة قسنطينة 1 الإخوة منتوري

السنة الدراسية: 2025/2024

