وزارة التعليم العالي و البحث العلمي
جامعة منتـــوري (قسنطينـــة)
كليـــة الحقـــوق

مذكرة لنيل شهادة الماجستيـــر
شعبة : القانون الجنائـــي

تحـــت عنـــوان :

جرائم المعلوماتية على ضوء القانون الجزائري و المقارن

إعداد الطالب :
دردور نسيـــم

تحت إشراف :
الأستـــاذ الدكتـــور طاشـــور عبد الحفيـــظ

أعضـــاء لجنـــة المناقشـــة :

الأستاذ الدكتور مالكي محمد الأخضر	أستاذ التعليم العالي	جامعة قسنطينة	رئيس
الأستاذ الدكتور رحماني منصور	أستاذ التعليم العالي	جامعة سكيكدة	عضو
الأستاذ الدكتور طاشور عبد الحفيظ	أستاذ التعليم العالي	جامعة قسنطينة	مشرف

السنة الجامعية 2013/2012

الشكـــــر

أتقدم بأحر الشكر و التقدير و الإحترام أولا إلى أستاذي و المشرف على عملي، الأستاذ الدكتور : طاشور عبد الحفيظ، كما أشكره على كل النصائح و التوجيهات العلمية الهامة التي أنرني بها طوال مدة إعدادي لهذه المذكرة المتواضعة، و كذا كلية حقوق قسنطينة و أعضاء المجلس العلمي كلهم بدون إستثناء و أخيرا أتقدم بأحر الشكر إلى كلا من الأستاذ الدكتور مالكي محمد الخضر أستاذ التعليم العالي بجامعة قسنطينة رئيس لجنة المناقشة و كذا الأستاذ رحماني منصور أستاذ التعليم العالي بجامعة سكيكدة عضو في لجنة المناقشة على موافقتهم على مناقشة المذكرة المقدمة للفحص.

الإهـــــداء

" إلـــى أبـــي فيصل، أمـــي الزهرة، أخواتـــي نجلاء و نسرين، و جدي زروق "

" بسم الله الرحمن الرحيم "

مـــقـــدمـــة

مقدمـــــــة

تسري حاليا في العالم ثورة تكنولوجية، و هذه الثورة تمس بصفة خاصة تكنولوجيات الإعلام و الإتصال (المعلوماتية و وسائل الإتصال الحديثة).

هذه التغيرات أدت إلى خلق مصطلح جديد تحت تسمية الإجرام المعلوماتي "***La criminalité informatique***"، بحيث الجريمة تقع على المعلومـــة [1] بمعناها المعلوماتي (معطيات "***Données***"، برامج "***Programmes***" و ما له من وجود منطقي "***Logique***" في النظام المعلوماتي)، أي معالجتها، نشرها و إستعمالها الغير مشروع.

أولا : أهمية الموضوع

حسب ما جاء في وثيقة المعلومات رقم 6 تحت عنوان : الإجرام المعلوماتي "***Délinquance informatique***"[2]، و هو الموضوع الذي كان محل دراسة من طرف اللجنة الثانية التي تم تشكيلها و في جلستها التاسعة مساءا يوم 22 أفريل 2005[3]، و هذا في إطار المؤتمر الحادي عشر للأمم المتحدة ***(O.N.U)*** حول : الوقاية من الجريمة و العدالة الجنائية "***La prévention du crime et la justice pénale***" أيام 18 إلى 25 أفريل 2005 ببنكوك (تايلاند)[4]، فإنه من الصعب فهم جيدا أين يبدأ الإجرام المرتبط بالمعلوماتية و أين ينتهي ما دام أن مجال المعلوماتية في تطور مستمر وسريع بالمقارنة بمختلف التشريعات العقابية في هذا المجال، أي تحديد بدقة أصناف الجرائم المرتبطة بتقنية المعلوماتية، لذلك تبرز أهمية هذا الموضوع في عرض بطريقة واضحة، منظمة و مبسطة، أولا : المفاهيم و العناصر الأساسية التي تدور حول الإجرام المعلوماتي ، و ثانيا : محاولة تحديد أهم أنواع هذه الجرائم التي ظهرت إلى حد الآن في التشريع الجزائري و المقارن.

ثانيا : أسباب إختيار الموضوع

يعود سبب إختيارنا لهذا الموضوع لكونه حديث تزامن مع التطور التكنولوجي لوسائل الإتصال و الإعلام هذا من جهة و من جهة أخرى نظرا لكونه من بين الجرائم الأكثر تعقيد خاصة في ما يخص إشكالية إتيان الأدلة المؤدية إلى إدانة المتهم أو تبرئته و أن الدليل في مثل هذه الجرائم في أغلب الأحيان دليل ذات طبيعة خاصة أي ذات طبيعة إلكترونية بالنظر إلى المحيط الذي ترتكب فيه الجريمة المعلوماتية و كذا في ما يخص التكييف

---

(1)_ أساس الجريمة المعلوماتية هي "المعلومة" و التصرفات المجرمة قانونا التي يمكن أن تقع عليها أو بواسطتها و التي قد تمس بمال الغير أو بالأشخاص و الحريات.

(2)_ لمزيد من المعلومات حول التقرير الصحافي لنتائج المؤتمر بشأن الإجرام المعلوماتي أنظر : **الملحق رقم 1**

(3)_ أنظر : **الملحق رقم 2**

(4)_ هذا يبين أن الجريمة المعلوماتية بمختلف أنواعها أصبحت ذات أهمية و طابع عالمي.

الصحيح لكل تصرف في مجال المعلوماتية الذي جرمه القانون و الذي كان غالبا من خلال نصوصه القانونية غامضا نوعا ما، أيضا إختيارنا لهذا الموضوع لم يأتي صدفة بل قمنا بإختياره نظرا لإهتمامنا الكبير بمجال المعلوماتية من الناحية التقنية مما دفع بنا إلى دراسة الجانب القانوني العقابي كقانونيين في الأصل.

ثالثا : الدراسات السابقة للموضوع

أهم الدراسات في مجال الإجرام المعلوماتي إلى يومنا هذا هي دراسات أجنبية بإعتبار أن الرصيد التشريع العقابي في هذا المجال في الدول الأجنبية ثري و أسبق بالمقارنة مع التشريع الوطني في حين أن الكتابات الوطنية لم تقتصر فقط إلا في الدراسات الجامعية بحوث ماجستير و دكتوراه و مقالات في مجلات علمية و لكنها قليلة بالمقارنة بالرصيد العلمي القانوني في هذا المجال.

رابعا : التعريف القانوني للجريمة المعلوماتية

المشرع الفرنسي لم يضع تعريف قانوني واضح و شامل للجريمة المعلوماتية بل تولى هذه المهمة رجال الفقه، في حين أن المشرع الجزائري و على خلاف المشرع الفرنسي فلم يضع تعريف لها إلا مؤخرا من خلال المادة 2 فقرة 1 من القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق لـــ 5 أوت 2009 المتضمن : "القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها" و الذي دخل حيز النفاذ بموجب الجريدة الرسمية/العدد 47 الصادرة بتاريخ 16 أوت 2009[1] و تجدر الإشارة إلى أن التعريف الذي ورد في هذا القانون جاء حسب رأينا عاما و خالي من أي دقة تقنية حيث إكتفى المشرع بتعريفها على أنها كل الجرائم سواء المتعلقة بالمساس بالأنظمة أو غيرها من الجرائم الأخرى التي ترتكب أو يسهل إرتكابها بإستعمال منظومة معلوماتية أو أي نوع آخر من نظم الإتصال الإلكتروني حسب مضمون المادة 2 فقرة 1 من القانون السالف الذكر، و بالتالي لن نتوقف بدورنا في هذا الحد بل سنتعمق أكثر في دراسة تعريف هذا النوع الخاص من الجرائم في نظر مختلف فقهاء القانون بعد تحديد المصطلحات القانونية التقنية المرتبطة بها.

أ- تحديد المصطلحات

قبل التطرق إلى تعريف الجريمة المعلوماتية كان لابد علينا من تحديد أولا المصطلحات التي يمكن إستعمالها للتعبير عن هذه الجريمة المستحدثة، و تجدر الإشارة إلى أن هنالك إختلاف كبير بشأن هذه المصطلحات المستخدمة للدلالة على الظاهرة الجرمية الناشئة في بيئة الكمبيوتر و الشبكات المعلوماتية، و هو إختلاف رافق مسيرة نشأة و تطور ظاهرة الإجرام المتصل بتقنية المعلوماتية، ومن بين أهم هذه المصطلحات : مصطلح

---

[1] _ أنظر : **ملحق رقم 2**

الجرائم المعلوماتية ***"Les crimes ou infractions informatiques"***، جرائم الكمبيوتر ***"Les crimes d'ordinateur"***، جرائم التقنية العالية ***"Les crimes de la haute technologie"***، جرائم الهاكرز ***"Les crimes de hackers"***، جرائم الأنترنت ***"Les crimes d'Internet"***، الإجرام في الفضاء الخيالي ***"La criminalité dans le cyber espace"***، الجرائم عبر شبكات الإتصال عن بعد [1] ***"Les crimes à travers les réseaux de télécommunications"***، أو أيضا ما يسمى بالسيبر كرايم ***"Cyber crime"*** بالغة الأنجليزية و بالغة الفرنسية ***"La cyber criminalité"***، كل هذه المصطلحات تدل على الجرائم المعلوماتية المرتكبة إما في محيط معلوماتي مغلق أو مفتوح على الشبكات المعلوماتية[2].

ب- محاولة وضع تعريف للجريمة المعلوماتية

في ما يخص تعريف الجريمة المعلوماتية، فلقد أعطى الفقهاء عدد لا بأس به من التعاريف التي تتباين حسب نوع الجريمة المرتبطة بالمعلوماتية سواء إرتكبت في مجال معلوماتي مغلق أو مفتوح على الشبكات المعلوماتية، إذ أنه إلى حد الآن لا يوجد تعريف ثابت، جامع و متكامل متفق عليه :

و بالتالي يمكن أن نعرف بدورنا الجريمة المعلوماتية بأنها "كل عمل أو إمتناع عن عمل [3] غير مشروع يتم بواسطة كمبيوتر أو أي جهاز معالجة آلية للمعطيات المعلوماتية سواء كان الجهاز أداة لإرتكاب الجريمة [4] أو محل لإرتكاب الجريمة[5] في مجال إلكتروني أو معلوماتي مغلق أو مفتوح على الشبكات المعلوماتية أو محيط لإرتكاب الجريمة، و التي يجب أن تتوافر لدى فاعلها الأصلي المعرفة الكافية لإرتكابها".

خامسا : خصوصيات الجريمة المعلوماتية من الناحية النظرية و العملية

هنا يمكن أن نعرض جملة من الخصائص ذات أهمية لا مثيل لها في الجرائم الأخرى و التي تعبر جيدا عن وضع التشريع العقابي في هذا المجال [6]، إلا أنه يمكن أن نقول و نؤكد بأن هذه الخصوصيات قابلة للتغير و

---

(1)_ و بما فيها : الشبكات المعلوماتية ***"Les réseaux informatiques"*** (السلكية ***"Réseaux électronique ou informatique par câble"*** أو اللا سلكية ***"Réseau électronique ou informatique sans fil"***).

(2)_ أنظر المستند **(WORD)** (يونس عرب، تحت عنوان : **جرائم الكمبيوتر والانترنت المعنى والخصائص والصور و إستراتيجية المواجهة القانونية**، أكتوبر 2006، المركز الوطني للتوثيق: قاعدة المعطيات حول التنمية الاقتصادية والاجتماعية – المركز المتعدد الوسائط) المستنسخ Téléchargé من صفحة الأنترنت التالية : www.doc.abhatoo.net.ma/IMG/doc/dro5.doc (de la page 1 à 6 du document)

(3)_ مثال ذلك : إمتناع الطبيب عن تجهيز و تشغيل برنامج الآلة لمعالجة مريض و الذي نتيجة لذلك الإمتناع يتعرض لضرر أو الموت.

(4)_ مثال ذلك : جريمة إرسال بواسطة الحاسب الآلي الفيروسات المعلوماتية عبر الشبكات المعلوماتية إضرار بأنظمة الغير.

(5)_ مثال ذلك : حالة الموظف الذي يفسد عمدا السير العادي للنظام المعلوماتي التابع للجهة أو الإدارة التي يعمل بها.

(6)_ من خلال دراستنا للموضوع لاحظنا أنه رغم التطور السريع للجانب التشريعي و القضائي الفرنسي في مجال الإجرام المعلوماتي على الجزائري إلا أنه يمكن أن نؤكد بأن خصائص هذا النوع من الجرائم بقي نفسه في الدولتين و كذا الدول الأوروبية الأخرى لسبب الصعوبات التي تحيط بهذا الموضوع وهو ما سنلاحظه من خلال دراستنا خصوصيات الجريمة المعلوماتية.

هذا من خلال تطور الجانب التشريعي (أي التقنين العقابي) بالإضافة إلى الممارسة القضائية (الإجتهادات القضائية)، و كذا التكوين التقني الكافي لأعوان الشرطة العلمية في هذا المجال.

أ- القوانين المتعلقة بجرائم المعلوماتية حديثة

لم يظهر أول نص قانوني في مجال جرائم المعلوماتية (جرائم المساس بأنظمة المعالجة الآلية للمعطيات) إلا سنة 1988 في فرنسا [1]، حيث أنه إلى غاية هذا التاريخ لم يكن يتمتع أي من الدولتين (الجزائر و فرنسا) بتشريع عقابي في هذا المجال[2].

في البداية لم يكن يعتبر الكمبيوتر كأداة يمكن بواسطتها إرتكاب الجرائم، بل كان يعتبر أداة في خدمة مختلف الإدارات كما تسمح بتخزين جل المعلومات المرتبطة بحياة المواطن لا أكثر.

و تجدر الإشارة إلى أنه قبل صدور قانون 1988 الفرنسي (قانون رقم 88-19 لـــ 5 جانفي 1988 الصادر بالجريدة الرسمية لـــ 6 جانفي 1988 المتعلق بالغش المعلوماتي، الفصل الثالث من قانون العقوبات الفرنسي تحت عنوان : ببعض الجرائم في مجال المعلوماتية) [3]، سبقه قانون آخر وضعه البرلمان الفرنسي و هو القانون رقم 78-17 المؤرخ في 6 جانفي 1978 و المتعلق بالمعلوماتية، المعطيات و الحريات و الذي عدل 10 مرات[4]، كما تجدر الإشارة إلى أن آخر تعديل كان بموجب القانون رقم 2009-526 المؤرخ في 12 ماي 2009 الذي دخل حيز النفاذ في 13 ماي 2009 لتوفير حماية أفضل للأشخاص الطبيعية من المعالجات للمعطيات ذات طابع شخصي أي المعطيات الإسمية ***"Fichiers nominatifs"*** [5]، و وردت العقوبات الجزائية في حالة مخالفة مقتضيات هذا القانون في قانون العقوبات الفرنسي في (المواد 226-16 إلى 226-24)[6]، و تجدر الإشارة إلى أنه كان هدف التشريع الفرنسي من خلال هذا القانون هو وضع النظام القانوني للمعلوماتية، و سمي قانون سنة 1978 بـــ : المعلوماتية و الحريات ***"Informatique et liberté"***، و في هذه الفترة لم تكن تعتبر

---

(1)_ أنظر : André Lucas, Jean Devrèze, Jean Frayssinet, ***Droit de l'informatique et de l'Internet***, édition Dalloz, collection Thémis (Droit Privé), Novembre 2001, (France), de la page 679.

(2)_ أول نص تشريعي جزائري في مجال جرائم المعلوماتية لم يظهر إلا سنة 2001 (مادة 144 مكرر و مكرر 1 و مكرر 2 و 146 ق.ع.ج)، يليه سنة 2004 نص تشريعي يظم سبعة مواد من المادة 394 مكرر إلى المادة 394 مكرر 7 تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات" القسم السابع مكرر من قانون العقوبات الجزائري، و مؤخرا القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق لـــ 5 أوت 2009 المتضمن : "القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها" و الذي دخل حيز النفاذ بموجب الجريدة الرسمية/العدد 47 الصادرة بتاريخ 16 أوت 2009.

(3)_ أنظر : **الملحق رقم 4**

(4)_ لمعرفة القوانين التي عدلت القانون رقم 78-19 أنظر : **الملحق رقم 5**

(5)_ أنظر : **الملحق رقم 5**

(6)_ أنظر : **الملحق رقم 6**

تكنولوجيا المعلوماتية إلا أداة بإمكانها المساس بحقوق الشخص، لاسيما منها الحق في إحترام حرمة الحياة الشخصية و ليس كأداة بإمكانها المساس بمال الغير و هذا إلى غاية صدور القانون رقم 88-19 السالف الذكر المتعلق المتعلق بالغش المعلوماتي.

إذا التشريع الفرنسي قبل قانون 88-19 في مجال الإجرام المعلوماتي لم يعالج إلا جريمة خرق القواعد في مجال حماية المعطيات ذات طابع شخصي ***"Données à caractère personnel"***، إذا بعد مرور 10 سنوات من المصادقة على قانون "المعلوماتية و الحريات"، البرلمان الفرنسي صادق على نص قانوني ثاني متعلق بمسألة المساس الغير المشروع بأنظمة المعالجة الآلية للمعطيات بما فيها الأنظمة المعلوماتية ***"Les systèmes informatiques"*** (المواد من 462-2 إلى 462-9 من قانون العقوبات الفرنسي) الذي تبعه في ما بعد بعض التغييرات في النصوص كرفع في حصة العقوبات و حذف إحدى التجريمات و الذي أدخل إلى قانون العقوبات و دخل حيز التنفيذ في 1 جانفي 1994[1] و الذي بموجب القانون رقم 2004-575 لـــ 21 جوان 2004 المتعلق بالثقة في الإقتصاد المعلوماتي، هذا القانون سمي بقانون ڤودفران ***"Loi GODFRAIN"*** نسبة إلى أحد نواب البرلمان الفرنسي المسمى بـــ : ڤودفران، كما عدل هذا القانون بصفة نهائية نظرة المشرع الفرنسي حول موضوع الساعة، حيث إعتبر أن الأنظمة المعلوماتية عبارة عن مال في حد ذاته، ولا بد على قانون العقوبات أن يحميه من المساسات الغير مشروعة[2].

أول نص تشريعي جزائري في مجال الإجرام المعلوماتي لم يظهر في قانون العقوبات إلا في 26 جويلية 2001 بموجب القانون رقم 01-09، المواد 144 مكرر و 146 و 144 مكرر 1 و 144 مكرر2 و 146 من قانون العقوبات الجزائري و المتعلق بجريمة القذف و السب و الإهانة إزاء رئيس الجمهورية أو في ما يخص دين الإسلام (الرسول و باقي الأنبياء أو ما هو معلوم من الدين) أو ضد الهيئات المؤسسة أو الهيئات العمومية، و من خصوصيات المادة 144 مكرر ق.ع.جزائري، أن المشرع أدرج فيها لأول مرة مصطلح "... وسيلة إلكترونية أو معلوماتية ... " التي تسمح بتجريم الأفعال السالفة الذكر في محيط المعلوماتية و الأنترنت بالإضافة إلى المواد 144 مكرر1 و 2 و 146 ق.ع.جزائري، وبعدها جاء القانون رقم 04-15 المؤرخ في 27 رمضان 1425 الموافق 10 نوفمبر سنة 2004 الذي أدخل إلى قانون العقوبات قسم سابع مكرر تحت عنوان : "المساس بأنظمة المعالجة الآلية للمعطيات " (المواد من 394 مكرر إلى 394 مكرر 7 ق.ع.جزائري).

---

[1] _ أنظر : **الملحق رقم 7**

[2] _ أنظر : André Lucas, Jean Devrèze, Jean Frayssinet, ***Op.cit***, de la page 679 à 680.

و تجدر الإشارة إلى أنه في حالة إنعدام نصوص خاصة بالجرائم المعلوماتية فهذا لا يمنع في بعض الأحوال تطبيق النصوص التقليدية في حالة إرتكاب جرائم تقليدية بواسطة تقنية المعلوماتية، إذ هناك نوعان من الجرائم المعلوماتية أولها : الجرائم المعلوماتية البحتة كجرائم المساس بالأنظمة المعلوماتية التي تستدعي تشريع نصوص عقابية خاصة تنظمها، و ثانيها : الجرائم التقليدية المرتكبة بواسطة المعلوماتية كجريمة السرقة المعلوماتية و التي يمكن تجريمها من خلال النصوص العقابية التقليدية الواردة في قانون العقوبات.

ب- القوانين المتعلقة بجرائم المعلوماتية قوانين نظرية ذات دور محدود

البرلمان الفرنسي لم يكن هدفه من خلال قانون 1988 وضع المبادئ الأساسية الكبرى لمكافحة جرائم المعلوماتية، و إنما تلخص هدفه في تلك الفترة بالدرجة الأولى في تغطية الفراغ القانوني السائد آنذاك في مجال جرائم المعلوماتية [1]، مع العلم بأن قانون ڤودفران عرف تعديل أول عند إدخاله في قانون العقوبات الفرنسي الجديد لسنة 1994، هذا التعديل شمل حذف إحدى التجريمات الواردة فيه و المتعلقة بالتزوير المعلوماتي بإعتبار أن المادة 441 فقرة 1 ق.ع.فرنسي تسمح بإدماج مثل هذا التجريم ضمن نصها، ومن جهة أخرى شمل التعديل الرفع في حصة العقوبات.

إذا الإجرام المعلوماتي آنذاك في نظر المجتمع الفرنسي كان ذات أهمية محدودة و بالتالي النص القانوني لسنة 1988 ذات دور محدود إذ أنه من ناحية الكم لم يتضمن إلا فئات قليلة من الجرائم في مجال المعلوماتية و التي أحيانا تكون أركانها غامضة، وفي هذا المجال تجدر الإشارة إلى أن المشرع الفرنسي وضع تعريف لنظام المعالجة الآلية للمعطيات تقريبا سنة قبل صدور المواد العقابية في هذا المجال [2] في حين أن المشرع الجزائري تأخر بحوالي 5 سنوات [3] وهو ما سنراه في المبحث الأول من الفصل الأول.

بعد صدور قانون ڤودفران لسنة 1988 الذي عدل في سنة 1994، إنطلقت أول مرحلة لمشروع قانون للحكومة الفرنسية حول فضاء الأنترنت، مثل ما تم التصريح به من طرف الوزير الأول جون بيار رفران

---

(1)_ أنظر : André Lucas, Jean Devrèze, Jean Frayssinet, ***Ibid***, page 679.

(2)_ و بالتالي تعريف نظام المعالجة الآلية للمعطيات جاء به مجلس الأمة الفرنسي بموجب الجريدة الرسمية، مجلس الأمة، لـــ 4 نوفمبر 1987، صفحة 3656، كتدعيم لاحق للرصيد العقابي الساري المفعول في هذا المجال.

(3)_ المشرع الجزائري على خلاف زميله الفرنسي أورد هذا التعريف مؤخرا بموجب المادة 2 (في ما يخص تعريف الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال، و المنظومة المعلوماتية، بالإضافة إلى تعريف المعطيات المعلوماتية و أخيرا من هم مقدمو الخدمات المعلوماتية عبر الشبكات) من القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق لـــ 5 أوت 2009 و المتضمن : "القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها" و الذي دخل حيز النفاذ بموجب صدوره في الجريدة الرسمية / العدد 47 بتاريخ 16 أوت 2009 أي 5 سنوات بعد صدور القانون حول جرائم المساس بأنظمة المعالجة الآلية للمعطيات (المواد من 394 مكرر إلى 394 مكرر 7 ق.ع.جزائري)، و من الملاحظ أن المشرع الجزائري كان على خطأ عندما فعل كذلك إذ أنه كان لا بد عليه أن يصدر كل من القانونين معا أو إدماجهما في قانون واحد أو على الأقل أن يسلك نفس المسلك الذي إتبعه المشرع الفرنسي، لضمان التطبيق السليم للقانون العقابي في هذا المجال خاصة و كما سبق ذكره تعريف المصطلحات في هذا المجال يتوقف أساسا عليها التطبيق السليم للمواد العقابية 394 مكرر و ما يليها و هو ما سيتم توضيحه في المبحث الأول من الفصل الأول.

"Jean Pierre Raffarin"، "المشروع التمهيدي لقانون حول الإقتصاد المعلوماتي " عرض على مجلس الوزراء و نوقش في البرلمان، بعده صدر ال قانون رقم 2004-575 لـــ 21 جوان 2004 تحت عنوان : "الثقة في الإقتصاد المعلوماتي" (متمم في 11 جويلية 2010)، الذي تتضمن أربعة مواضيع رئيسية، بالترتيب : حرية الإتصال عبر شبكة الأنترنت، التجارة الإلكترونية، الأمن في الإقتصاد المعلوماتي، و مجال أنظمة الأقمار الصناعية. و في هذا القانون سيهمنا بالأخص الفصل الثاني تحت عنوان : "المكافحة ضد الإجرام المعلوماتي" من الباب الثالث تحت عنوان : "الأمن في الإقتصاد المعلوماتي" من هذا القانون [1] لأنه أدخل تعديلات على قانون الإجراءات الجزائية الفرنسي و ذلك بإضافة المحيط المعلوماتي إلى نصوصها التقليدية (المواد 56، 94، 97 ق.إ.ج.فرنسي)، كما يعدل هذا القانون المادة 227 مكرر 23 من قانون العقوبات الفرنسي حول النشر و التثبيت، التسجيل أو بعث صور ذات طابع جنسي للقصر، كما عدل قانون ڤودفران في مواده 323-1 و 2 و 3 و 4 و 7، و شمل التعديل رفع في حصة العقوبات ، و إضافة مادة تضم تجريم جديد في قانون ڤودفران (المادة 323-3-1)، و بهذا فإن قانون ڤودفران قد عدل في قانون العقوبات الفرنسي للمرة الثالثة [2]، و تجدر الإشارة إلى أنه في نفس السنة 2004 التي صدر فيها قانون حول الثقة في الإقتصاد المعلوماتي صدر القانون 2004-801 لـــ 6 أوت 2004 المعدل قانون 1978 و الذي عدل من جديد مؤخرا بموجب القانون رقم 2009-526 المؤرخ في 12 ماي 2009 الذي دخل حيز النفاذ في 13 ماي 2009.

و قبل صدور القانون حول الثقة في الإقتصاد المعلوماتي، جاء مشروع قانون وضع من طرف الوزير الفرنسي للشؤون الخارجية أمام مجلس الوزراء في 11 جوان 2001، وهذا النص الذي وضع من طرف دومنيك دوفيلبان ***"Dominique de Villepin"*** يقترح المصادقة على إتفاقية بيداباست[3] حول : الإجرام المعلوماتي ***« Lacyber criminalité »*** [4] التي تم المصادقة عليها أمام المجلس الأوروبي في بيداباس ت في 23 نوفمبر 2001[5].

---

(1)_ أنظر : **الملحق رقم 8**

(2)_ أنظر : **الملحق رقم 9**

(3)_ أنظر : **الملحق رقم 10**

(4)_ ***"Cyber"*** : يقصد به المعلوماتية و الشبكات المعلوماتية ***"Les réseaux informatiques"*** و يعبر عنها أيضا بالفضاء الخيالي ***"Cyber espace"***.

(5)_ الهدف الأساسي من إتفاقية بيداباست هو وضع السياسة الجنائية العامة و المشتركة في مجال جرائم المعلوماتية الواجبة الإتباع من طرف الدول الأوروبية المصادقة على هذه الإتفاقية و ذلك بترجمة التوجيهات ***"Directives"*** في مجال الإجرام المعلوماتي التي جاءت بها هذه الإتفاقية على المستوى الوطني و بالتالي تحقيق الإنسجام ***"Harmonisation"*** في التشريع العقابي المتعلق بمحيط المعلوماتية في منطقة الإتحاد الأوروبي.

بعد أن تمت المصادقة على هذه الإتفاقية من طرف البرلمان الفرنسي يمكن أن نقول بأن الحكومة الفرنسية تحصلت على رصيد قانوني و إجرائي لا بأس به لمكافحة الإجرام المعلوماتي، لاسيما في مجال التعاون الدولي لتسليم المجرمين و كذا التعاون الردعي ضد الإجرام المعلوماتي، و هو ما حددته بالتفصيل إتفاقية بيداباست كون أن هذا النوع من الجرائم يدخل في صنف الجرائم العابرة للحدود***"Infractions transfrontalières"***.

ج- القوانين المتعلقة بجرائم المعلوماتية قليلة التطبيق

في حقيقة الأمر، القانون الجنائي للمعلوماتية قانون يعتمد أساسا على نصوص قانونية و يكاد يخلو من الإجتهادات القضائية، نظرا لحداثة الموضوع[1].

على المستوى الكمي، المكنزم التشريعي سواء الفرنسي أو الجزائري بقي أساسا نظري بالإضافة إلى قلة النصوص التشريعية، كما أن المحاكم بصفة عامة لم تطبق هذه النصوص إلا في مناسبات نادرة[2].

في فرنسا، في بداية الأمر بعد صدور القانون حول الغش المعلوماتي، أهم الأحكام القضائية التي صدرت عن قضاة الموضوع لم تتعلق إلا بجريمة المساس بالمعطيات المعلوماتية أو الأنظمة المعلوماتية في محيط إلكتروني كلاسيكي[3] إلا أن الوضع سرعان ما تغير بعد ذلك و لاسيما بظهور الشبكات المعلوماتية التي تسمح بربط أجهزة الكمبيوتر فيما بينها و في أغلب الأحيان بصفة مستمرة ***"Ordinateurs interconnectés en permanence"***.

على المستوى النوعي، المحاكم في بداية الأمر إمتنعت عن وضع إجتهادات قضائية بناءة لتكملة النقائص الواردة على مستوى النصوص القانونية.

و في هذا الصدد محكمة النقض الفرنسية قالت بأنه : في حالة عدم وجود نص تشريعي عقابي صريح فإنه غير ممكن للقاضي الجنائي معاقبة تصرف معين، و بالتالي حسب نظرها فإن مستعمل الموزع الإلكتروني للنقود بواسطة بطاقته الإلكترونية البنكية إذا إستعمل طرق إحتيالية تقنية للحصول على مبلغ مالي يفوق المبلغ المحدد في رصيده لا يشكل جريمة، و لا يعتبر إلا نزاع يطرح أمام القاضي المدني بين مالك البطاقة البنكية أي الزابون و البنك، نفس الشيء بالنسبة لمن يبرمج و يوزع الفيروسات المعلوماتية فلا تشكل هذه التصرفات جريمة ما دام أن قانون العقوبات لم يجرمها صراحة لكن الوضع لم يدم طويلا، بفضل تطور الإجتهادات القضائية في هذا الميدان.

---

(1)_ أنظر : André Lucas, Jean Devrèze, Jean Frayssinet, ***Op.cit***, page 679.

(2)_ أنظر : André Lucas, Jean Devrèze, Jean Frayssinet, ***Idem***.

(3)_ أي الجرائم المرتكبة في مجال معلوماتي مغلق خارج عن أي شبكة إتصال معلوماتية.

د- وسائل إرتكاب الجريمة المعلوماتية مستحدثة

إرتكاب جريمة معلوماتية على خلاف الجرائم التقليدية الأخرى يستلزم توافر جهاز كمبيوتر أو أي جهاز بإمكانه المعالجة الآلية للمعطيات المعلوماتية كأجهزة فك الرموز المقرصنة ***"Les décodeurs ou appareil de décryptage pirates"*** التي يمكن مثلا إستعمالها لسرقة الأموال من أجهزة التوزيع الآلي للنقود أو إستعمالها بهدف الدخول الإحتيالي في نظام معلوماتي محمي تقنيا.

ه- صعوبة إكتشاف و إثبات الجريمة المعلوماتية

لأنها لا تترك أثرا مرئيا أو كتابيا لما يجرى خلال تنفيذ الجريمة، كما يمكن للجاني حذف المعلومات و المعطيات التي يمكن أن تستخدم كدليل ضده [1]، و بالتالي فهي صعبة الإكتشاف و الإثبات لإدانة مرتكبها و هذا ما يشكل تحديا للمشرع، و الشرطة القضائية التي لن يكون بيدها إلا حل وحيد و هو إستعمال نفس الوسيلة التي يستعملها المجرم المعلوماتي أي المعلوماتية كالسبيل الوحيد لإكتشاف و إثبات الجريمة.

و- الجريمة المعلوماتية تتعدى حدود الدولة الواحدة

بمعنى أنه يمكن للجريمة أن تمتد من دولة إلى أخرى، أو ترتكب من دولة لتصيب دولة أخرى بإستخدام الشبكات المعلوماتية وهنا تطرح مشكلة الإختصاص القضائي و كذا قانون العقوبات الواجب التطبيق.

ي - الإختصاصات الإستثنائية لضباط الشرطة القضائية في الجرائم المعلوماتية

يؤول إختصاص المحاكمة في الجزائر و على خلاف النظام القضائي الفرنسي في ما يخص الجرائم المعلوماتية و بما فيها الماسة بأنظمة المعالجة الآلية للمعطيات المعلوماتية إلى الأقطاب المتخصصة ***"Des pôles spécialisés"*** بعدد أربعة على المستوى الوطني (بقسنطينة، الجزائر العاصمة – سيدي أمحمد، وهران و ورقلة)، كما أن المشرع الجزائري على خلاف سائر الجرائم الأخرى فإنه وسع من إختصاص ضباط الشرطة القضائية بصفة إستثنائية في حالة ما إذا كان التحقيق التمهيدي يخص جرائم معينة أي تلك المتعلقة بـــ : المخدرات، تبييض الأموال أو تلك المتعلقة بالتشريع الخاص بالصرف أو الماسة بأنظمة المعالجة الآلية للمعطيات و الجريمة المنظمة عبر الحدود الوطنية و كذا جرائم الفساد المنصوص و المعاقب عليها بموجب القانون رقم 06-01 المؤرخ في 20 فيفري 2006 و المتعلق بالوقاية و مكافحة الفساد، فقد أصبح بموجب القانون رقم 06-01 المؤرخ في 20 ديسمبر 2006 المعدل و المتم لقانون الإجراءات الجزائية يتمتع بإختصاصات أوسع في سبيل تسهيل إجراءات البحث و التحري عن تلك الجرائم و كشف مرتكبيها و جمع الإستدلالات عنها بما يمكنه من مواجهة الصعوبات التي قد تعترضه نظرا لخطورة و طبيعة تلك الجرائم، كما

---

[1]_ أنظر : هشام محمد فريد رستم، **مرجـــع سابـــق**، صفحة 27.

مكن المشرع ضباط الشرطة القضائية بموجب القانون رقم 06-22 من إختصاصات جديدة لم يكن يتمتع بها قبل صدور هذا القانون و هي سلطة مراقبة الأشخاص و الأموال و الأشياء و إعتراض المراسلات و تسجيل الأصوات و الصور و القيام بعمليات التسرب[1].

سادسا : الإشكال القانوني المتعلق بجرائم المعلوماتية

مع العلم بأن الإعلام الآلي و وسائل الإتصال الحديثة قد عرفت تطور تكنولوجي سريع و هائل، هذا التطور من جهة أخرى أدى إلى خلق نوع جديد من الجرائم و هو ما يسمى بـــ "الجرائم المعلوماتية"، هذا النوع من الجرائم أثار عدة إشكالات و صعوبات سواء من الناحية النظرية لاسيما تعريفها، موضوعاتها، أصناف الجرائم المرتبطة بها أو من الناحية العملية لقلة الأحكام و الإجتهادات القضائية و البحوث الفقهية البناءة[2].

إلى يومنا هذا ظهرت أنواع كثيرة من جرائم المعلوماتية سواء في محيط إلكتروني كلاسيكي غير مرتبط بشبكة إتصال معينة أو جرائم عبر شبكة الأنترنت أو شبكة معلوماتية خاصة و غيرها من أنواع الشبكات المعلوماتية[3]، بحيث أدى ذلك إلى خلق فارق كبير بين النصوص التشريعية و هذا النوع الجديد من الجرائم، بمعنى تظل هذه الجرائم في تطور مستمر و سريع بالمقارنة مع التشريع العقابي، مع العلم بأن النصوص التقليدية غير كافية و غير صالحة في أغلب الأحيان لتطبيقها على هذا النوع من الجرائم [4] إلا في حالات معينة.

إهتمامنا الأول في هذه المذكرة و إن كانت المهمة صعبة نوعا ما هو محاولة ذكر كل أنواع جرائم المعلوماتية التي ظهرت إلى حد الآن و كذا ترتيبها حسب التقسيم التقليدي للجرائم، و أخيرا تقييم هذه الجرائم.
و بالتالي الإشكال الأول الذي سيطرح هو :

---

(1)_ أنظر : محمد حزيط، "**مذكرات في قانون الإجراءات الجزائية الجزائري**"، دار هومه، الطبعة الثالثة 2008، الجزائر، صفحة 68.

(2)_ هذه الصعوبات سواء النظرية إلى جانب الصعوبات الميدانية و العملية التي تطرحها الممارسة السياسية و القضائية في هذا الميدان المستحدث تنبأ بها الأستاذ الدكتور طاشور عبد الحفيظ بموجب تحليله الموسع و الشامل لميدان المعلوماتية و الأنترنت من حيث الصعوبات سواء القانونية العملية أو السياسية في مقاله :
أ. طاشور عبد الحفيظ، "**شبكة الأنترنت، الرهانات التكنولوجية و الإشكالات القانونية**"، أعمال المؤتمر التاسع للإتحاد العربي للمكتبات و المعلومات، دمشق أيام 21 إلى 26 أكتوبر 1998، تونس، المنظمة العربية للتربية و الثقافة و العلوم و الإتحاد العربي للمكتبات و المعلومات 1999، من الصفحة 251 إلى 258.

(3)_ هذه الشبكة يمكن لأي مستعمل لأكثر من كمبيوتر إنشائها حيث تسمح الربط بين جهازي كمبيوتر أو أكثر بهدف تسهيل نقل المعلومات فيما بينها، أمثلة عنها : شبكة وايفي ***"Wifi"*** أو بلوتوث ***"Bluetooth"*** (شبكات إتصال لا سلكية) أو إيثرنت ***"Ethernet"*** (شبكة إتصال سلكية).

(4)_ أنظر المستند **(WORD)**، (إعداد : يونس عربي، تحت عنوان : **جرائم الكمبيوتر والانترنت – إيجاز في المفهوم و النطاق و الخصائص و الصور و القواعد و القواعد الإجرائية للملاحقة و الإثبات** المستنسخ Téléchargé من صفحة الأنترنت التالية :
www.doc.abhatoo.net.ma/IMG/doc/dro35.doc (page 3 du document)

ماهي جرائم المعلوماتية التي تدخل في قسم الجرائم ضد الأموال و تلك التي تدخل في قسم الجرائم ضد الأشخاص و الحريات في نظر القانون الجزائري و التشريعات المقارنة ؟

من جهة أخرى و مع العلم بأن القانون الجنائي غير قابل للتطبيق إلا وفقا للتفسير الضيق للمواد الجزائية كمبدأ من مبادئ شرعية الجرائم و العقوبات و بالتالي لا يجوز للقاضي تحت غطاء التفسير الواسع خلق جرائم تخرج عن نطاق نص القانون كما لا يجوز له القياس في حالة الجرائم التقليدية المرتكبة بواسطة المعلوماتية بالنصوص التقليدية إلا إذا توافرت الأركان التي حددتها هذه النصوص[1]، و في سبيل الخروج من هذا اللبس، الإشكال الثاني الذي يمكن طرحه هو :

أين وصل الإطار القانوني الجزائي الجزائري و المقارن لردع هذا النوع الجديد من الجرائم و ما يتضمنه من صعوبات ؟

سابعا : المنهجية المتبعة

إتبعنا أثناء إعداد المذكرة منهجين، المنهج الوصفي و المنهج التحليلي حيث قمنا بوصف كل جريمة من الجرائم المعلوماتية، كما إتبعنا المنهج المقارن و الذي يعد في نظرنا أهم منهج بإعتباره سيسمح لنا مقارنة الوضعية في كل من القانون الجزائري و المقارن بهدف إبراز أوجه الشبه و الإختلاف إن وجدت و بهذه الطريقة يمكن تحسين التشريع بصفة عامة في ميدان المعلوماتية من الجانب العقابي.

ثامنا : الخطة المتبعة مع التسبيب

كما قلنا في الإشكال القانوني الأول أي، ما هي جرائم المعلوماتية التي تدخل في قسم الجرائم ضد الأموال و تلك التي تدخل في قسم الجرائم ضد الأشخاص و الحريات في نظر القانون الجزائري و التشريعات المقارنة ؟، الإجابة على هذا التساؤل تظهر من خلال الفصلين أي التقسيم التقليدي للجرائم، و بالتالي ستضم المذكرة فصلين، الفصل الأول تحت عنوان جرائم المعلوماتية ضد مال الغير (بمعناه المعنوي) و الفصل الثاني تحت عنون حرية التعبير و جرائم المعلوماتية ضد الأشخاص و الحريات.

---

[1]_ أنظر : أحسن بوسقيعة، "**الوجيز في القانون الجزائي العام** "، (الطبعة الأولى، طبعة 2002)، الديوان الوطني للأشغال التربوية، (الجزائر)، صفحة 58.

الفصل الأول :
جرائم المعلوماتية الماسة بالأموال ذات طبيعة إلكترونية

- المبحث الأول : الفعل الإجرامي ضد أنظمة المعالجة الآلية للمعطيات
- المبحث الثاني : جريمة التزوير المعلوماتي
- المبحث الثالث : جريمة السرقة المعلوماتية
- المبحث الرابع : جريمة النصب المعلوماتي
- المبحث الخامس : جريمة خيانة الأمانة المعلوماتية

الـــفـــصـــل الأول :
جرائم المعلوماتية الماسة بالأموال ذات طبيعة إلكترونية

في هذا الفصل سنتكلم أولا عن نوع جديد من الجرائم الخاصة بمحيط المعلوماتية أي الفعل الإجرامي ضد الأنظمة المعلوماتية، في القانون الفرنسي في المواد من 323-1 إلى 323-7 التي أدخلت إلى قانون العقوبات الفرنسي في فصل تحت عنوان : المساسات بأنظمة المعالجة الآلية للمعطيات ***"Les atteintes contre les systèmes de traitement automatisé"***، مقارنة مع القانون الجزائري لاسيم ا منه المواد 394 مكرر إلى 394 مكرر 7، التي أدخلت إلى القسم السابع مكرر من قانون العقوبات الجزائري ، تحت عنوان : المساس بأنظمة المعالجة الآلية للمعطيات، و تجدر الإشارة إلى أن هذه القوانين هدفها هو معاقبة مختلف أنواع التصرفات الماسة بأنظمة المعالجة الآلية للمعطيات أي الأنظمة المعلوماتية ***"Les systèmes informatiques"*** بكل أنواعها (المبحث الأول).

بعد ذلك سنتكلم عن الجرائم التقليدية الأخرى التي يمكن أن ترتكب بواسطة المعلوماتية و في محيط المعلوماتية، و هنا عدد معين من الجرائم التقليدية التي تستعمل في إرتكابها تقنية المعلوماتية يمكن أن يطبق عليها القواعد الجزائية التقليدية حسب الظروف و الحالات، و بالتالي فلا يمكن تطبيق أو مطابقة النصوص التقليدية بصفة مباشرة على جرائم التقنية العالية إلا إذا توافرت شروط معينة تسمح بذلك أي أركان الجريمة، و هنا سنتكلم عن جريمة التزوير المعلوماتي (المبحث الثاني)، جريمة السرقة المعلوماتية (المبحث الثالث)، جريمة النصب المعلوماتي (المبحث الرابع)، و أخيرا سنتكلم عن جريمة خيانة الأمانة المعلوماتية (المبحث الخامس)، كل هذه الجرائم تخضع إلى الأحكام العقابية الواردة في قانون العقوبات الجزائري و المقارن ، و بالتالي دراستنا ستقتصر على هذه الجرائم المرتكبة بواسطة المعلوماتية و في محيط معلوماتي و المال محل الجريمة المعلوماتية هو بطبيعة الحال مال في شكله المعلوماتي***"Bien immatériel"*** [1].

---

[1] _ نحن في مذكرتنا بإستثناء المبحث الأول الذي سندرس فيه جريمة معلوماتية بحتة، فإننا سنركز دراستنا في ما يلي ذلك على الجرائم التقليدية و لكن مرتكبة في محيط المعلوماتية، مثلا : عندما سنتكلم عن جريمة السرقة المعلوماتية فإننا سنركز دراستنا على سرقة الأموال المعنوية كالمعطيات و النقود المعنوية و المعلومات بصفة عامة بإعتبارها تنتمي إلى المحيط المعلوماتي، و هو ما يشكل صعوبة إضافية بالمقارنة مع المال في شكله التقليدي الملموس المتعارف عليه.

المبحث الأول :

الفعل الإجرامي ضد أنظمة المعالجة الآلية للمعطيات

في ما يخص القانون حول المساسات بالأنظمة المعلوماتية (المواد من 394 مكرر إلى 394 مكرر 7 ق.ع.جزائري)، فلقد إتخذت الحكومة الجزائرية الإجراءات اللازمة لإصداره و ذلك توافقا مع المادة 86 في قسم تحت عنوان : "الوقاية و مقاومة الجريمة المنظمة " بما في ذلك مقاومة الجريمة المعلوماتية المنصوص عليها في الإتفاقية الأورومتوسطية (إتفاقية دولية متعددة الأطراف) المؤرخة في 22 أفريل 2002[1] و التي كانت تهدف إلى ربط الجهود بين الوحدة الأوروبية و الدول الأعضاء فيها من جهة و الحكومة الجزائرية من جهة أخرى في ميادين مختلفة، و منها ما ورد في الفصل الثامن ***"(Titre VIII)*** تحت عنوان : "التعاون في مجال القضاء و الشؤون الداخلية"[2] ***"Coopération dans le domaine de la justice et des affaires intérieurs".***

و تجدر الإشارة إلى أن الحكومة الجزائرية في ما بعد صادقت على (إتفاقية دولية ثنائية) بينها و بين الحكومة الفرنسية و المتعلقة بـــ : "التعاون في مجال الأمن و مكافحة الإجرام المنظم " الموقع عليها بالجزائر في 25 أكتوبر 2003 و التي دخلت حيز النفاذ بموجب المرسوم الرئاسي رقم 07-375 المؤرخ في 21 ذي القعدة عام 1428 الموافق لـــ 1 ديسمبر 2007 المنشور في الجريدة الرسمية المؤرخة في 9 ديسمبر 2007/العدد 77[3].

و بهذا المجهود تكون الحكومة الجزائرية قد أكدت إرادتها في وضع رصيد تشريعي عقابي محكم في سبيل مكافحة الجريمة المعلوماتية بشتى أنواعها و كذا تكريس و تعزيز التعاون الدولي في هذا المجال بإعتبار أن المواجهة الوطنية المنفردة لهذه الظاهرة المستحدثة ليس بحل كافي نظرا لكون أن هذا النوع المستحدث من الجرائم يتعدى حدود الدولة الواحدة كما ذكرناه سابقا في مقدمة هذه المذكرة.

في هذا المبحث سنحاول أولا تعريف نظام المعالجة الآلية للمعطيات وحدوده في ما يخص تطبيق قانون العقوبات على الإنتهاكات التي تتم عليه[4] و كذا محاولة تعريف صاحب النظام المعلوماتي (المطلب الأول)، ثم سنتحدث عن الجرائم التي يمكن أن ترتكب في هذا المحيط الجديد و بالأخص عن الدخول و البقاء الإحتيالي

---

(1)_ أنظر : **الملحق رقم 11**

(2)_ ملاحظة هامة : هذه الإتفاقية لا تشمل فقط الجرائم ضد الأنظمة المعلوماتية بل تمتد أحكامها إلى كل أنواع جرائم المعلوماتية سواء كانت ضد الأموال أو الأشخاص و الحريات بإعتبار أن المقصود من المادة 86 من هذه الإتفاقية كان واسع.

(3)_ أنظر : **الملحق رقم 12**

(4)_ أنظر : **الملحق رقم 13 : برنامج مبعوث خاص *Envoyé Special* في قناة التلفزية *France 2* ليوم : الخميس 7 ماي 2010 تحت عنوان : المجرمين المعلوماتيين *Les Cybercriminels***، روبرتاج إعداد كل من : آن ريشارد، جيروم بافلوفسكي و ستيفان روسي ***Un reportage de Anne Richard, Jérôme Pavlovsky et Stéphane Ross.***

في نظام معلوماتي مملوك للغير (المطلب الثاني)، و كذا المساسات الإرادية بالأنظمة المعلوماتية (المطلب الثالث)، و أخيرا المساسات بالمعطيات المعلوماتية الموجودة داخل هذا النظام (المطلب الرابع).

المطلب الأول : نظام المعالجة الآلية للمعطيات

هنا سنتكلم عن النظام المعلوماتي من حيث التعريف الذي وضعه قانونيين بالتعاون مع مختصين في مجال المعلوماتية كدراسة أساسية من خلالها يمكن فهم الجرائم الماسة بها (الفرع الأول)، و حدود هذا التعريف من حيث التطبيق على الحالات العملية التي تطرح على القاضي الجزائي و إن كانت في أغلب الأحيان نادرة (الفرع الثاني)، ثم سنعرف صاحب النظام المعلوماتي بإعتبار أن ذلك سيسمح من جهة أخرى تحديد المسؤوليات في حالة خرق نظام معلوماتي (الفرع الثالث)، و أخيرا سنعرض بالشرح الوافي جملة من الجرائم التي تدخل في نطاق المساسات بالأنظمة المعلوماتية على ضوء التشريع العقابي الجزائري و المقارن و بالأخص القانون الفرنسي (الفرع الرابع)، بإعتبارها جرائم معلوماتية بحثة مستحدثة لا مثيل لها في الجرائم التقليدية.

الفرع الأول : تعريف نظام المعالجة الآلية للمعطيات

تعريف نظام المعالجة الآلية للمعطيات يتفق مع التعريف التقني للنظام المعلوماتي، و لمزيد من الدقة يمكن الرجوع إلى التعريف الذي وضعه مجلس الأمة الفرنسي (الجريدة الرسمية، مجلس الأمة، 4 نوفمبر 1987، صفحة 3656) كما يلي : "هو كل مجموعة منسجمة تتكون من وحدة أو عدة وحدات معالجة، ذاكرة، و برامج، و معطيات، وحدات إدخال و إخراج، و إتصال بين هذه المكونات التي تؤدي إلى إعطاء نتيجة محددة، و هذه المجموعة تكون محمية تقنيا بموجب أي وسيلة أو مكنزم إئتمان[1] ***"Dispositif de sécurité"***[2].

---

[1] _ الوسائل المستعملة غالبا لحماية الأنظمة المعلوماتية هي : البرامج المضادة للفيروسات و القرصنة ***"Les programmes anti-virus et anti-piratage (Pare-feu ou Firewall)"*** و كذا برامج أو مكنزمات الحماية بموجب رموز أو شفرات إئتمان سرية ***"Les programmes ou dispositifs de protection par des codes de sécurité"*** و المشرع بصفة عامة لم يشترط صراحة توافر حماية معينة للنظام و بالتالي عدم توافر حماية لا يعفي من تطبيق قانون العقوبات، إلا أنه في الجانب العملي يستحسن توافر حماية تقنية للنظام كوسيلة إثبات إضافية على منع الدخول في النظام من طرف الغير سيء النية.

[2] _ أنظر : Hollande Alain, De Bellefonds Linant Xavier, ***Pratique du droit de l'informatique***, édition Delmas (5e édition), Avril 2002, (France), page 250.

"إذا رجعنا الآن إلى تعريف مجلس الأمة الفرنسي فإننا نستنتج بأن نظام المعلوماتية هو كل مجموعة معلوماتية مهما كان حجمها، أو أسلوب إتصالها بمكونات أو أنظمة أخرى، و مهما كان أسلوب معالجتها للمعطيات [1] فإنها تشكل نظام معلوماتي"[2].

يمكن أن نستنتج أيضا أنه حتى نكون بصدد نظام معلوماتي (نظام معالجة آلية للمعطيات المعلوماتية) فإنه لا يشترط أن يتوافر فيه حجم معين و تعدد أو قلة العناصر المادية المكونة له أو التي هي بإتصال به[3].

و تجدر الإشارة إلى أن المشرع الجزائري تأخر كثيرا في وضع تعريف واضح لمحل الجرائم المنصوص عليها في المواد 394 مكرر إلى 394 مكرر 7 ق.ع.جزائري، أي 5 سنوات بعد صدور هذه المواد العقابية، و هذا على خلاف المشرع الفرنسي الذي أخذ إحتياطاته في وضع تعريف لنظام المعالجة الآلية للمعطيات قبل إصداره للقانون حول المساسات الغير مشروعة بأنظمة المعالجة الآلية للمعطيات، لكون أن هذا التعريف يعد لب هذا القانون، و بما أن التطبيق السليم لهذا القانون يتوقف على توافر تعريف لمحل الجريمة أي نظام المعالجة الآلية للمعطيات، فإنه كان لا بد على المشرع الجزائري أن يتبع نفس المنهج الذي إتبعه المشرع الفرنسي في هذا المجال لا غير أما في ما يخص صياغة هذا التعريف فسنرى بأن المشرع الجزائري جاء في قانونه الجديد بتعريف أحسن و أشمل إلى كل أنواع الأنظمة المعلوماتية، عن الذي وضعه المشرع الفرنسي في 1987.

بالرجوع إلى المادة 2 تحت عنوان : المصطلحات، من القانون رقم 09-04 المؤرخ في 5 أوت 2009 و المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها (الجريدة الرسمية لـــ 16 أوت 2009 / العدد : 47)، نجدها تنص عما يلي :

"يقصد في مفهوم هذا القانون بما يأتي :

...

ب- منظومة معلوماتية : أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين،

---

[1]_ و تجدر الإشارة إلى أن إتفاقية بيداباست عرفت هي الأخرى النظام المعلوماتي في المادة 1 من الفصل الأول من الإتفاقية تحت عنوان : المصطلحات "***Terminologie***"، و يمكن أن نلاحظ حسب رأينا بأن هذا التعريف لا يتعارض مع التعريف الذي جاء به مجلس الأمة الفرنسي ماعدا في ما يخص نقطة الحماية التقنية للنظام المعلوماتي التي سرعان ما ألغى شرط توافرها حتى تقوم الجريمة، بفضل إجتهاد قضائي لمجلس قضاء باريس في 5 أفريل 1994.

[2]_ أنظر : Hollande Alain, De Bellefonds Linant Xavier, ***Op.cit***, page 250.

[3]_ أنظر : Hollande Alain, De Bellefonds Linant Xavier, ***Idem***.

"..."[1].

يمكن أن نلاحظ بعد الإطلاع على كل من التعريفان في التشريع الفرنسي و الجزائري، بأن هنالك إختلاف واضح من حيث صياغة تعريف أنظمة المعالجة الآلية للمعطيات، يتمثل في كون أن المشرع الجزائري جاء بتعريف عام و غير دقيق بالمقارنة مع التعريف الذي وضعه مجلس الأمة الفرنسي سنة 1987، غير أنه رغم ذلك يمكن التأكيد بأن التعريف الذي جاء به المشرع الجزائري صحيح و لا ربما أحسن من التعريف الفرنسي و الأوروبي من خلال إتفاقية بيداباست لسبب بسيط هو أن أنواع الأنظمة المعلوماتية كثيرة و لا تنحصر فقط في أجهزة الكمبيوتر كما أشار إليه مجلس الأمة الفرنسي من خلال تعريفه و الذي كان لا بد عليه أن يعدله و السبب في ذلك سنفسره لاحقا، مما يؤكد بأن المشرع الجزائري كان على صواب على الرغم من تأخره في وضع هذا التعريف بالإضافة إلى تعريفات أخرى التي على أساسها يتوقف التطبيق السليم للمواد 394 مكرر إلى 394 مكرر 7 ق.ع.جزائري، من جهة أخرى مجلس الأمة الفرنسي إشترط في تعريفه أن يكون النظام المعلوماتي محمي تقنيا حتى تقوم الجريمة و هو عكس ما ورد في التعريف الذي جاءت به إتفاقية بيدابست المادة 2 منها، حيث سنرى بأن الإجتهاد القضائي الفرنسي خالف هذه القاعدة، في حين أن المشرع الجزائري لم ينص صراحة على وجوب توافر حماية تقنية للنظام حتى تقوم الجريمة.

إذا مما سبق يجب أن نوضح بأن القانون الفرنسي لسنة 1988 أو الجزائري لسنة 2004 المتعلق بالمساس بنظام المعالجة الآلية للمعطيات "***L' atteinte au système de traitement automatisé***" لا يصوب مباشرة و بصفة منفردة الكمبيوتر فقط بل كذلك كل نظام أو جهاز بإمكانه المعالجة الآلية للمعطيات المعلوماتية، و بالتالي فإن شبكة الأنترنت ***"Le réseau Internet"*** يمكن أن تكيف هي الأخرى بنظام معالجة آلية للمعطيات [2]، كما أكد الأستاذ جون دفراز "***Jean Devrèze***" بأن البريد الإلكتروني "***Boite e-mail***" بالإضافة إلى مصالح الخدمات التقنية للدخول إلى شبكة الأنترنت أو تثبيت صفحات أو مواقع أنترنت في شبكة الأنترنت ***"Les services techniques d'accès ou d'hébergement sur Internet"*** تعد أنظمة معلوماتية، كما يمكن إعتبار موقع الأنترنت " ***Site Web***" في حد ذاته نظام معلوماتي مستقل عن مختلف الخدمات التي يمكن أن تثبتها فيه و تفتحها لمستعملي الأنترنت، كما تعتبر مجرد بطاقة إلكترونية " ***Carte à microprocesseur ou électronique"*** نظام معلوماتي و بالتالي حسب ما سلف ذكره فإن قراءة المعلومات المحتواة في أي بطاقة إلكترونية يشكل جريمة، بإعتبار أن هذه البطاقات

---

(1)_ أنظر النص بالغة الفرنسية :

Art 2 sous le titre : Terminologie, de la loi n° 09-04 du 5 août 2009 portant règles particulière relatives à la prévention et à la lutte contre les infraction et de la communication :
« Au sens de la présente loi, on entend par :
…
b – Système informatique : tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentées qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données
… ».

(2)_ أنظر : Bensoussan Alain (sous la direction de), ***Internet : aspect juridique***, édition Hermès, juin 1996, (France), page 107.

عبارة عن جزء من نظام معلوماتي كامل بإمكانه قراءة أو إدخال معلومات في هذه البطاقات عندما تكون في إتصال معه، ومثال ذلك : بطاقة الإئتمان البنكية التي تعد هي الأخرى جزء من نظام معلوماتي و هو الموزع الإلكتروني أو الآلي للعملة أو النقود ، إذا البطاقة الإلكترونية البنكية تعد أيضا نظام معلوماتي [1]، أيضا يعتبر نظام معلوماتي القرص النقال "***Disque amovible (CD-Rom, Disquette, Flash disque)***" أو القرص المرن ***"Disque dur"*** إذا كان يحتوي على برنامج معلوماتي خاص بالمحاسبة أو يحتوي على معطيات أو بيانات أو مستندات محاسبة، نفس الشيء بالنسبة للقرص المضغوط الذي يحتوي على قاعدة معطيات ***"Base de données"*** و البرنامج المعلوماتي الذي يسمح الدخول إلى هذه القاعدة[2].

و تجدر الإشارة إلى أنه في نظر فقهاء القانون يمكن أن يمتد تعريف نظام المعلوماتية أيضا إلى ما يعرف بالأشرطة الممغنطة "***Bandes magnétiques cryptées***" التي تحتوي على معلومات أو معطيات محمية برموز سرية، أو أي دعامة مادية "***Support matériel***" أخرى تحتوي على معطيات بإعتبارها جزء من نظام معلوماتي و لكن بشرط أن تكون محمية بموجب خوارزمية تجعل من الصعب فك رموزها "***Algorithme de cryptage***" [3].

نفس الشيء بالنسبة للأقراص المضغوطة أو أي دعامة مادية خاصة بتخزين المعلومات و التي تحمل ضمنها برنامج خاص لكي يكون مقروء من طرف جهاز إلكتروني معين، فإنه يشكل نظام مع هذا الجهاز.

من جهة أخرى تجدر الإشارة إلى أنه لا يهم إذا إرتكب التصرف الغير مشروع ضد الأنظمة في مجال إلكتروني مغلق (خارج عن أي شبكة معلوماتية) ***"Connexion matérielle"*** أو مفتوح (بإستعمال شبكة الأنترنت أو الأنترانت أو أي شبكة خاصة للربط بين أجهزة الكمبيوتر) ***"Connexion électronique"*** و ليس لذلك أثر على التكييف القانوني للجريمة مادام أن الشبكة المعلوماتية (أنترنت أو أنترانت) تعتبر هي الأخرى نظام معلوماتي، و بالتالي يمكن معاقبة كل الجرائم المتعلقة بنظام المعلوماتية بإعتباره محل للجريمة[4].

كما أنه لا بد أن نشير إلى أن هذا القانون حول المساسات بالأنظمة المعلوماتية سواء الفرنسي أو الجزائري يطرح إشكال من حيث القانون الواجب التطبيق و كذا الجهة القضائية المختصة بالمحاكمة في حالة ما إذا كان مرتكب الجريمة في دولة و الجريمة ضد النظام المعلوماتي في دولة أخرى من خلال إحدى شبكات الإتصال المعلوماتية ؟

---

(1)_ ***Jugement du tribnal de Paris du 25 février 2000***.

(2)_ أنظر : André Lucas, Jean Devrèze, Jean Frayssinet, ***Droit de l'informatique et de l'Internet***, édition Dalloz, collection Thémis (Droit Privé), Novembre 2001, (France), de la page 689 à 690.

(3)_ أنظر : Hollande Alain, De Bellefonds Linant Xavier, ***Op.cit***, page 250.

(4)_ أنظر : Bensoussan Alain (sous la direction de), ***Op.cit***, page 107.

في ما يخص إشتراط أو عدم إشتراط توافر حماية تقنية للنظام المعلوماتي حتى تقوم الجريمة : فتجدر الإشارة إلى أن قرار صادر عن مجلس قضاء باريس، غرفة الجنح في 5 أفريل 1994 حدد بأنه : "حتى يعاقب الدخول أو البقاء يجب أن يتم دون ترخيص و مع علم المجرم بأن دخوله أو بقائه غير مسموح به و تجدر الإشارة إلى أنه لا يشترط حتى تقوم الجريمة أن يكون النظام محمي بمكنزم إئتمان ***"Dispositif de sécurité"*** بل يكفي أن يكون صاحب أو مالك النظام قد صرح أو وضح للجمهور بأن الدخول أو البقاء في النظام غير مسموح به بإستثناء مثلا الأشخاص الذين تحصلوا على رخصة لذلك، و بالتالي بدون ترخيص تقوم الجريمة إلا إذا تم الدخول أو البقاء خطأ أو بالصدفة ***"Accès ou maintien Accidentel ou par coïncidence"*** و دون أن يكون هدف الشخص الإضرار بالنظام"[1].

الفرع الثاني : حدود هذا التعريف

تعريف النظام المعلوماتي وفقا للتشريع الفرنسي يشترط بالضرورة توافر في آن واحد مكونات مادية ***"Hardware"*** (ما هو ملموس في الجهاز و له دور مهم لتشغيل النظام محل الحماية الج) + مكونات معنوية ***"Software"*** (أي البرامج و المعطيات المعلوماتية الموجودة في النظام محل الحماية الجنائية)، و بالتالي من بين حدود التعريف أن القانون حول المساسات بالأنظمة لا يعنيه المساسات بالمكونات المادية وحدها (كالمساس بقارئة الأقراص المضغوطة أو إفساد شاشة الكمبيوتر أو الذاكرة) أو المكونات المعنوية وحدها (كتفكيك برنامج أو نسخة من برنامج لا علاقة له بالنظام محل الحماية الجنائية أو موجود فيه) [2] ، في حين أن المشرع الجزائري من خلال صياغته لتعريف المنظومة المعلوماتية يكون قد أعطى مجال أوسع للقاضي في تقدير ما إذا كان المال محل الجريمة يدخل في حكم المنظومة المعلوماتية أم لا، و ما يكرس هذا الطرح هي الآراء الفقهية السالفة الذكر في هذا المجال.

غير أنه من الصعب إستبعاد التعريف الذي جاء به المشرع الفرنسي كليا و الذي يفهم منه بأن المواد العقابية حول المساسات بالأنظمة لا تحمي المكونات المعزولة (مادية وحدها أو معنوية وحدها) [3]، و إنما تحمي مجموعة منسجمة ***"Ensemble harmonieux"*** يهدف دورها في إعطاء نتيجة معينة [4]، و هو المنطق الذي إتبعه

---

(1)_ أنظر صفحة الأنترنت (مقال من أليكس باسكال *Pascal Alix* تحت عنوان : *L'accès ou le maintien non autorisé dans un système informatique*، www.net-iris.fr، 23 نوفمبر 2004) في العنوان التالي :
http://www.net-iris.com/publication/author/document.php3?document=342

(2)_ أنظر : Hollande Alain, De Bellefonds Linant Xavier, ***Op.cit***, page 251.

(3)_ كأن تكون المكونات المادية أو المعنوية التي تم المساس بها غير متصلة بالنظام المعلوماتي مباشرة.

(4)_ أنظر : André Lucas, Jean Devrèze, Jean Frayssinet, ***Op.cit***, page 680.

المشرع الجزائري من خلال ما جاء به في المادة 2 من القانون رقم 09-04 المؤرخ في 5 أوت 2009، في ما يخص إجبارية إنسجام مكونات النظام بهدف تحقيق نتيجة معينة :

" ... ب- منظومة معلوماتية : أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين، ... "[1].

وفقا لما سبق توضيحه ففي نظرنا إذا تم المساس بمكونات مادية معزولة أو معنوية معزولة و التي تعد جزء من النظام المعلوماتي : فإن القانون يمتد تطبيقه بالإضافة إلى التجريم الأصلي المتعلق بالدخول و البقاء الغير مشروع داخل النظام بواسطة المعلوماتية، إلى المساسات بالمكونات المادية خلافا عن القاعدة العامة، شريطة أن تكون لها علاقة مباشرة بالنظام المعلوماتي محل الحماية الجنائية، أما في ما يخص المكونات المعنوية فلا يشترط أن يؤدي المساس بها إلى الإضرار بالنظام المعلوماتي فمثلا : المساس بالمعطيات المعلوماتية يشكل جريمة سواء أدى ذلك إلى الإضرار بالنظام أم لا و دليل ذلك المادة 323-3 ق.ع.فرنسي و المادة 394 مكرر 1 ق.ع.جزائري التي لم تنص صراحة على أنه يجب أن يؤدي إدخال، حذف أو تعديل المعطيات إلى المساس أو الإضرار بالنظام المعلوماتي.

أيضا حتى تقوم الجريمة يجب أن يكون النظام المعلوماتي غريب عن مرتكب الجريمة أي ليس ملك له[2]، كما أن الدخول إلى مجموعة معلومات معلوماتية مخزنة والتي تم وقف معالجتها لا يمكن أن يدخل في حيز الحماية الجنائية، نفس الشيء بالنسبة للمساس بنقاط الحفظ ***"Les points de sauvegarde"*** التي تمثل مرحلة متجاوزة ***"Période Antérieur"*** أو قديمة لبرنامج المعالجة المعني بالحماية[3].

الفرع الثالث : تعريف المسؤول أو صاحب النظام المعلوماتي

مجلس الأمة الفرنسي وفقا لـــ : (ملف سنة 1987-1988، أول جلسة، رقم 1087) يعرف صاحب النظام المعلوماتي أو المسؤول ***"Le maître du système"*** "ككل شخص طبيعي أو معنوي، كل سلطة عمومية، أو مصلحة أو منظمة مختصة بالتصرف في النظام المعلوماتي أو تصمم تشكيلة هذا النظام ***"Sa conception"*** و كذا تنظيمه أو تصمم الهدف منه"[4].

---

(1)_ أنظر النص باللغة الفرنسية :

" ...
b - Système informatique : tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données.
...".

(2)_ أنظر : Hollande Alain, De Bellefonds Linant Xavier, ***Op.cit,*** page 251.

(3)_ أنظر : Hollande Alain, De Bellefonds Linant Xavier, ***Idem***.

(4)_ أنظر : André Lucas, Jean Devrèze, Jean Frayssinet, ***Op.cit***, page 690.

صاحب النظام المعلوماتي حسب هذا التعريف ليس بالضرورة مبتكره، أو الذي سمح بإستعماله، و بالتالي قد يكون الشخص الذي إكتسب عادة حق إستعماله سواء لأهداف شخصية أو للتجارة بالخدمات التي يقترحها أو إذا كان يستعمله لحساب الجهة المستخدمة له، إلا أنه لا يدخل في تعريف صاحب النظام المعلوماتي المستعمل العادي الذي ليس له أي مسؤولية أو أي حق شخصي ثابت على النظام المعلوماتي[1].

محاولة تحديد صاحب النظام المعلوماتي بمفهوم المسؤول عنه لحساب الغير لها أهمية كبرى إذ من جهة قد تثار مسؤوليته الجنائية، باعتباره مسؤول عنها لحساب جهة أخرى و يحتمل في بعض الأحيان أن تكون الجرائم المرتكبة ضد النظام خارجة عن إرادته[2].

من جهة أخرى تحديد صاحب النظام المعلوماتي بمفهوم المالك الأصلي لهذا النظام مهم لمعرفة الطرف المضرور في حالة إرتكاب جريمة ضد هذا النظام المعلوماتي، و هذا رأينا الشخصي.

الفرع الرابع : الأفعال المجرمة في القانون الجزائري و المقارن

الجرائم المتعلقة بالمساس بنظام المعلوماتية لم يتم تفريدها من طرف المشرع بصفة عامة على أساس تكييفات محددة[3]، إلا أنه بعد المقارنة بين التشريع الفرنسي و الجزائري في هذا المجال، يمكن إستنتاج 8 تصرفات مجرمة تدخل في صنف الجنح، و يمكن أن نلاحظ بأن المشرع بصفة عامة لم يعتد في هذه الجرائم بالقصد الجنائي الخاص أي الباعث في إرتكاب الجريمة بل إكتفى بتوافر القصد الجنائي العام حتى تكون هذه التصرفات محل عقوبة جزائية :

1 - الدخول أو البقاء في النظام المعلوماتي دون التأثير عليه (المادة 323-1 فقرة 1 ق.ع.فرنسي) و (المادة 394 مكرر فقرة 1 ق.ع.جزائري).
2 - الدخول أو البقاء في النظام المعلوماتي مع التأثير عليه (المادة 323-1 فقرة 2 ق.ع.فرنسي) و (المادة 394 مكرر فقرة 2 ق.ع.جزائري).
3 - جرائم المساس الإرادي بالسير العادي للنظام المعلوماتي بمعنى : الإعتراض أو التحريف للسير العادي النظام المعلوماتي (المادة 323-2 ق.ع.فرنسي) أما المشرع الجزائري فلم ينص عليها.
4 - الفعل الإجرامي في مجال المعطيات المعلوماتية (بمعنى إدخال معطيات بطريقة الغش، تعديلها أو حذفها من النظام) (المادة 323-3 ق.ع.فرنسي) و (المادة 394 مكرر 1 ق.ع.جزائري).

---

(1) _ أنظر : André Lucas, Jean Devrèze, Jean Frayssinet, ***Op.cit***, page 690.

(2) _ أنظر : André Lucas, Jean Devrèze, Jean Frayssinet, ***Ibid***, page 680.

(3) _ بقي المشرع نوعا ما غامضا و عاما بشأنها نظرا لنقص العديد من التوضيحات في ما يخص كيفية إرتكاب الجريمة و لسبب التقارب الموجود بين الجرائم المقررة في هذا القانون.

5 -الجرائم المتعلقة بالمعطيات التي يمكن أن تستعمل في سبيل المساس بالأنظمة المعلوماتية (المادة 323-3-1 ق.ع.فرنسي، المشرع الفرنسي حدد بدقة بأن وسيلة إرتكاب الجرائم المتعلقة بالنظام المعلوماتي قد تكون بواسطة معطيات معلوماتية "كما ذكره المشرع الجزائري" و أضاف وسائل أخرى بما فيها البرامج المعلوماتية و التجهيزات مهما كان نوعها وضعت أو أنشئت لإرتكاب الجرائم السالفة الذكر و بالتالي المشرع الفرنسي كان أكثر وضوحا في ما يخص الوسائل التي كان من الممكن إستعمالها لإرتكاب الجرائم ضد الأنظمة) و (المادة 394 مكرر 2 ق.ع.جزائري، المشرع الجزائري أضاف في الفقرة الأولى من نفس المادة جريمة تصميم المعطيات (مهما كان نوعها) و كذا جريمة الإتجار بهذه المعطيات التي يمكن أن تستعمل للمساس بالأنظمة المعلوماتية و في الفقرة الثانية من نفس المادة أضاف جريمة حيازة، إنشاء، نشر، أو إستعمال المعطيات المتحصل عليها من الجرائم المذكورة في القسم الخاص بالمساس بالأنظمة، كل هذه الجرائم التي وضعها المشرع الجزائري لم يذكرها المشرع الفرنسي في التعديل الأخير لقانونه).

6 -المشاركة في مجموعة مشكلة أو في إتفاق بهدف إرتكاب الجرائم سالفة الذكر (المادة 323-4 ق.ع.فرنسي) و (المادة 394 مكرر5 ق.ع.جزائري).

7 -إرتكاب جريمة المساس بالأنظمة المعلوماتية التابعة للدفاع الوطني أو الهيئات و المؤسسات الخاضعة للقانون العام (لم ينص عليها المشرع الفرنسي)، (المادة 394 مكرر 3 ق.ع.جزائري).

8 -إرتكاب جرائم المساس بالأنظمة المعلوماتية من طرف الشخص المعنوي (المادة 323-6 ق.ع.فرنسي) و (المادة 394 مكرر 4 ق.ع.جزائري).

و بالتالي يكون محل عقوبة الجرائم السالفة الذكر ضد النظام المعلوماتي كمحل للجريمة[1].

سندرس بالتفصيل الجرائم التي تمس بنظام المعالجة الآلية للمعطيات المعلوماتية أي النظام المعلوماتي و إن كانت غالبا أركانها غامضة، من المطلب الثاني إلى غاية المطلب السابع.

---

(1)_ ملاحظة هامة : ترتكب الجريمة المعلوماتية ضد النظام المعلوماتي أساسا بطريقتين، الأولى بالإتصال المادي ***Connexion matérielle*** مباشرة بالجهاز الحامل للنظام المعلوماتي المستهدف بالجريمة (كالكمبيوتر مثلا) أو بطريقة ثانية و هي الطريقة الأكثر إنتشار في عالم الإجرام المعلوماتي أي الإتصالات الإلكترونية عن بعد ***Connexions électroniques à distance*** التي عرفها المشرع الجزائري في المادة 2 تحت عنوان المصطلحات، من القانون رقم 09-04 لـــ 5 أوت 2009 كما يلي :

"... و- الإتصالات الإلكترونية : أي تراسل أو إرسال أو إستقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية ...".

« ... f - Communications électroniques : toute transmission, émission ou réception de signes, de signaux, d'écrits, d'images, de sons ou de renseignements de toute nature, par tout moyen électronique. ... ».

و بالتالي الجرائم المعلوماتية يمكن أن ترتكب بأي نوع من أنواع الإتصالات الإلكترونية سواء كانت سلكية أو لا سلكية و عبر أي نوع من أنوع الشبكات الإلكترونية أو المعلوماتية و بواسطة أي آلة أو جهاز أو منظومة تسمح أو تسهل إرتكاب مثل هذه.

المطلب الثاني : جريمة الدخول و البقاء الإحتيالي في الأنظمة المعلوماتية

في هذا المطلب سنتطرق إلى جريمتين أساسيتين للمساس بأنظمة المعالجة الآلية للمعطيات، و هي جريمة الدخول الإحتيالي إلى النظام ***"L'accès frauduleux dans un système"***، و جريمة البقاء الإحتيالي في النظام ***"Le maintien frauduleux dans un système"***، المواد 323-1 ق.ع.فرنسي و 394 مكرر ق.ع.جزائري.

هنالك نقطة أساسية يتعين توضيحها قبل دراسة هذه الجرائم كونها توضح بدقة المقصود بكل أو جزء من النظام المعلوماتي، بكل بساطة إذا دخل شخص في إحدى برامج النظام أي جزئ منه محمية تقنيا أم لا بهدف تعديله أو تحويل ***"Détourner"*** جزء منه لوظيفة أخرى فإن ذلك يشكل جريمة سواء كان ذلك البرنامج المعني يشارك أو لا يشارك في عملية أو وظيفة نشيطة وضعت من طرف نظام معلوماتي كامل مثلا : قاعدة برامج ***"Banque de programme"***، و بالتالي كقاعدة عامة إذا دخل شخص في جزء أو كل من نظام معلوماتي فإنه يعاقب جزائيا بنفس العقوبة المنصوص عليها في المواد 323-1 ق.ع.فرنسي و 394 مكرر ق.ع.جزائري.

الفرع الأول : جريمة الدخول الاحتيالي في الأنظمة المعلوماتية

قبل دراسة هذه الجريمة هنالك نقطتين كان لابد علينا من توضيحها و ذات أهمية بالغة :

المقصود من محاولة الدخول أو البقاء في النظام المعلوماتي : و هي الشروع في الجريمة لكن دون تحقيق نتيجة، و في هذه الحالة يعاقب المتهم بنفس العقوبة التي تقرر لمن تمكن من الدخول أو البقاء، و الشروع هنا يتمثل في جملة من العمليات و بدأ في تصرفات مادية (أي الركن المادي) التي يفهم من خلالها ذهاب نية المتهم إلى إرتكاب الجريمة و كذا توافر النية الجرمية أي الدخول أو البقاء من غير حق (أي الركن المعنوي) لكن لأسباب خارجة عن إرادته لا تتحقق الجريمة[1].

هل القيام بعملية مسح أو مراقبة نقاط الدخول إلى نظام معلوماتي ***"Le scan ou surveillance des ports ou points d'accès à un système informatique"*** يعد بمثابة جريمة محاولة الدخول إلى النظام ؟

نظرا لكون التكييف القانوني لفعل الدخول و البقاء في نظام معلوماتي جاء نوعا ما غامضا سواء في التشريع العقابي الفرنسي أو الجزائري، فإن ذلك قد يطرح في ما بعد بعض الصعوبات العملية في ما يخص الممارسة القضائية، إذ يمكن ملاحظة جملة من التصرفات عبر الشبكات المعلوماتية و التي تتقارب نوع ما مع

---

[1]_ أنظر : أحسن بوسقيعة، **مرجـــع سابـــق**، صفحة 91.

التصرفات المجرمة قانونا أي فعل الدخول أو البقاء، و من بين هذه التصرفات : عملية مسح أو مراقبة نقاط الدخول في نظام معلوماتي الذي في الأصل لا يعد حالة معروفة في النصوص التشريعية الحالية[1].

هذه العملية في الأصل يقوم بها المسؤولين عن الأنظمة المعلوماتية أو الأعوان التقنيين المكلفين بصيانتها بهدف الرقابة و ضمان سلامتها و مدى توافر الحماية التقنية الكافية لها من جل أنوع القرصنة، في هذه الحالة يعد التصرف في حد ذاته مشروع، غير أن الوضع قد يصبح غير ذلك في حالة القيام بعملية المسح و مراقبة نقاط الدخول في أي نظام من طرف الغير و من دون أي ترخيص من صاحب النظام و في أغلب الأحيان من طرف قراصنة المعلوماتية و بسوء نية، كعملية تحضيرية لهجمات معلوماتية على النظام المستهدف، وبالتالي هذا التصرف قد يدخل في نطاق تطبيق المواد العقابية بخصوص الدخول و البقاء في الأنظمة المعلوماتية[2].

هل أن عملية المسح أو مراقبة نقاط الدخول إلى نظام معلوماتي يعد بمثابة بداية لعملية تنفيذ ***"Le commencement d'exécution"*** لجريمة أو مجرد عمل تحضيري ***"Acte préparatoire"*** لها ؟

مبدئيا التفرقة بين الحالتين يعد نوعا ما غامضا، نظرا لكون الثانية غير معاقب عليها في حين أن الحالة الأولى تدخل في حيز تنفيذ قانون العقوبات و من تم المواد الجزائية الخاصة بجريمة المساس بالأنظمة المعلوماتية قابلة للتنفيذ تحت غطاء المحاولة في الجريمة[3].

و في نظر محكمة النقض الفرنسية، تكييف المحاولة في الجريمة هي مسألة قانونية بحتة و ليست بمسألة تقنية و بالتالي فهي تخضع لرقابة النصوص القانونية، كما إعتبرت بأن البدأ في عملية التنفيذهو[4] :

" تصرف يهدف أساسا إلى إرتكاب أو تسهيل إرتكاب جنحة عندما يكون قد تم بسوء نية أي بنية تحقيق هذه الجنحة "[5] [6].

و بالتالي هذا التعريف يحيلنا مباشرة إلى الركن المعنوي للجريمة أي وجوب توافر النية الجرمية.

---

(1)_ أنظر : Xavier LEMARTELEUR, ***« Le scan de port : une intrusion dans un STAD ? »***, Article de recherche édité sur le site Web : www.juriscom.net le 13/06/2008 à l'adresse : http://www.juriscom.net/pro/visu.php?ID=1074 ***(voir la page de présentation du sujet de recherche)***

(2)_ أنظر : Xavier LEMARTELEUR, ***Idem.***

(3)_ أنظر : مستند **(PDF)**، من المؤلف : Xavier LEMARTELEUR، تحت عنوان : ***« Le scan de port : une intrusion dans un STAD ? »***، المستنسخ من صفحة الأنترنت : http://www.juriscom.net/documents/priv20080613.pdf (Page 4)

(4)_ أنظر : مستند **(PDF) نفسه**، المستنسخ من صفحة الأنترنت : http://www.juriscom.net/documents/priv20080613.pdf ***idem***

(5)_ أنظر النص باللغة الفرنسية :
« L'acte qui tend directement au délit lorsqu'il a été accompli avec l'intention de le commettre ».

(6)_ أنظر : مستند **(PDF) نفسه**، المستنسخ من صفحة الأنترنت : http://www.juriscom.net/documents/priv20080613.pdf ***idem***

و تجدر الإشارة و أمام غياب إجتهادات قضائية جامعة و فاصلة فإن المسألة تبقى مفتوحة للمناقشة بين رجال القانون و المختصين في ميدان المعلوماتية.

و في نظر الفقيه الفرنسي كسافي لومارتلور ***"Xavier LEMARTELEUR"*** من خلال دراسته لهذه المسألة فإنه لا يعتقد بأن عملية المسح الآلي لنقاط الدخول في النظام تشكل تصرف غير مشروع يسمح بإتيان دليل وجود بداية تنفيذ جنحة، أما في ما يخص مسألة الركن المعنوي لجريمة المحاولة فإنه من الصعب إثباته، في حين أنها تكون قائمة في حالة الإثبات بأن المحتال المعلوماتي أو الهكرز قام بعملية المسح أو مراقبة نقاط الدخول في نظام معلوماتي بهدف الدخول فيه لاحقا[1].

في هذا الفرع سنوضح بأن القانون لا يعاقب بنفس الطريقة الدخول الإحتيالي الذي لا يترتب عنه نتائج سلبية أو تأثير ***"Sans influence"*** على نظام المعلوماتية و ذلك الدخول الذي يترتب عنه نتائج سلبية أو تأثير ***"Avec influence"*** على نظام المعلوماتية.

و تجدر الإشارة إلى أن الدخول الإحتيالي في نظام معلوماتي على عكس البقاء الإحتيالي يعد من الجرائم الآنية كمعظم الجرائم الأخرى إذ يتحقق في فترة زمنية محددة أي في لحظة الدخول الغير مشروع إلى النظام المعلوماتي[2].

الفقرة الأولى : جريمة الدخول الإحتيالي في الأنظمة المعلوماتية "دون التأثير عليها"

الجريمة المتعلقة بالدخول الإحتيالي دون التأثير على نظام المعلوماتية معاقب عليها بالمادة 323-1 فقرة 1 ق.ع.فرنسي و المادة 394 مكرر فقرة 1 ق.ع.جزائري.

حسب هذه المادتين فإن الدخول يعتبر مكون للجريمة إذا تم بطريقة أو مناورة إحتيالية (الغش) [3] و بطريقة عمدية و بالتالي الدخول الخطأ أو بالصدفة إلى النظام غير معاقب عليه، من جهة أخرى يجب أن يكون مرتكب الجريمة على علم بأنه دخل إلى النظام المعلوماتي بطريقة غير عادية أي أنه على علم بأن الدخول إلى هذا النظام ممنوع، و الجريمة لا تكون مؤسسة أمام القاضي الجزائي إلا بإثبات عملية الدخول إلى النظام[4].

و عليه فإن عملية الدخول في النظام المعلوماتي بإعتبارها مسألة تقنية بحتة، قد تتم بعدة طرق أهمها :

---

(1)_ أنظر : مستند (PDF) **نفسه**، المستنسخ من صفحة الأنترنت : ***Op.cit*** : http://www.juriscom.net/documents/priv20080613.pdf

(2)_ أنظر : أحسن بوسقيعة، **المرجـــع نفســـه**، صفحة 85.

(3)_ الغش هنا يقصد به : الدخول في النظام المعلوماتي مع العلم بأنه غير جائز أو مباح من طرف مالكها، و هنا قد يتم الدخول مثلا بعد التلاعب بوسائل الحماية التقنية لهذا النظام محل الجريمة.

(4)_ أنظر : Bensoussan Alain (sous la direction de), ***Op.cit***, page 108.

– الإتصال المادي المباشر بالنظام المعلوماتي ***"Connexion matérielle directe dans un système"*** :

و يقصد بها الدخول في النظام دون الحاجة إلى شبكة إتصال معلوماتية أو إلكترونية لتحقيق الجريمة أي أن الجاني موجود في نفس المكان الذي يوجد فيه النظام محل الجريمة و ما عليه في هذه الحالة إلا إجراء عمليات سواء مادية ***"Manipulations matériels"***، مثلا : إدخال دعامة مادية كالقرص المضغوط تحتوي على برنامج فك الرموز للدخول في النظام المعلوماتي المحمي تقنيا أو إزالة أو حذف عنصر مادي من الكمبيوتر محل الجريمة لتسهيل عملية الدخول في النظام، كما قد يتم الدخول في النظام بإجراء عمليات إلكترونية أو منطقية ***"Manipulations électronique ou logique"*** كالتلاعب في عين مكان النظام بمعطياته أو برامجه أو إجراء تعديلات فيها بهدف تسهيل عملية الدخول فيه.

– الإتصال المعنوي عن بعد بالنظام المعلوماتي ***"La connexion électronique ou logique à un système"*** :

و يقصد به الدخول في النظام المعلوماتي محل الجريمة بإستعمال وسائل الإتصال عن بعد المستحدثة (الشبكات المعلوماتية أو الإلكترونية السلكية أو اللاسلكية)، و في هذه الحالة لا يشترط حتى تقوم الجريمة أن يكون الجاني موجود في نفس مكان وجود الكمبيوتر محل الجريمة و هذا خلاف للحالة الأولى السالفة الذكر.

و تهدف كل من حالتي الإتصال بالنظام محل الجريمة القيام بتصرفات غير مشروعة من بينها :

– حالة إستعمال أو مناداة برنامج عن بعد أو قرب داخل النظام دون أي ترخيص أو من دون أي صلاحية.

– حالة إستجواب أو التطلع على محتوى معطيات معلوماتية موجودة في النظام من دون أي ترخيص أو صلاحية.

إذا في ما يخص الركن المادي للجريمة : فهو الدخول سواء كان مادي أو معنوي و بأي طريقة كانت إلى النظام المعلوماتي في جزء منه أو كله و دون أي حق أو ترخيص[1].

و تجدر الإشارة إلى أن القانون بصفة عامة لم يحدد على سبيل الحصر طرق الدخول الغير مشروع إلى النظام و بالتالي و بالإضافة إلى ما سبق ذكره فإن الدخول الغير مشروع إلى النظام يتم بمجرد الإتصال بهذا الأخير كما أن الدخول قد يتم بطريقة نشيطة ***"Active"*** : بواسطة القيام ببعض العمليات المعلوماتية ***"Manipulations informatiques"*** التي تسمح الدخول إلى النظام كالتعدي على مكنزم حماية النظام [2] أو إستعمال أرقام سرية تم الحصول عليها بطريقة غير مشروعة، من جهة أخرى قد يتم الدخول بطريقة غير نشيطة ***"Passive"*** : و مثال

---

[1]_ أنظر : جميل عبد الباقي الصغير، "**القانون الجنائي و التكنولوجيا الحديثة (الكتاب الأول : الجرائم الناشئة عن إستخدام الحاسب الآلي)**" (الطبعة الأولى)، دار النهضة العربية، ، طبعة 1992، القاهرة (مصر)، صفحة 150.

[2]_ في قرار صادر عن مجلس قضاء باريس غرفة الجنح في 5 أفريل 1994، إعتبر القاضي الجزائي بأن جريمة الدخول الغير مشروع في النظام المعلوماتي تعد قائمة حتى في حالة غياب نظام حماية لهذا الأخير و بالتالي مجرد الدخول من دون ترخيص يشكل جريمة و هذا وفقا لما سلف ذكره في ما يخص إشتراط أو عدم إشتراط توافر حماية تقنية للنظام المعلوماتي حتى تقوم الجريمة.

ذلك مجرد الإحساس ***"Perception"*** أو الإطلاع على معلومات صادرة عن النظام بواسطة دخول المجرم إلى شبكة الإتصال المعلوماتي ***"Le réseau de communication informatique"*** أو إقتطاع الإشعاعات ***"Captation des rayonnements"*** الصادرة عن الجهاز المكون للنظام المعلوماتي، و في كل من حالتي الدخول الركن المعنوي للجريمة أي النية الجرمية متوافرة، إلا أن المشرع لا يفرق في الجريمة بين الدخول بطريقة نشيطة أو غير نشيطة[1] و بالتالي لا يفرق القاضي بين الحالتين عند تقرير العقوبة، و هذا يعد في نظرنا غير عادي و كان لابد على المشرع تقرير عقوبات تختلف حسب الحالات.

في ما يخص الركن المعنوي للجريمة : فيكفي توافر القصد الجنائي العام أي أن الدخول إلى النظام يجب أن يكون إرادي[2] و ليس خطأ أو بالصدفة، إذا هذا التصرف يعد جريمة عمدية [3] و بالتالي الدخول الغير إرادي غير مجرم من طرف القانون، و يجب أن يكون المجرم على علم بأن دخوله إلى النظام غير مسموح به، حتى يتسنى معرفة توافر سوء النية لدى المجرم إذا كان دخوله إلى النظام نتيجة إختراق مكنزم حماية هذا الأخير مثلا[4]، و توافر نية الإضرار بالنظام غير ملزمة حتى تقوم الجريمة إذ لم يشترط المشرع قصد جنائي خاص.

و لا عبرة في هذه الجريمة بصفة مرتكبها فقد يكون الفاعل شخص مسؤول عن الجهاز أو مكلف بصيانته و قد يكون شخص آخر تمكن من الدخول إلى النظام عن طريق كمبيوتر آخر في مكان آخر بواسطة شبكة إتصال معلوماتية.

في ما يخص عقوبة الدخول إلى النظام دون التأثير عليها : في القانون الفرنسي هي سنتين حبس و 30 ألف € أما في القانون الجزائري فالعقوبة من 3 أشهر إلى سنة حبس و بغرامة من 50 ألف د.ج إلى 100 ألف د.ج، و بالتالي فإن المشرع الجزائري على غرار المشرع الفرنسي أعطى للقاضي الجزائي سلطة تقديرية أوسع في تقرير العقوبة المناسبة.

الفقرة الثانية : جريمة الدخول الإحتيالي في الأنظمة المعلوماتية "مع التأثير عليها"

الدخول إلى النظام المعلوماتي مع التأثير عليه معاقب عليه في المادة 323-1 فقرة 2 ق.ع.فرنسي و المادة 394 مكرر فقرة 2 ق.ع.جزائري، و تجدر الإشارة إلى أن التأثير السلبي على النظام المعلوماتي يعد ظرف مشدد للعقوبة.

---

(1)_أنظر : André Lucas, Devrèze Jean, Frayssinet Jean, ***Op.cit***, page 681.

(2)_ أنظر : André Lucas, Devrèze Jean, Frayssinet Jean, ***Ibid***, page 683.

(3)_ أنظر : جميل عبد الباقي الصغير، **مرجـــع سابـــق**، صفحة 151.

(4)_ أنظر : André Lucas, Devrèze Jean, Frayssinet Jean, ***Op.cit***, page 683.

المشرع الفرنسي فسر التأثير على النظام بأنه إما حذف أو تغيير المعطيات المحتواة فيه أو إفساد سير النظام أو تخريبه، أما المشرع الجزائري فلقد حصر تفسير التأثير بأنه تخريب نظام إشتغال المنظومة أو النظام المعلوماتي، و بالتالي إذا نتج عن الدخول الغير مشروع حذف أو تغيير معطيات المنظومة دون التأثير عليها فالقاضي الجزائي الجزائري حسب رأينا لا يعاقب عليه و في كل الأحوال يخضع الأمر إلى السلطة التقديرية للقاضي.

في ما يخص الركن المادي للجريمة : فهو نفس الركن المادي المقرر بالنسبة للدخول بدون التأثير على النظام المعلوماتي إلا أنه يضاف إليها في هذه الحالة التأثير على النظام المعلوماتي بمعنى إفساد أو تخريب ***"Altération"*** النظام المعلوماتي أو إنقاص من قدراته التقنية في المعالجة.

في ما يخص الركن المعنوي للجريمة : يكفي توافر القصد الجنائي العام و هو الدخول الإرادي و المتعمد إلى النظام مع العلم بأنه دخول غير مسموح به و نية الإضرار بالنظام ليست شرط أساسي لقيام الجريمة[1]، و إنما المهم هو تحقق النتيجة أي الإضرار بالنظام المعلوماتي، و بالتالي يكفي توافر القصد الجنائي العام حتى تقوم الجريمة.

في ما يخص عقوبة التأثير الغير إرادي على النظام الناتج عن الدخول الغير مشروع : فالمشرع الفرنسي حددها بـــ 3 سنوات حبس و 45 ألف € أما المشرع الجزائري فحددها بـــ 6 أشهر إلى سنتين حبس و الغرامة من 50 ألف د.ج إلى 150 ألف د.ج.

الفرع الثاني : جريمة البقاء الاحتيالي في الأنظمة المعلوماتية

البقاء الإحتيالي هو المرحلة التي تلي الدخول إلى النظام [2]، و نصت عليها كلا من المادة 323-1 فقرة 1 ق.ع.فرنسي و المادة 394 مكرر فقرة 1 ق.ع.جزائري.

من جهة أخرى جريمة البقاء الإحتيالي في النظام المعلوماتي تعد من الجرائم المستمرة، فالجريمة تستمر كلما زادة مدة البقاء الغير مشروع داخل النظام و بالتالي إستمرار الفعل الجرمي، و تكتمل الجريمة بإكتمال عملية البقاء الغير مشروع في النظام المعلوماتي[3].

---

(1)_ أنظر : André Lucas, Devrèze Jean, Frayssinet Jean, ***Op.cit***, page 683.

(2)_ إلا أن الدخول نوعين : قد يكون غير مشروع و قد يكون مشروع و رغم ذلك يعد البقاء غير مشروع كمن يدخل إلى شبكة الأنترنت أو النظام المعلوماتي بترخيص من صاحبها ليستعملها لمدة 30 دقيقة و بعد إنتهاء المدة، المستخدم للشبكة يستعمل طرق إحتيالية للبقاء لمدة زمنية تفوق الوقت المرخص له في ذلك.

(3)_ أنظر : أحسن بوسقيعة، **مرجـــع سابـــق**، من الصفحة 85 إلى 86.

و هنا سنتكلم عن البقاء الغير مشروع في النظام دون التأثير ***"Sans influence"*** أو مع التأثير عليها ***"Avec influence"*** حيث أن المشرع فرق بينهما من حيث العقوبة المقررة.

الفقرة الأولى : جريمة البقاء الإحتيالي في الأنظمة المعلوماتية "دون التأثير عليها"

البقاء في النظام المعلوماتي قد يكون ممنوع منعا باتا، و قد يكون غير مشروع إذا تعدى مستخدم النظام الوقت المرخص له من صاحبها للبقاء فيه و بالتالي قد يكون البقاء ناتج عن دخول شرعي إلى النظام أو غير شرعي، من جهة أخرى في ما يخص الركن المعنوي للجريمة : فيكفي توافر القصد الجنائي العام الذي إشترطه الإجتهاد القضائي الفرنسي حتى تقوم الجريمة أي يجب أن يكون مرتكب الجريمة قد كان يعلم بأن ليس له الحق أن يقوم بهذا التصرف أي البقاء و مع ذلك إرتكب الجريمة و بالتالي النية الجرمية متوافرة، حيث أن مجلس قضاء باريس (فرنسا) في إحدى قراراته إعتبر بأن الجريمة لا تقوم إذا كان مستغل النظام لا يعلم وجوب الحصول على ترخيص للدخول و البقاء في النظام[1].

في ما يخص الركن المادي للجريمة : بكل بساطة هو مجرد البقاء الفعلي فيه و حسب رئينا قد يقاس البقاء الغير مشروع بالمدة التي إستعمل فيها المجرم النظام، إذا تكتمل الجريمة مع إكتمال البقاء لمدة زمنية معينة، عكس ما هو الحال بالنسبة للدخول الغير مشروع في النظام.

و يمكن أن نعرف البقاء الإحتيالي في نظام المعلوماتية بأنه : "كل تواجد غير عادي كالإتصال بواسطة الشبكة المعلوماتية ***"Le réseau informatique"*** بالنظام المعلوماتي أي الدخول و النظر فيه أي في المعطيات التي يتضمنها، و غيرها من التصرفات الغير مسموح بها التي تشكل بدورها بقاء إحتيالي"[2].

عقوبة البقاء الإحتيالي دون التأثير على النظام : في المادة 323-1 فقرة 1 ق.ع.فرنسي هي سنتين حبس و 30 ألف € و في المادة 394 مكرر فقرة 1 ق.ع.جزائري هي الحبس من 3 أشهر إلى سنة و غرامة من 50 ألف د.ج إلى 100 ألف د.ج.

الفقرة الثانية : جريمة البقاء الإحتيالي في الأنظمة المعلوماتية "مع التأثير عليها"

لقيام جريمة البقاء الغير مشروع مع التأثير على النظام المعلوماتي، القضاء الفرنسي لم يشترط أن تتوافر لدى المجرم نية الإضرار بالنظام المعلوماتي بل يكفي أن تقوم بمجرد البقاء فقط إذا كان غير مشروع، أما إذا

---

[1] _ أنظر العنوان السالف الذكر في ما يخص إشتراط أو عدم إشتراط توافر حماية تقنية للنظام المعلوماتي حتى تقوم الجريمة.

[2] _ أنظر : Bensoussan Alain (sous la direction de), ***Op.cit***, Page 109.

تسبب المجرم زيادة على بقائه الغير مشروع في النظام إلى الإضرار بهذا الأخير فإن القاضي الجزائي يأخذها بعين الإعتبار على مستوى تقرير العقوبة و بالتالي الإضرار بالنظام يشكل ظرف مشدد للعقوبة[1].

في ما يخص الركن المعنوي للجريمة : فيكفي توافر القصد الجنائي العام حتى تقوم الجريمة دون شرط توافر القصد الجنائي الخاص، إذ أن مجرد حدوث تأثير و لو غير إرادي يكفي حتى تطبق الفقرة الثانية من المواد 323-1 ق.ع.فرنسي و 394 مكرر ق.ع.جزائري.

في ما يخص الركن المادي للجريمة : فهو نفس الركن المكون لجريمة البقاء الإحتيالي دون التأثير على النظام المعلوماتي[2]، حيث أن المشرع لم يفرق بين الدخول مع التأثير على النظام و البقاء مع التأثير عليها من خلال الفقرة 2 من المادتين 323-1 ق.ع.فرنسي و المادة 394 مكرر ق.ع.جزائري تطبق على الحالتين و بنفس العقوبة.

في ما يخص عقوبة البقاء الإحتيالي في النظام مع التأثير عليه : في المادة 323-1 فقرة 2 ق.ع.فرنسي هي 3 سنوات حبس و غرامة تقدر بـــ 45 ألف € و في المادة 394 مكرر فقرة 2 ق.ع.جزائري الحبس من 6 أشهر إلى سنتين و غرامة من 50 ألف د.ج إلى 150 ألف د.ج.

المطلب الثالث : جرائم المساس الإرادي بالسير العادي للأنظمة المعلوماتية

في هذا المطلب سنتعرض لجرائم المساس الإرادي بالسير العادي للأنظمة المعلوماتية أو ما يسمى في الفقه القانوني الفرنسي بجرائم إفساد سير الأنظمة المعلوماتية [3] ***"Altération du fonctionnement du système"*** التي تشمل جريمتي الإعتراض (أو عرقلة أو إعاقة أو تعطيل) سير النظام المعلوماتي و تحريف (أو تغيير) سير الأنظمة المعلوماتية ***"Fausser le fonctionnement du système"*** التي ذكرها المشرع الفرنسي في المادة 323-2 ق.ع.فرنسي، أما المشرع الجزائري فلم يتطرق لهذه الجرائم و هنا يثار التساؤل حول عدم نصه عليها بإعتبار أن هاتين الجريمتين من الجرائم الأساسية المرتكبة ضد الأنظمة المعلوماتية ؟

الفرع الأول : جريمة الاعتراض للسير العادي للأنظمة المعلوماتية

يتعلق الأمر هنا بفعل إجرامي مستقل عن الجرائم السالفة الذكر حتى و إن كان في أغلب الأحيان يأتي في مرحلة لاحقة للدخول الإحتيالي في النظام المعلوماتي و أثناء مرحلة البقاء فيه.

---

(1)_ أنظر : André Lucas, Devrèze Jean, Frayssinet Jean, ***Op.cit***, de la page 683 à 684.

(2)_ أنظر : Bensoussan Alain (sous la direction de), ***Op.cit***, page 109.

(3)_ جريمة إفساد سير النظام المعلوماتي هي مرحلة لاحقة للدخول في النظام سواء كان هذا الدخول مشروع أو غير مشروع، و تتم أثناء البقاء في النظام سواء كان هذا البقاء مشروع أو غير مشروع.

في ما يخص الركن المادي للجريمة : يتمثل في تقنية الإعتراض ***"L'entrave"*** و هو نوع آخر من أنواع المساسات بالنظام المعلوماتي، إلا أن الإشكال الأساسي هنا هو تحديد بدقة المقصود بالإعتراض في نظر المشرع إذ المصطلح ذاته له مفهوم واسع و بالتالي يكفي أن يكون هنالك تأثير سلبي ***"Influence négative"*** على النظام حتى يكون مصطلح الإعتراض قابل للتوظيف في هذه الحالة [1]، و بالتالي فعل الإعتراض قد يشمل : تحطيم المكونات المادية للنظام المعلوماتي، إستعمال الفيروسات، إستعمال القنابل المنطقية، تغيير الرموز أو الأرقام السرية للنظام المعلوماتي، إحتلال جزء كبير من ذاكرة الكمبيوتر، لتحقيق إحدى الهدفين : تعطيل أو تأخير إستعمال النظام أو منع إستعماله لمدة أو لحظة محددة أو غير محددة[2]، و بالتالي يمكن أن نقول بأن جريمة الإعتراض من الجرائم المستمرة إذا كان الإعتراض يطول من حيث الزمن، و من بين الآثار السلبية التي قد تنتج عن فعل الإعتراض : هو التوقيف كلي أو جزئي للنظام، عدم إمكانية إستعمال النظام أو وجود إنقاص جذري أو كلي لقدراته الآلية أو العلاجية للمعطيات، و تجدر الإشارة كما سلف ذكره إلى أن الإعتراض قد يكون دائم ***"Entrave permanente"*** أي لمدة غير محددة كما هو الحال بالنسبة لتحطيم البرنامج الأساسي في النظام المعلوماتي بموجب فيروس فهنا الضرر ضرر دائم، كما قد يكون الإعتراض دوري ***"Entrave périodique"*** كما هو الحال بالنسبة لإدخال نوع من الفيروسات التي تعترض للنظام بصفة دورية.

في ما يخص الركن المعنوي للجريمة : فهو الفعل الإحتيالي الإرادي و المتعمد ضد ملك الغير أي القصد الجنائي العام بمعنى أن الشخص يعلم بأن هذا التصرف محضور و مع ذلك يقدم على إرتكابه، و يتمثل هذا التصرف في منع السير العادي للنظام أو تعطيل أو تأخير إستعماله، أو إعاقته، و بصفة عامة هذا النوع من الجرائم يتم بطريقة إيجابية، غير أن محكمة النقض الفرنسية في سنة 1996 إعتبرت بأن الإعتراض يمكن أن يتم بطريقة غير إيجابية أو غير مباشرة (الحياد أو الإمتناع) ***"Abstention ou neutralité"***، في هذه الحالة إشترطت محكمة النقض حتى تقوم الجريمة أن يكون هذا التصرف أي الإمتناع واقع على السير العادي للنظام المعلوماتي و الذي يؤدي فيما بعد إلى إحداث إضطرابات ***"Perturbations"*** فيه[3] و توافر نية الإضرار بالنظام مع العلم بأن ذلك التصرف غير مشروع و بالتالي الخطأ الغير متعمد لا يشكل جريمة.

و التجريم المتعلق بالإعتراض للنظام المعلوماتي لا يطبق في حالة إضراب الموظفين المختصين في المعلوماتية بإعتباره نوع آخر من الإضطرابات و الإعتراضات التي قد تمس بالسير العادي للنظام[4].

---

(1)_ أنظر : Bensoussan Alain (sous la direction de), ***Op.cit***, page 109.

(2)_ أنظر : André Lucas, Devrèze Jean, Frayssinet Jean, ***Op.cit***, page 685.

(3)_ أنظر : André Lucas, Devrèze Jean, Frayssinet Jean, ***Op.cit***, de la page 684 à 685.

(4)_ أنظر : X. Linant de Bellefonds, A. Hollande, ***Droit de l'Informatique et de la Télématique***, Encyclopédie Delmas pour la vie des affaires, édition J. Delmas et Cie, 2ème édition, 01 décembre 1997, (France), page 102.

في ما يخص عقوبة الإعتراض للنظام المعلوماتي : فهي 5 سنوات حبس و 75 ألف € غرامة حسب المادة 323-2 ق.ع.فرنسي، أما المشرع الجزائري فلم ينص على هذه الجريمة في قانون العقوبات.

الفرع الثاني : جريمة تحريف سير الأنظمة المعلوماتية

الغموض الذي يشمل مصطلح الإعتراض هو نفس الغموض الذي ورد في المصطلح الثاني المستعمل من طرف المشرع الفرنسي أي تحريف سير النظام المعلوماتي ***"Fausser le fonctionnement du système de traitement automatisé"*** [1].

و يمكن القول بأن هذه الجريمة مشتركة مع جريمة الإعتراض لسير النظام المعلوماتي، و في ما يخص الركن المعنوي للجريمة : فهو نفس الركن المعنوي المكون لجريمة الإعتراض لسير النظام المعلوماتي[2].

أما في ما يخص الركن المادي للجريمة : فهو إفساد سير النظام المعلوماتي معبر عليه في نص المادة 323-2 ق.ع.فرنسي بتحريف سير نظام المعالجة الآلية للمعطيات[3].

و تجدر الإشارة كما سبق ذكره في مقدمة هذا المطلب إلى أن إفساد سير النظام المعلوماتي ***"Altération du fonctionnement du système"*** يشمل جريمتي الإعتراض و تحريف السير العادي للنظام المعلوماتي : و بالتالي الهدف الأساسي من جريمة الإعتراض كما سبق ذكره هو تعطيل ***"Ralentir"*** أو تأخير ***"Retarder"*** أو منع ***"Empêcher"*** أو العرقلة ***"Sabotage"*** بطريقة مؤقتة أو دائمة لسير النظام المعلوماتي[4]، أما الهدف الأساسي من جريمة التحريف لسير النظام المعلوماتي هو التشويه ***"Déformation"*** المتعلق بنتائج المعالجة الآلية أو تعديل دور برامج النظام الذي بفعل هذا المساس يؤدي إلى إعطاء نتائج أخرى مختلفة عن ما كان سيعطيه النظام المعلوماتي في حالة السير العادي[5]، و تجدر الإشارة إلى أن التحريف المعلوماتي قد يكون هو الآخر دائم أو مؤقت و بالتالي يمكن أن نقول بأن جريمة التحريف من الجرائم المستمرة إذا كان هذا التحريف يطول من حيث الزمن و بالتالي تكتمل الجريمة بإكتمال فعل التحريف.

من جهة أخرى يقصد بإفساد سير النظام المعلوماتي هو تغيير حالة السير العادي للنظام أي التأثير السلبي على البرامج و المعطيات الموجودة داخل النظام و التي تعد جزء منه.

---

(1) _ أنظر : André Lucas Devrèze Jean, Frayssinet Jean, ***Op.cit***, page 684.

(2) _ أنظر : Bensoussan Alain (sous la direction de), ***Op.cit***, de la page 109 à 110.

(3) _ أنظر : Bensoussan Alain (sous la direction de), ***Idem***.

(4) _ أنظر : Bensoussan Alain (sous la direction de), ***Idem***.

(5) _ أنظر : André Lucas, Devrèze Jean, Frayssinet Jean, ***Op.cit***, page 685.

و بالتالي منع النداء إلى برنامج داخل النظام المعلوماتي أو التمكن من قراءة تعليمات أو معطيات آمرة في النظام يمكن أن يؤدي إلى إفساد السير العادي للنظام أي تحريف السير العادي للنظام و منعه من تحقيق هدفه و كذا تحريف النتائج الناجمة عن المعالجة الآلية التي قام بها هذا النظام[1].

أخيرا، يمكن أن يتم إفساد سير النظام المعلوماتي من خلال إفساد إحدى مكوناته، مثلا : المساس بشبكة الإتصال المعلوماتي من خلال الإعتراض له أو تحريفه بإعتباره نظام معلوماتي في حد ذاته[2].

في هذا الصدد القضاء الجزائي الفرنسي سنة 2003 فصل في قضية شركة توزيع الخدمات التلفزية عبر شبكة الأنترنت ***"NOOS"*** ضد فيليب ***"Philippe"*** على أساس جريمة المساس الغير مشروع بالنظام المعلوماتي للشركة (موقع الأنترنت التابع للشركة)[3] و التأثير عليها بواسطة قنبلتها أو الإرسال إلى نظامها رسائل إلكترونية ***"e-Mails"*** بكثافة ***"Le mail-bombing"*** [4] بهدف إفساد السير العادي للنظام أي الإعتراض، و هنا تعرض مرتكب الجريمة إلى عقوبة 4 أشهر حبس و غرامة تقدر بـــ 20 ألف €، كما فصلت محكمة جزائية فرنسية في قضية غش معلوماتي في مجال شبكات الإتصال الهاتفي للنقالات ***"Radiotéléphones Mobiles"***، المتهمين في هذه القضية تمت محاكمتهم على أساس التحريف الإرادي لنظام إستغلال معلوماتي لشبكة ***"RADIO 2000"*** إحتكارا لحقوق الغير[5].

في ما يخص العقوبة المقررة لجريمة تحريف سير النظام المعلوماتي فهي نفس العقوبة لجريمة الإعتراض للنظام المعلوماتي و التي تنظمها المادة 323 مكرر 2 ق.ع.فرنسي.

المطلب الرابع : الفعل الإجرامي في مجال المعطيات المعلوماتية

موضوع الفعل الإجرامي في مجال المعطيات المعلوماتية ***"Les données informatiques"*** يعد مجال واسع لسبب بسيط هو أن معظم الجرائم في مجال الغش المعلوماتي متعلقة بهذه المكونات التي تعد جزء مهم من النظام المعلوماتي، من جهة أخرى فإنه من الصعب التفرقة بين الجرائم المتعلقة بالمعطيات المعلوماتية و الجرائم المتعلقة بالمساسات الإرادية بالسير العادي للنظم المعلوماتية ***"Les atteintes volontaires au fonctionnement des systèmes"*** التي نص عليها المشرع الفرنسي وحده و التي سبق و أن درسناها، إذ أنه يمكن المساس بالسير

---

(1)_ أنظر : Bensoussan Alain (sous la direction de), ***Op.cit***, de Page 109 à 110.

(2)_ أنظر : Bensoussan Alain (sous la direction de), ***Idem***.

(3)_ إستعمال الرسائل المقنبلة (أي بكثافة) ***"Mail-bombing"*** يعد نوع من أنواع الإعتراض للنظام المعلوماتي.

(4)_ برنامج ***"Mail-bombing"*** يكمن دوره في إرسال عدد هائل من الرسائل الإلكترونية بهدف إفساد البريد الإلكتروني و إحداث عطب فيه.

(5)_ أنظر : Bensoussan Alain (sous la direction de), ***Op.cit***, de Page 109 à 110.

العادي للنظام المعلوماتي من خلال المساس بالمعطيات الموجودة فيه [1]، و بالتالي السؤال الذي يمكن طرحه هو : لماذا المشرع الفرنسي لم يدمج الجرائم المتصلة بالمعطيات المعلوماتية و جرائم إفساد السير العادي للنظام المعلوماتي (أي الإعتراض و تحريف سير النظام) في مادة واحدة بإعتبار أن المساس بالمعطيات يؤدي هو الآخر إلى المساس بالنظام المعلوماتي و العكس صحيح ؟

المشرع الفرنسي لم يدمجهما معا في مادة واحدة لأنه في بعض الأحيان قد لا يؤدي المساس بالمعطيات المعلوماتية إلى المساس حتما بالسير العادي للنظام و هذا ما يجعلنا نفرق بين المعطيات المهمة للسير العادي للنظام كمعطيات النظام ***"Les fichiers systèmes"*** و المعطيات الثانوية.

في هذا المطلب سنتكلم عن جرائم إدخال معطيات معلوماتية بطريقة الغش إلى نظام معلوماتي أو حذفها منه أو تعديلها بطريقة الغش من خلال تحليل المواد 323-3 ق.ع.فرنسي و 394 مكرر 1 ق.ع.جزائري، ثم سنتكلم دائما في مجال الإجرام المتعلق بالمعطيات المعلوماتية عن الجرائم الأخرى المرتبطة بها من خلال تحليل المواد 323-3-1 ق.ع.فرنسي و 394 مكرر 2 ق.ع.جزائري.

الفرع الأول : تعريف المعطيات المعلوماتية و طبيعتها القانونية

المشرع الجزائري مؤخرا و على خلاف زميله الفرنسي فإنه أعطى تعريف للمعطيات المعلوماتية من خلال مقتضيات المادة 2 فقرة (ج) من القانون 09-04 لـــ 5 أوت 2009 كما يلي :

" ...

ج- معطيات معلوماتية : أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها.

... "[2].

و بالتالي يدخل في حكم معطيات معلوماتية أي معلومة مهما كانت طبيعتها بشرط أن تكون في شكل معلوماتي أو إلكتروني و التي قد تلعب دور مهم في تشغيل منظومة معلوماتية.

---

[1] _ أنظر : André Lucas, Devrèze Jean, Frayssinet Jean, ***Op.cit***, Page 686.

[2] _ أنظر النص بالغة الفرنسية :

« ...

C- Données informatiques : 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.

... ».

في ما يخص الطبيعة القانونية للمعطيات المعلوماتية و بما أن المشرع سواء الفرنسي أو الجزائري إعتبر النظام المعلوماتي مال من خلال تجريم المساس به في قسم الجرائم ضد الأموال فإن إعتبار المعطيات المعلوماتية بدورها بأنها مال يعد منطقي بإعتبارها جزء لا يتجزئ من النظام المعلوماتي كما أنها عنصر أساسي فيه ***"Eléments essentiels du système"***.

الفرع الثاني : الفعل الإجرامي ضد المعطيات المعلوماتية

يتجلى الفعل الإجرامي أساسا في المساس بإستقرار المعطيات و ما لها من خاصية الوجود المنطقي أي في صورة إلكترونية و في هذا المجال يمكن أن نفرق بين نوعين من التصرفات الماسة بها أي الحذف أو التعديل.

في هذا الفرع سنتكلم عن جريمتي حذف و تعديل المعطيات المعلوماتية المنصوص عليها في المادة 323-3 ق.ع.فرنسي و المادة 394 مكرر 1 ق.ع.جزائري.

الفقرة الأولى : جريمة حذف المعطيات المعلوماتية

يفهم من هذه الجريمة أن مجرد حذف بطريقة إحتيالية معطيات معلوماتية سواء كانت في شكل معطيات، بيانات، أو برامج معلوماتية أو كل ما له وجود منطقي في النظام المعلوماتي معاقب عليه قانونا.

في ما يخص الركن المعنوي للجريمة : يكفي توافر القصد الجنائي العام إذ يجب أن يكون هذا التصرف الغير مشروع إرادي أي توافر النية الجرمية بمعنى الإضرار بالمعطيات المعلوماتية الموجودة في النظام المعلوماتي المملوك للغير و مع العلم بأن ذلك غير مسموح به، و هنا المشرع لم يشترط قصد جنائي خاص[1].

في ما يخص الركن المادي للجريمة : فإنه يتوافر بمجرد وجود تأثير سلبي ***"Une Influence négatif"*** على المعطيات المعلوماتية المتمثل في حذفها ***"Suppression"*** من النظام المعلوماتي، و هذا مهما كانت أهمية هذه المعطيات داخل النظام و مهما كانت وضعية النظام ***"L'état du système"*** جيدة أو سيئة[2]، و مهما كان نوع هذه المعطيات المحذوفة، و مهما كانت النتائج المترتبة عن هذا الحذف لهذه المعطيات من النظام، و تجدر الإشارة إلى أنه في أغلب الأحيان المساس بالمعطيات المعلوماتية (حذفها) يعد في كل الأحوال مساس بالسير العادي للنظام المعلوماتي[3].

---

(1)_ أنظر : جميل عبد الباقي الصغير، **مرجـــع سابـــق**، صفحة 160.

(2)_ أنظر : Bensoussan Alain (sous la direction de), ***Op.cit***, de Page 111.

(3)_ أنظر : X. Linant de Bellefonds, A. Hollande, ***Op.cit***, Page 103.

في ما يخص عقوبة حذف المعطيات المعلوماتية : هي 5 سنوات حبس و غرامة قدرها 75 ألف € حسب المادة 323-3 ق.ع.فرنسي، و من 6 أشهر إلى 3 سنوات حبس و غرامة من 500 ألف د.ج إلى 2 مليون د.ج حسب المادة 394 مكرر 1 ق.ع.جزائري.

الفقرة الثانية : جريمة تعديل المعطيات المعلوماتية

يفهم من هذه الجريمة على خلاف الجريمة السابقة هو التعديل بطريقة إحتيالية معطيات معلوماتية سواء كانت معطيات، بيانات، أو برامج معلوماتية أو كل ما له وجود منطقي في النظام المعلوماتي معاقب عليها قانونا.

في ما يخص الركن المعنوي للجريمة : وهو نفس الركن المعنوي المذكور في جريمة حذف المعطيات المعلوماتية.

في ما يخص الركن المادي للجريمة : و كما هو الحال في الجريمة السالفة الذكر، تقوم الجريمة بمجرد وجود تأثير سلبي على المعطيات المعلوماتية المتمثل في تعديلها ***"Modification"***، و هذا مهما كانت أهمية هذه المعطيات داخل النظام و مهما كانت وضعية النظام جيدة أو سيئة، و مهما كان نوع هذه المعطيات المعدلة، و مهما كانت النتائج المترتبة عن هذا التعديل للمعطيات على النظام.

و تجدر الإشارة كما سلف ذكره إلى أن المساس بالمعطيات المعلوماتية (تعديلها) يعد في كل الأحوال مساس بالسير العادي للنظام المعلوماتي كما هو الحال في حالة حذفها.

إلا أن الإشكال الذي يطرح في هذه الجريمة يدور حول عملية التعديل للمعطيات و المقصود منها : هو تغيير الحالة التي كانت عليها في الأصل، وفي ما يخص طرق التعديل فلم يحددها المشرع و بصفة عامة لا تهم الطريقة المستعملة لتعديل هذه المعطيات و إنما المهم هو تحقق النتيجة أي تغيير الحالة الأصلية التي كانت عليها هذه المعطيات، كما لا يهم مثلما سبق ذكره نوع هذه المعطيات التي تم المساس بها.

في ما يخص عقوبة تعديل المعطيات المعلوماتية : فهي نفس العقوبة المقررة في حالة حذف المعطيات المعلوماتية.

الفرع الثالث : الفعل الإجرامي ضد الأنظمة المعلوماتية بواسطة المعطيات المعلوماتية

و يقصد به حسب المواد 323-3 ق.ع.فرنسي و 394 مكرر 1 ق.ع.جزائري : جريمة إدخال بطريقة الغش معطيات معلوماتية في النظام المعلوماتي.

في ما يخص الركن المعنوي للجريمة : أي القصد الجنائي العام فإن النية الجرمية تتشكل منذ لحظة إدخال إراديا معطيات معلوماتية داخل النظام المعلوماتي محل الجريمة[1] مع العلم بأن ذلك غير مسموح به من طرف صاحب النظام، و لا يشترط في هذه الجريمة كما هو الحال في الجرائم السالفة الذكر توافر قصد جنائي خاص.

في ما يخص الركن المادي للجريمة : بكل بساطة هو مجرد إدخال معطيات معلوماتية مهما كان نوعها (مثلا : فيروس معلوماتي أو مستندات أو بيانات أو برامج) في النظام المعلوماتي محل الجريمة و مهما كانت حالة النظام عند إدخال هذه المعطيات و مهما كانت النتائج المترتبة عن ذلك، إذ لم يشترط المشرع أن يترتب عن هذا الإدخال للمعطيات تأثير على النظام[2].

في ما يخص عقوبة إدخال معطيات معلوماتية : فهي نفس العقوبة المقررة للجريمتين سالفتي الذكر.

الفرع الرابع : جرائم المواد 323-3-1 ق.ع.فرنسي و 394 مكرر 2 ق.ع.جزائري

من خلال إجراء دراسة للقانون الجزائري في موضوع المساس بأنظمة المعالجة الآلية للمعطيات مقارنة بالقانون الفرنسي الأسبق في هذا المجال، أي المادة 394 مكرر 2 ق.ع.جزائري و المادة 323-3-1 ق.ع.فرنسي، فإننا يمكن أن نلاحظ جملة من أوجه الشبه و كذا بعض الإختلافات من خلال دراسة 4 فئات من الجرائم المتعلقة بالمعطيات المعلوماتية المقرصنة.

الفقرة الأولى : جريمة تصميم معطيات معلوماتية مقرصنة

نصت عليها أيضا الفقرة الأولى من المادة 394 مكرر 2 ق.ع.جزائري، أما المشرع الفرنسي فلم ينص عليها.

تتمثل جريمة التصميم ***"Conception"*** لمعطيات معلوماتية مقرصنة في برمجتها ***"Sa programmation"*** بواسطة المعلوماتية أي الكمبيوتر و مثال ذلك : الفيروسات المعلوماتية، برامج القرصنة التي يمكن أن تستعمل في إرتكاب جرائم معلوماتية إما ضد الأنظمة المعلوماتية أو المعطيات المعلوماتية في حد ذاتها.

من جهة أخرى يقصد بالمعطيات المعلوماتية المقرصنة : هي المعطيات في شتى أنواها (معطيات أو بيانات ***"Données"***، مستندات ***"Documents"***، برامج ***"Programmes"***)، و دورها الأساسي هو الإضرار بالأنظمة أو المعطيات المعلوماتية، إذا فهي تتمتع بخاصية الإضرار بالأنظمة المعلوماتية.

---

(1) _ أنظر : Bensoussan Alain (sous la direction de), ***Op.cit***, de Page 111 à 112.

(2) _ أنظر : Bensoussan Alain (sous la direction de), ***Idem***.

في ما يخص الركن المعنوي للجريمة : أي القصد الجنائي العام يتمثل في توافر النية الجرمية المتمثل في التصميم الإرادي لمعطيات مقرصنة، أي إرتكاب الجريمة عمدا مع العلم بأن ذلك غير مسموح به، و لا يشترط توافر القصد الجنائي الخاص لقيام الجريمة.

في ما يخص الركن المادي للجريمة : هو قيام المجرم بعملية تصميم هذه المعطيات المقرصنة، ففي ما يخص كيفية تصميمها فلم يشترط المشرع الجزائري طريقة معينة، كما لم يشترط إستعمال هذه المعطيات في جرائم أخرى، و لكن يشترط أن تكون وسيلة بإمكانها المساس سواء بالأنظمة (المادة 394 مكرر ق.ع.جزائري) أو المعطيات المعلوماتية السليمة (المادة 394 مكرر1 ق.ع.جزائري).

في ما يخص عقوبة تصميم المعطيات المعلوماتية المقرصنة : فلقد نصت عليها المادة 394 مكرر 2 ق.ع.جزائري أي الحبس من شهرين إلى 3 سنوات و غرامة تتراوح بين مليون د.ج و 5 ملايين د.ج.

الفقرة الثانية : جريمة بحث أو تجميع معطيات معلوماتية مقرصنة

نصت عليها أيضا الفقرة الأولى من المادة 394 مكرر 2 ق.ع.جزائري و المادة 323-3-1 ق.ع.فرنسي.

في ما يخص الركن المعنوي للجريمة : أي القصد الجنائي العام فيتمثل في توافر النية الجرمية بمعنى بحث أو تجميع معطيات معلوماتية مقرصنة، وبالتالي هذه التصرفات تتم بطريقة عمدية و رغم علم المجرم بأنها غير مشروعة، و لا يشترط توافر القصد الجنائي الخاص.

في ما يخص الركن المادي للجريمة : و هو قيام المجرم بعملية بحث أو إستوراد ***"Recherche ou importation"*** عبر شبكات الإتصال المعلوماتية أو أي مصدر آخر، أو تجميع ***"Réunir ou rassembler et détenir"*** معطيات معلوماتية مقرصنة، من الممكن إستعمالها للمساس بالأنظمة أو المعطيات المعلوماتية السليمة، فإذا كانت هذه المعطيات لا تشكل ضرر على الأنظمة أو المعطيات المعلوماتية فلا تقوم الجريمة و هذه القاعدة تطبق على الجرائم المنصوص عليها في المواد 394 مكرر 2 فقرة 1 ق.ع.جزائري و 323-3-1 ق.ع.فرنسي.

و عموما البحث و تجميع المعطيات المعلوماتية المقرصنة يتم في أغلب الأحيان عبر شبكة الأنترنت من خلال عملية الإستنساخ ***"Le Téléchargement"***.

في ما يخص عقوبة هذه الجريمة : فتتمثل في الحبس من شهرين إلى 3 سنوات و غرامة تتراوح بين مليون د.ج و 5 ملايين د.ج حسب المادة 394 مكرر 2 ق.ع.جزائري، أما في القانون الفرنسي فالمشرع لم يحدد بدقة العقوبة المقررة في هذه الحالة و بالتالي السلطة التقديرية تعود إلى القاضي الجزائي حسب المادة 323-3-1 ق.ع.فرنسي مع إمكانية تشديد العقوبة.

الفقرة الثالثة : جريمة توفير أو نشر معطيات معلوماتية مقرصنة

نصت عليها أيضا الفقرة الأولى من المادة 394 مكرر 2 ق.ع.جزائري و المادة 323-3-1 ق.ع.فرنسي.

في ما يخص الركن المعنوي للجريمة : أي القصد الجنائي العام و كما سبق ذكره في الجرائم السالفة الذكر يتمثل في توافر النية الجرمية من خلال التصرف المادي أي توفير أو نشر معطيات معلوماتية مقرصنة، وبالتالي هذه التصرفات تتم بطريقة عمدية و رغم علم المجرم بأن هذه التصرفات غير مشروعة، ولا يشترط توافر قصد جنائي خاص.

في ما يخص الركن المادي للجريمة : و هو قيام المجرم بعملية توفير أو نشر***"Offrir, céder, mettre à disposition ou diffusion"*** معطيات معلوماتية مقرصنة، من الممكن إستعمالها للمساس بالأنظمة أو المعطيات المعلوماتية السليمة، فإذا كانت هذه المعطيات لا تشكل خطر على سلامة الأنظمة أو المعطيات المعلوماتية فلا تقوم الجريمة.

و عموما تتم عملية النشر أو التوفير عبر شبكة الأنترنت و في أغلب الأحيان من خلال عرض على جمهور الأنترنت هذه المعطيات المجرمة سواء من خلال تثبيتها في مواقع أو صفحات الأنترنت قابلة للإستنساخ أو نشرها أيضا عن طريق البريد الإلكتروني أو عن طريق برامج الإستنساخ بين الخواص ***"Peet to peer"***.

في ما يخص عقوبة هذه الجريمة : فهي نفس العقوبة المقررة بالنسبة للجريمة السالفة الذكر مع إمكانية تقرير عقوبة أشد في ما يخص التشريع الفرنسي.

في ما يخص الجرائم السالفة الذكر المشرع الفرنسي على عكس المشرع الجزائري عندما تكلم عن هذه المعطيات التي يمكن أن تستعمل في جريمة معلوماتية أخرى فإنه وسع تعريفها إلى كل وسيلة سواء كانت تجهيز ***"Equipement"*** أو آلة ***"Instrument"*** أو برنامج معلوماتي ***"Programme informatique"*** أو أي معطيات أنشأت لإرتكاب إحدى جرائم المساس بالأنظمة أو المعطيات المعلوماتية، إذا الوسيلة قد تكون مادية أو معنوية أما المشرع الجزائري فحصرها في مصطلح معطيات معلوماتية فقط أي وسيلة معنوية و بالتالي كان على المشرع الوطني إستدراك هذا الفراغ القانوني بإتباع الصياغة التي جاء بها المشرع الفرنسي بإعتبارها أشمل.

الفقرة الرابعة : الجرائم المتعلقة بالمعطيات المعلوماتية المتحصل عليها من إحدى الجرائم الماسة بالأنظمة المعلوماتية

بكل بساطة و حسب الحالات التي ذكرتها المادة 394 مكرر 2 فقرة 2 هي حيازة ***"Détenir"***، إفشاء ***"révéler"***، نشر ***"Divulguer"***، أو إستعمال ***"Utiliser"*** المعطيات المعلوماتية المتحصل عليها من إحدى الجرائم المنصوص

عليها في القسم الخاص بالمساس بأنظمة المعالجة الآلية للمعطيات، و تجدر الإشارة إلى أن المشرع الفرنسي لم ينص على هذه الجرائم.

في ما يخص الركن المعنوي للجريمة : أي القصد الجنائي العام و كما سبق ذكره في الجرائم السالفة الذكر يتمثل في توافر النية الجرمية المتمثلة هذه المرة في حيازة، إفشاء، نشر، أو إستعمال المعطيات المعلوماتية المتحصل عليها من إحدى الجرائم المنصوص عليها في القسم الخاص بالمساس بأنظمة المعالجة الآلية للمعطيات، وبالتالي هذه التصرفات تتم بطريقة عمدية و رغم علم المجرم بأن ذلك غير مشروع دون شرط توافر قصد جنائي خاص من الجريمة.

في ما يخص الركن المادي للجريمة : فيتمثل في قيام المجرم بعملية حيازة، إفشاء، نشر أو إفشاء، أو إستعمال المعطيات المعلوماتية المتحصل عليها من إحدى الجرائم المنصوص عليها في القسم الخاص بالمساس بأنظمة المعالجة الآلية للمعطيات، و هذه المعطيات المتحصل عليها بطريقة غير مشروعة لم يشترط المشرع الجزائري أن تكون وسيلة من الممكن إستعمالها من جديد للمساس بأنظمة أو معطيات المعلوماتية السليمة أخرى، فإذا كانت هذه المعطيات لا تشكل ضرر على الأنظمة أو المعطيات المعلوماتية ففي هذه الحالة لا تقوم الجريمة و هذه القاعدة تطبق كما سلف ذكره على كل الجرائم المنصوص عليها في المادة 394 مكرر 2 ق.ع.جزائري و المادة 323-3-1 ق.ع.فرنسي.

في ما يخص عقوبة الجرائم المنصوص عليها في الفقرة 2 من المادة 394 مكرر 2 ق.ع.جزائري : فهي نفس العقوبة المقررة للجرائم المنصوص عليها في الفقرة 1 من نفس المادة.

و تجدر الإشارة إلى أنه بالإضافة إلى العقوبات المقررة بالنسبة لكل جريمة من جرائم المساس بالأنظمة المرتكبة من طرف شخص طبيعي فإن المشرع الفرنسي أدخل عقوبات تكميلية ***"Peines complémentaires"*** أخرى بشأنها في المادة 323-5 ق.ع.فرنسي.

المطلب الخامس : الجرائم الأخرى ضد الأنظمة المعلوماتية

في هذا المطلب سنتكلم عن المشاركة في مجموعة أو إتفاق في جريمة معلوماتية ضد الأنظمة المعلوماتية (المواد 323-4 ق.ع.فرنسي و 394 مكرر 5 ق.ع.جزائري)، و عن المساس بالأنظمة المعلوماتية التابعة للدفاع الوطني و المؤسسات الخاضعة للقانون العام (المادة 394 مكرر 3 ق.ع.جزائري، أما المشرع الفرنسي فلم ينص عليها)، و أخيرا سنتكلم عن إرتكاب جرائم المساس بالأنظمة من طرف الشخص المعنوي (المواد 323-6 ق.ع.فرنسي و 394 مكرر 4 ق.ع.جزائري).

الفرع الأول : المشاركة في مجموعة أو إتفاق لإرتكاب جرائم ضد الأنظمة المعلوماتية

من الواضح أن الجرائم ضد الأنظمة المعلوماتية و إن كانت مستحدثة إلا أنها في بعض الحالات تبقى جرائم مثلها مثل بقية الجرائم التقليدية الأخرى من حيث المبدأ حتى و إن كانت وسيلة إرتكابها مستحدثة، و بالتالي من الممكن أن ترتكب من طرف مجموعة أو إتفاق أي تكوين جمعية أشرار ***"Association de malfaiteurs"*** بهدف إرتكاب جريمة من الجرائم ضد نظام معلوماتي، حيث أنه ورد تعريفها في المادة 176 ق.ع.جزائري التي تنص : "كل جمعية أو إتفاق مهما كانت مدته و عدد أعضائه تشكل أو تؤلف بغرض الإعداد لجناية أو أكثر،أو لجنحة أو أكثر ... "، هنا يتعلق الأمر بالمشاركة في مجموعة أو فرقة مكونة من أكثر من شخص واحد تحضيرا لجريمة أو عدة جرائم في إيطار المساس بالأنظمة المعلوماتية، كما أن التحالف بين الأشرار قد ينتج عن مشاركتهم في العملية الإجرامية، و بالتالي يفهم من هذه المشاركة وجود تصرفات مادية فعلية سابقة عن إرتكاب الجريمة و المتمثلة في تبادل برامج القرصنة بين الأشخاص و المعلومات أو الأرقام السرية للنظام محل الجريمة فيما بينهم حيث إشترط المشرع الفرنسي (مادة 323-4) و الجزائري (مادة 394 مكرر 5) في هذه الجريمة أن يكون هنالك إعداد أو تحضير للجريمة و المجسد بفعل أو عدة أفعال مادية، في هذه الحالة هذه المجموعة تعاقب بنفس العقوبات المقررة للجرائم المذكورة في القسم الخاص بالمساس بالأنظمة المعلوماتية، و تجدر الإشارة على أنه يجب أن تتوافر لدى هذه الأشخاص النية الجرمية أي الإرادة في المشاركة في عملية غير مشروعة و أن يكونوا على علم بأن تصرفهم غير مشروع، كما أنه من جهة أخرى لا يشترط أن يكون كل عضو من هذه الجمعية يعلم بتصرفات الأعضاء الأخرى[1] [2].

المشرع بصفة عامة وضع هذه التجريمة لمقاومة و وضع حد لنوادي و منظمات القراصنة المعلوماتيين أو الهاكرز ***"Clubs et associations d'informaticien pirates ou de hackers"***، وبصفة عامة المحاكم الفرنسية إستعملت هذه التجريمة لمعاقبة أفعال المشاركة في الجريمة ضد الأنظمة و ليس الأعمال التحضيرية للجنحة و بالتالي القاضي الجزائي الفرنسي غير المعنى الذي كانت تذهب إليه التجريمة[3].

الفرع الثاني : الجرائم ضد الأنظمة المعلوماتية التابعة لهيئات و مؤسسات الدولة

نص عليها المشرع الجزائري في المادة 394 مكرر 3 حيث قرر مضاعفة العقوبات المنصوص عليها في قسم المساس بالأنظمة و مع إمكانية تقرير القاضي الجزائي لعقوبة أشد و بالتالي هذه الحالة تعد ظرف مشدد

---

(1) _ ***Arret de la cour d'Aix en Provence de l'année 1993.***

(2) _ أنظر : André Lucas, Devrèze Jean, Frayssinet Jean, ***Op.cit***, de la Page 687 à 688.

(3) _ أنظر : André Lucas, Devrèze Jean, Frayssinet Jean, ***Idem***.

للعقوبة، أما المشرع الفرنسي فلم ينص عليها إذ أن العقوبات التكميلية التي قررها بالنسبة لمرتكب الجرائم ضد الأنظمة المعلوماتية تعد وسيلة فعالة لردعها ***"Moyen dissuasif"***.

و تجدر الإشارة إلى أن المساس بالأنظمة المعلوماتية التابعة للدفاع الوطني و إن كانت في الأصل جريمة مساس بمال الدولة قد يشكل علاوة على ذلك جريمة الإضرار بالدفاع الوطني (مادة 61 فقرة 4 ق.ع.جزائري) و التي يمكن أن تدخل أيضا في جريمة الإرهاب المعلوماتي.

الفرع الثالث : الجرائم المرتكبة ضد الأنظمة المعلوماتية من طرف شخص معنوي

نصت عليها المادة 323-6 ق.ع.فرنسي حيث وضعت الشروط المتعلقة بإثارة المسؤولية الجزائية للشخص المعنوي وفق المادة 121-2 ق.ع.فرنسي، أما في ما يخص العقوبات فلقد حددها المشرع في المادة 131-38 ق.ع.فرنسي بالنسبة للغرامة أما العقوبات الأخرى فحددتها المادة 131-39 ق.ع.فرنسي.

بالنسبة للمشرع الجزائري فالعقوبة التي قررها بالنسبة للشخص المعنوي فهي غرامة تعادل 5 مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي في الجرائم المذكورة في قسم المساسات بالأنظمة المعلوماتية وفقا للمادة 394 مكرر 4 ق.ع.جزائري.

بخصوص الشروع في الجريمة ضد الأنظمة المعلوماتية فلقد نصت عليها المواد 323-7 ق.ع.فرنسي و 394 مكرر 7 ق.ع.جزائري و عاقب عليها المشرع بصفة عامة بنفس العقوبة المقررة للجنح المنصوص عليها في القسم الخاص بالمساسات بالأنظمة المعلوماتية.

أما في ما يخص الإجراءات الجزائية المتخذة في حالة إرتكاب إحدى الجنح ضد الأنظمة المعلوماتية سواء من طرف شخص معنوي أو شخص طبيعي، فلقد نص المشرع الجزائري في المادة 394 مكرر 6 ق.ع على مصادرة الأجهزة و البرامج و الوسائل المستعملة بالإضافة إلى إغلاق المواقع التي تكون محلا للجريمة من جرائم المساس بالأنظمة كما يغلق المحل أو مكان الإستغلال إذا كانت الجريمة قد إرتكبت مع علم مالك المحل و من بين أمثلة هذه الجريمة تلك المرتكب في نوادي الأنترنت ***"Cybercafés"***.

المطلب السادس : الفيروسات المعلوماتية كأهم وسائل المساس بالأنظمة المعلوماتية

في هذا الفرع سنتكلم عن الفيروسات المعلوماتية بإعتبارها من أهم وسائل المساس بالأنظمة المعلوماتية و المعطيات المعلوماتية و أكثرها إستعمالا، و نظرا للخطورة البالغة الناتجة عن إستعمالها على الإقتصاد بصفة خاصة، حيث أن الواقع المعاش في العالم يثبت ذلك، و عليه الدول المتقدمة سرعان ما تنبأت بها نظرا

للخسائر المالية الضخمة التي سببتها و لا زالت تسببها إلى حد الآن للمؤسسات مهما كان نوعها وطنية ***"Etatique"*** أو خاصة ***"Privé"***، كبيرة كانت أو صغيرة، إدارية كانت أو إقتصادية.

لهذا سنحاول وضع تعريف دقيق و مبسط للفيروس المعلوماتي، ثم سنتكلم عن الصور المختلفة التي يمكن أن يأخذها عند إستعماله ضد الأنظمة المعلوماتية، و أخيرا و هو المهم سنرى كيف عالج القانون الجزائري و المقارن مشكلة الإستعمال الغير مشروع للفيروسات المعلوماتية.

الفرع الأول : التعريف التقني للفيروسات المعلوماتية و خصائصها

في ما يخص التعريف التقني للفيروس المعلوماتي[1] ***"Le virus informatique"*** فهو تعليمة أو عدة تعليمات طفيلية خبيثة في شكل برامج صغيرة، موجهة من جهة للإنتشار ***"Prolifération"*** في الكمبيوتر و تعديل بطريقة سلبية نظام الإستغلال ***"Le système d'exploitation"*** [2] و كذا تحطيم أو التأثير سلبيا على المعلومات المعلوماتية في مختلف أنواعها (معطيات، بيانات، برامج)، أي كل ما له وجود منطقي في نظام معلوماتي سليم بمعنى إفساد السير العادي للنظام المعلوماتي بعد إستقرارها في ذاكرة الكمبيوتر ***"La mémoire de l'ordinateur"*** كالقرص المرن ***"Disque dur"*** [3].

في ما يخص الخصائص التقنية للفيروس المعلوماتي :

– فهو عبارة عن برنامج صغير ***"Petit programme"*** يختفي بسهولة في النظام المعلوماتي [4]، و مجرمي المعلوماتية المختصين في برمجة الفيروسات المعلوماتية تمكنوا من إستغلال هذه الخاصية لوضع فيروسات معلوماتية من الصعب العثور عليها بالبرامج المضادة للفيروسات و تجدر الإشارة إلى أن معظم الفيروسات المعلوماتية تتمتع بخاصية الخفية ***"Furtifs"***.

– له قدرة فائقة على مهاجمة المكونات المعنوية لجهاز الحاسب الآلي و الشبكات المعلوماتية التي تربطها فيما بينها مما يزيد من قدرته على الإنتشار ***"Capacité à ce propagé"*** و السرعة في تنفيذ أهدافه ***"Capacité a exécuté rapidement ses objectifs"*** [5].

---

(1)_ لمزيد من المعلومات حول الفيروسات المعلوماتية أنظر موقع الأنترنت الجزائري الأول في مجال الحماية المعلوماتية في العنوان التالي : www.wikayanet.dz

(2)_ أنظر صفحة الأنترنت (مقال تحت عنوان : ***Les virus***) في العنوان التالي : **http://www.wikayanet.dz/modules.php?name=Virus**

(3)_ أنظر : Pansier Frédéric-Jérôme, Jez Emmanuel, ***Initiation à l'Internet juridique***, édition Litec (2e édition), 1er trimestre 2000, (France), Page 67.

(4)_ أنظر : هدى حامد قشقوش، "**جرائم الحاسب الإلكتروني في التشريع المقارن**"، (الطبعة الأولى)، دار النهضة العربية، القاهرة (مصر)، سنة 1992، صفحة 99.

(5)_ أنظر : محمد سامي الشوا، "**ثورة المعلومات و إنعكاساتها على قانون العقوبات**"، دار النهضة العربية، القاهرة (مصر)، سنة 1993، صفحة 189.

– يمكن أن يتسلل إلى النظام المعلوماتي بموجب وحدات الإدخال إلى النظام ***"S'introduit dans le système à partir des Unités d'entrée"***، كقارئة الأقراص المضغوطة أو المودم الذي يسمح الدخول إلى شبكة الأنترنت أو الأقراص المتنقلة ***"Disque amovible (ex : flash disque)"***.

– قد يبدأ في الإشتغال من تلقاء نفسه بعد دخوله إلى النظام المعلوماتي أو يشتغل إذا شغل المستخدم إحدى البرامج أو المعطيات المصابة به ***"Ce déclanche automatiquement ou manuellement"*** مما يزيد من قدرته في الإنتشار داخل النظام المعلوماتي.

– قد يؤخذ صور عديدة ***"Peut prendre plusieurs formes"***، مثلا : في شكل معطيات (مستند وارد ***"Fichier (Word)"***)، أو برامج، أو بيانات بعد إصابتها.

و من هذا المنطلق يعتبر الفيروس المعلوماتي شديد الصلة بالجريمة[1] إذ يعد وسيلة تقنية فعالة لإرتكاب جرائم معلوماتية معينة و أهمها المساس بإستقرار نظام المعالجة الآلية للمعطيات[2].

الفرع الثاني : أنواع الفيروسات المعلوماتية

هناك تقسيم للفيروسات المعلوماتية بحسب وظيفتها :

– فيروسات في شكل برامج ***"Virus programmes"*** : و هي فيروسات أنشأت أو صممت لإصابة المعطيات المطبقة ***"Exécutables"***، مثلا : ***"*.ExE"***، هذه الفيروسات تضيف رموز في المعطيات المطبقة و بالتالي بمجرد تشغيل هذه المعطيات المصابة فإن الفيروس يبدأ في العمل أي التدفق إلى الذاكرة المركزية بهدف إصابة برامج أخرى و يجعل هذه البرامج غير قابلة للإستعمال ***"Inutilisables"*** [3].

– فيروسات إشعال "***Virus d'amorçage***" : هذه الفيروسات تحتل مختلف المواقع في القرص المرن التي تحتوي على البرامج المهمة لتشغيل النظام المعلوماتي و ضمان سيره الجيد و تصيبها بخلل مهم بحيث لا تفتح الفرصة لإستعمال القرص المرن من جديد في المستقبل[4].

كما يوجد تقسيم آخر للفيروسات المعلوماتية بحسب نوعها، أي الفيروسات الخفية، الفيروسات متعددة الأشكال و أخيرا الفيروسات المحمية برموز.

---

(1)_ كما سنراه في العنوان : "**حكم الإستعمال الغير مشروع للفيروسات في نظر القانون**".

(2)_ أنظر : هدى حامد قشقوش، **مرجـــع سابـــق**، صفحة 99.

(3)_ أنظر صفحة الأنترنت في العنوان التالي : ***Op.cit* : http://www.wikayanet.dz/modules.php?name=Virus**

(4)_ أنظر نفس صفحة الأنترنت السابقة : ***Idem* : http://www.wikayanet.dz/modules.php?name=Virus**

– فيروسات خفية ***"Virus furtifs"*** : هذه الفيروسات تفلت من الرقابة بواسطة قدرتها على التنكر ***"le Camouflage"*** مما يجعل إكتشافها صعب[1].

– فيروسات متعددة الأشكال ***"Virus polymorphes"*** : هذه الفيروسات تتميز بالعبقريـة إذ تغير شكلها في كل عملية إصابة، و هذه الفئة تعد من أخطر الفيروسات[2].

– فيروسات محمية برموز أو شفرة ***"Virus cryptés"*** : هذه الفيروسات تحمي نفسها برموز أو شفرة متغيرة ***"Codes remplaçables"*** مما يجعل من الصعب العثور عليها[3].

التقسيم الأخير يتعلق ببرامج القرصنة، حيث أدمجنا هذه البرامج في طائفة الفيروسات [4] لسبب بسيط هو أنه يمكن العثور عليها داخل نظام معلوماتي بموجب البرامج المضادة للفيروسات ***"Les anti-virus"***، و إن كانت في الحقيقة ليست بفيروسات معلوماتية إلا أنها تشبهها في وظيفتها، وأهمها حصان طروبان، الدودة و القنبلة المنطقية.

– حصان طروبان ***"Le cheval de Troie"*** : و هو برنامج قرصنة يرسل في أغلب الأحيان عن طريق شبكة الأنترنت، و يمكن لهذا البرنامج أن يشتغل في أي وقت أو بمجرد تقبله لإشارة خارجة عن النظام محل الجريمة بواسطة شبكات الإتصال المعلوماتية، هذا البرنامج ليس بفيروس لأنه لا يتكاثر و لا ينتشر و لا يشتغل بصفة أوتوماتيكية و إنما بصفة يدوية، و عندما يشغل هذا البرنامج فإنه سيسهل للغير سيء النية التحكم في النظام المستهدف كحذف المعطيات أو نسخها أو التجسس على صاحب النظام مثلا، كما يستعمل حصان طروبان كوسيلة فعالة للسيطرة على برامج النظام المعلوماتي المملوك للغير عن بعد[5].

– الدودة ***"Le vers"*** : هو الآخر برنامج ينتشر في الشبكات المعلوماتية و الأنظمة أوتوماتيكيا كالفيروس المعلوماتي لكن دون إصابة برامج أخرى و وظيفته الوحيدة هي التكاثر إلى حد يؤدي إلى إحداث شلل الشبكات المعلوماتية مما يسهل تسرب الفيروسات المعلوماتية[6].

– القنبلة المنطقية ***"La bombe logique"*** : عبارة عن برنامج أو جزء من برنامج ينفذ في لحظة معينة أو في كل فترة زمنية بشكل منتظم، لذلك يطلق عليه أيضا تسمية القنبلة الزمنية ***"Bombe à retardement"***، كما أنه يمكن أن يشتغل بناءا على شروط منطقية، و حتى يكون البرنامج فعال لا بد من وضعه في شبكة معلوماتية و بالتالي

---

(1)_ أنظر نفس صفحة الأنترنت السابقة : ***Op.cit*** : **http://www.wikayanet.dz/modules.php?name=Virus**

(2)_ أنظر نفس صفحة الأنترنت السابقة : ***Idem*** : **http://www.wikayanet.dz/modules.php?name=Virus**

(3)_ أنظر نفس صفحة الأنترنت السابقة : ***Idem*** : **http://www.wikayanet.dz/modules.php?name=Virus**

(4)_ برامج القرصنة تعد الجيل الجديد من المخاطر المعلوماتية ***"la Nouvelle génération des menaces informatiques"*** و يمكن إعتبارها نوع آخر من الفيروسات المعلوماتية.

(5)_ أنظر صفحة الأنترنت في العنوان التالي : ***Op.cit*** : **http://www.wikayanet.dz/modules.php?name=Virus**

(6)_ أنظر نفس صفحة الأنترنت السابقة : ***Idem*** : **http://www.wikayanet.dz/modules.php?name=Virus**

فإنه لا يمكنه أن يأثر على الكمبيوتر الغير مرتبط بشبكة معلوماتية، و دور هذا البرنامج هو تسهيل تنفيذ عمل غير مشروع أي تخريب النظام المعلوماتي بعد إنفجاره في هذا الأخير[1].

الفرع الثالث : الوسائل التقنية للتصدي للفيروسات

أنجع وسيلة لمقاومة الفيروسات المعلوماتية هي الوقاية قبل اللجوء إلى القضاء [2]، و من بين هذه الوسائل البرامج المضادة للفيروسات المعلوماتية ***"Les programmes anti-virus"***، و كذا البرامج المعلوماتية المضادة لبرامج القرصنة ***"(FireWall) ou (Pare-feu)"***، و كذا حماية النظام و المعطيات المحتواة فيه بموجب رموز أو شفرات سرية تمنع التعرض لها.

الفرع الرابع : حكم الإستعمال الغير المشروع للفيروسات في نظر القانون

إدخال فيروس معلوماتي في نظام معلوماتي سليم يشكل بالدرجة الأولى وسيلة فعالة لإفساد سير النظام، فهي في نظرنا وسيلة إعتراض أو تحريف دائم أو دوري للنظام المعلوماتي، و كذا وسيلة مساس بمعطيات النظام المعلوماتي المستهدف بالجريمة.

الفقرة الأولى : الإعتراض للنظام المعلوماتي

من بين الأدوار الأساسية التي يمكن أن تلعبها الفيروسات المعلوماتية للمساس بأنظمة المعالجة الآلية للمعطيات هو الإعتراض لسيره العادي و هنا الإعتراض قد يكون إعتراض دائم أو دوري.

أولا : الإعتراض الدائم للنظام المعلوماتي

الفيروس عند دخوله للنظام فإنه لا يتوقف عن الإشتغال (أي المساس السلبي يستمر وفقا للتعليمات التي يحملها و التي تحدد وظيفته السلبية داخل النظام و كذا تكاثره في النظام محل الجريمة) مما يسبب تعطيل مهم في سيره العادي ***"Ralentir le système"***، إلى غاية العثور عليه تقنيا بموجب البرامج المعلوماتية المضادة للفيروسات المعلوماتية التي تقوم بحذفه من النظام و بالتالي وضع حد لهذا الإعتراض.

---

[1]_ أنظر : محمد سامي الشوا، **مرجـــع سابـــق**، من الصفحة 186 إلى 187.

[2]_ وهنا يمكن أن تكون هنالك متابعة قضائية سواء في الجزائر أو في فرنسة و سواء أدى إستعمال الفيروسات إلى المساس بالنظام المعلوماتي أم لا، وفقا للمواد 323–1 إلى 323–7 ق.ع.فرنسي و المواد 394 مكرر إلى 394 مكرر 7 ق.ع.جزائري.

ثانيا : الإعتراض الدوري للنظام المعلوماتي

كما هو الحال في حالة زرع نوع من الفيروسات التي تعترض للنظام في كل بداية شهر جديد مثلا، أو أن يشتغل في كل مرة يتم فيها تشغيل برنامج مصاب به في النظام محل الإعتراض، في كل الأحوال الإعتراض يعد قائم و من تم يكون محل متابعة جزائية.

الفقرة الثانية : التحريف الدائم أو المؤقت لسير النظام المعلوماتي

أي تشويه ***"Déformation"*** نتائج المعالجة الآلية أو تعديل دور برامج النظام أو السيطرة عليها أو على النظام بصفة دائمة أو مؤقتة بفعل المساس بواسطة الفيروسات المعلوماتية أو برامج القرصنة و من أشهرها برنامج حصان طرويان ***"Le cheval de Troie"*** الذي يؤدي إلى إعطاء نتائج أخرى أو خاطئة مختلفة عن ما كان سيعطيه النظام المعلوماتي في حالة سيره العادي بواسطة السيطرة عليه عن بعد، فإذا كان هذا البرنامج المعلوماتي ليس بفيروس إلا أن هذا لا يمنع من وجود فيروسات متمكنة هي الأخرى من تحريف سير النظام.

و تجدر الإشارة إلى أن إنشاء فيروس معلوماتي أو تجميعه أو الإتجار به أو نشره عبر الشبكات أو الأنظمة المعلوماتية يشكل جريمة بالنظر إلى القوانين الحالية أي المادة 394 مكرر 2 ق.ع.جزائري، كما تقوم الجريمة إذا ترتب عن إستعماله نتائج سلبية أي إفساد سير النظام المعلوماتي مهما كان نوعه بإعتباره من بين الوسائل الفعالة للإعتراض أو تحريف سير النظام.

الفقرة الثالثة : المساس بالمعطيات المعلوماتية

من جهة أخرى قد يدخل في حكم الإستعمال الغير مشروع للفيروس المعلوماتي المادة 323-3 ق.ع.فرنسي و المادة 394 مكرر 1 ق.ع.جزائري للأسباب التالية :

- الفيروسات المعلوماتية تؤخذ شكل معطيات أو برامج معلوماتية، مثلا : ***".exe, .dll ou .doc"***، يمكن إدخالها إلى النظام المعلوماتي بطريقة الغش.
- الفيروسات المعلوماتية قد تكون لها القدرة على إزالة معطيات معلوماتية من النظام المعلوماتي.
- الفيروسات المعلوماتية بإمكانها تعديل المعطيات المعلوماتية الموجودة في النظام المعلوماتي مثل : الفيروس بلبلا ***"Le virus BLEBLA"*** الذي إكتشف مؤخرا في شبكة الأنترنت، من بين خصائصه أنه ينتشر في النظام المعلوماتي بسرعة هائلة، كما يكمن دوره في تعديل خصائص المعطيات الموجودة داخل النظام حيث يجعلها معطيات غير معروفة ***"Fichiers inconnues"*** لا يمكن قراءتها.

في ما يخص مشكلة إثبات جريمة الإستعمال الغير مشروع للفيروسات المعلوماتية و القضايا التي طرحت بشأنها أمام القاضي الجزائي :

الإشكال الرئيسي في ما يخص الإستعمال الغير المشروع للفيروس المعلوماتي للإعتراض أو تحريف سير النظام المعلوماتي أو حتى المساس بالمعطيات المعلوماتية، هو صعوبة الإثبات بأن المجرم أدخل إراديا هذا الفيروس داخل النظام للمساس بالمعطيات الموجودة به، حيث أن إدخال الفيروس المعلوماتي يتم كما سبق ذكره بإحدى وحدات الإدخال إلى الكمبيوتر و في أغلب الأحيان يتم دون ترك أي أثر يسمح معرفة من أين تم إدخاله أو معرفة من أدخله أي الفاعل[1].

و تجدر الإشارة إلى أن الفيروس المعلوماتي ما دام أن دوره الأساسي هو الإضرار بالنظام المعلوماتي، لذلك فإن إستعماله كان منطقيا لا بد أن يجرم، و من بين القضايا التي طرحت في هذا الشأن : إحدى المجالس القضائية الفرنسية إعتبرت بأن شركة الصيانة في مجال المعلوماتية تسببت في حدوث إعتراض ضد السير العادي لنظام المعالجة الآلية للمعطيات المملوك للغير نتيجة تشغيل غير مشروع لقنبلة منطقية بعد إدخالها في النظام، لأسباب إدعى بها المتهم لم يأخذها القاضي الجزائي بعين الإعتبار و مهما كانت أهمية هذه الأسباب فإن الشركة مسؤولة عن الإعتراض الذي سببته في النظام المعلوماتي، و في هذه القضية إعتبر القاضي مسير الشركة الفاعل الأصلي في الجريمة ***"Auteur principal du délit"*** و العمال في الشركة الذين تسببوا في الإعتراض المادي يعدوان شركاء في الجريمة ***"Complice"*** [2].

أيضا مثال آخر في ما يخص المتابعة الجزائية على أساس إستعمال الفيروسات المعلوماتية ضد الأنظمة، هذه المرة تتمثل في أول محاكمة جزائية في ألمانيا سنة 2005، حيث أن التحقيق الإبتدائي للشرطة القضائية دام 7 أيام منذ بدايته في ولاية وافنسن (ألمانيا) ***"Waffensen (Allemagne)"*** و في الأخير تمكنت من العثور على منشأ فيروس ساسير ***"Virus Sasser"*** و إلقاء القبض عليه بفضل إبلاغ مصالح الشرطة القضائية من طرف أشخاص (شهود) من نفس المنطقة كانوا يعرفون صاحب الجريمة، حيث ظهر هذا الفيروس في شهر أفريل من سنة 2004 و من خصائصه أنه يصيب أجهزة الكمبيوتر بمجرد إتصالها بشبكة الأنترنت مما يجعل هذا الفيروس أكثر خطورة من الأنواع الأخرى من الفيروسات المعلوماتية، و مصمم فيروس ساسير و مستعمله هو شاب كان لا يتجاوز من العمر 18 سنة وقت إرتكابه للجريمة، و هذا الطفل كان طالب في ثانوية مهنية متخصصة في المعلوماتية، و الشرطة القضائية عند إلقائها القبض عليه وجدت في محل إقامته مصدر الفيروس المعلوماتي أي البرنامج المشكل منه الفيروس ***"Code source du virus"*** و إحتجزت جهاز كمبيوتره و بعض

---

(1) _ أنظر : Bensoussan Alain (sous la direction de), ***Op.cit***, de Page110 à 111.

(2) _ أنظر : Bensoussan Alain (sous la direction de), ***Idem***.

الأقراص المضغوطة كأدلة، و تمت محاكمة المتهم في جويلية 2005[1]، حيث تمت إدانته بعقوبة عام و تسعة أشهر حبس غير نافذ، و 30 ساعة من الأعمال الشاقة في مستشفى أو منزل المتقاعدين، و تجدر الإشارة إلى أن هذه العقوبة كانت مبنية على أساس التخريب المتعمد ***"Sabotage"*** أجهزة الكمبيوتر و تعديل معطياتها.

و بالتالي و حتى إن كانت أدلة الإثبات في القضية السالفة الذكر ذو طبيعة مادية أي أن أدلة إثبات الجريمة المعلوماتية محمولة على دعامة مادية، إلا أنه ليس دائما الحال في هذا النوع من الجرائم نظرا لكون أنها ترتكب في مجال معلوماتي، و بالتالي طبيعة الدليل الواجب إتيانه هو دليل بالدرجة الأولى ذو طبيعة معنوية غير ملموس إلكتروني أو معلوماتي و ذو خاصية هشة و متبخرة ***"Volatile"*** إذ يمكن أن يفلت من يد محققي الشرطة العلمية نظرا لسهولة حذفه من الذاكرات المعلوماتية مهما كان نوعها و مما سيخلق صعوبة إضافية لإتيان دليل الجريمة، و بالتالي و في سبيل ضمان توافر الأدلة الكافية لتكوين ملف الإتهام من طرف النيابة ضد المتهم، كان لابد على المشرع أن يوفر رصيد تشريعي إجرائي و عقابي كافي نظرا لكون أن الدليل في حد ذاته في هذا النوع من الجرائم بالدرجة الأولى و كما سلف ذكره ذو طبيعة معنوية غير ملموسة و سريعة الزوال و بالتالي التحريات هي الأخرى ستكون في مجال إلكتروني، و ينبغي أن تتوافر لذا خبراء الشرطة العلمية معرفة تقنية ذات مستوى عالي في المجال المعلوماتي و الإلكتروني و بما فيها الشبكات بمختلف أنواعها سلكية أو لاسلكية و كذا تحكمهم في تقنيات فك الرموز أو الشفراة، كما يستوجب أن تتم هذه التحريات بسرعة حتى لا تفلت أدلة الجريمة كما سبق توضيحه من يد محققي الشرطة العلمية في سبيل العثور على مرتكب الجريمة و إثبات إدانته أمام العدالة الجزائية.

---

[1] _ أنظر صفحة الأنترنت في العنوان التالي (مقال إعداد : تحت عنوان : ***Les virus sasser netsky décapités par l'arrestation de leur auteur***، 11 / 05 / 2004) : **http://solutions.journaldunet.com/0405/040511_sasser.shtml**

المبحث الثاني :

جريمة التزوير المعلوماتي

في هذا المبحث سنتكلم عن القوانين التي جرمت تزوير المعطيات المعلوماتية (المطلب الأول)، ثم سنعرف هذه الجريمة (المطلب الثاني)، و أخيرا سنحاول تحديد الأركان المكونة لهذه الجريمة (المطلب الثالث)، و تجدر الإشارة إلى أنه سنحصر دراستنا هنا في الجانب أو المحيط المعلوماتي لجريمة التزوير أي تزوير الدعائم المعنوية ***"Supports logiques incorporel ou immatériel"*** الغير ملموسة بإعتبارها جريمة تختلف عن جريمة التزوير التي تقع على الدعائم المادية ***"Supports matériels"*** (مثلا :المحررات الكتابية، العملات النقدية).

المطلب الأول : النصوص العقابية في مجال تزوير المعطيات المعلوماتية

أول نص عقابي لتزوير المعطيات المعلوماتية كان سنة 1988 في فرنسا بموجب القانون 88-19 المؤرخ في 5 جانفي 1988 و المتعلق بالغش المعلوماتي، الذي أدخل في قانون العقوبات المادة 462-5 : في ما يخص تزوير المستندات المعلوماتية و المادة 462-6 : في ما يخص الإستعمال الغير مشروع لهذه المستندات المعلوماتية المزورة[1].

في ما بعد ألغيت هذه المادتان سنة 1994 لسبب أن التعريف العام في ما يخص جريمة التزوير الذي جاءت به المادة 441-1 ق.ع.فرنسي أصبحت تسمح بإدماج حالة التزوير في محيط معلوماتي، و بالتالي تم حذفها من قانون 88-19.

في ما يخص التشريع العقابي الجزائري في موضوع جريمة التزوير فلقد خصص لها فصل كامل أي الفصل السابع لكافة جرائم التزوير (المواد من 197 إلى 241 ق.ع.جزائري)، و تجدر الإشارة إلى أنه رغم وفرة النصوص القانونية في قانون العقوبات حول جريمة التزوير إلا أن المشرع الجزائري إلى حد الآن لم يجرم عملية التزوير التي تقع على دعائم معنوية كالمستندات رقمية أو المعلوماتية ***"Documents numérique ou informatiques"*** (مثلا : معطيات معلوماتية ***"Données"***، مستندات معلوماتية ***"Documents"***، برامج معلوماتية ***"Programmes"***)، و لهذا سنركز دراستنا على المادة 441-1 ق.ع.فرنسي بإعتبارها عالجت هذا الموضوع.

---

[1] _ للإطلاع على مضمون المادتين 462 مكرر 5 و 6 ق.ع.فرنسي **أنظر : الملحق رقم 4**

المطلب الثاني : تعريف جريمة التزوير المعلوماتي و الآراء الفقهية بشأنها

في ما يخص التشريع العقابي الجزائري و زيادة لكونه لم يخصص لجريمة التزوير المعلوماتي نصوص معينة، فإنه لم يعرف بصفة عامة جريمة التزوير [1]، إلا أن هذا التعريف سنجده في نص المادة 441-1 ق.ع.فرنسي التي جمعت بين تعريف جريمة التزوير التقليدية (على دعامة مادية) و جريمة التزوير المعلوماتية (على دعامة معنوية كالمستندات المنطقية أو المعلوماتية) :

"يشكل مزور كل تغيير أو تحريف للحقيقة من طبيعته أن يسبب ضرر و الذي يتم بأي طريقة كانت، على محرر أو على دعامة أخرى للتعبير عن الفكرة الذي من خلال موضوعه أو أثره قد ينشئ الدليل عن حق أو واقعة لها نتائج قانونية ..."[2].

من الواضح أن المعلوماتية توفر وسائل إضافية للمزورين لتشكيل وثائق مزورة، كالعملات نقدية مزورة[3].

في ما يخص الوسائل المستعملة لتزوير المعطيات المعلوماتية فلم يحددها المشرع الفرنسي على سبيل الحصر و بالتالي الوسيلة المستعملة غير مهمة لتقرير العقوبة إلا أنه يشترط أن تتحقق النتيجة المتمثلة في تزوير المعطيات من خلال تغيير الحقيقة و أن يؤدي إستعمالها إلى إحداث ضرر للغير.

من جهة أخرى الدعائم المعنوية للتعبير عن فكرة أو عدة أفكار فمجالها واسع إذ قد يتعلق الأمر بتزوير إشارات مرئية ***"Signaux visuels"***، سمعية أو صوتية ***"Vocaux"*** أو معلوماتية ***"Informatiques"*** (مثلا : معطيات، بيانات، مستندات، برامج)، هذه الدعائم المعنوية نجدها في كل الدعائم المادية المعروفة إلى حد الآن : كالأقراص المضغوطة أو المرنة، البطاقات الإلكترونية، الأشرطة، أو أجهزة أو نظم الإقرار المرئي أو السمعي ***"Systèmes de reconnaissances visuelles ou sonores"*** [4]، شريطة أن تكون من خلال موضوعها أو أثرها منشأة لحق أو واقعة لها نتائج قانونية كأن تثبت حق ملكية مثلا.

و تجدر الإشارة إلى أن الدعامة المعنوية المحتواة في دعامة مادية على عكس الدعائم المادية البحتة أي المحررات المكتوبة فهي غير ملموسة و لا تكون دائما في شكل نص كتابي كما سلف ذكره.

---

(1)_ أنظر : المومني أنيس، ماجستير شعبة : القانون الجنائي، "**قانون العقوبات في مواجهة مخاطر الأنترنت** " تحت إشراف الأستاذ : بوكحيل لخضر، جامعة باجي مختار – كلية حقوق عنابة، سنة 2004، صفحة 50.

(2)_ أنظر نص المادة باللغة الفرنسية :

Art. 441-1 du code pénal français : « Constitue un faux toute altération de la vérité, de nature à causer un préjudice et accomplie par quelque moyen que ce soit, dans un écrit ou dans autre support d'expression de la pensée qui a pour objet ou qui peut avoir pour effet d'établir la preuve d'un droit ou d'un fait ayant des conséquences juridiques … ».

(3)_ أنظر : Hollande Alain, De Bellefonds Linant Xavier, ***Op.cit***, Page 256.

(4)_ أنظر : Hollande Alain, De Bellefonds Linant Xavier, ***Idem***.

في ما يخص الآراء الفقهية حول إمكانية تطبيق أو عدم تطبيق النصوص العقابية التقليدية على جريمة تزوير المعطيات المعلوماتية :

فلقد تباينت المواقف حول إمكانية تطبيق النصوص التقليدية في ما يخص حالة تزوير المعطيات المعلوماتية :

أولا : الفريق المعارض لتطبيق النصوص التقليدية على التزوير المعلوماتي

يستند هذا الفريق إلى الحجج التالية :

– جريمة التزوير في المحررات تستلزم أن تكون هنالك كتابة و هو ما لا تفترضه عمليات التزوير في مجال المعلوماتية أو الدعائم المعنوية التي تتطلب معالجة آلية للمعطيات[1].

– جريمة التزوير تبين إمكانية إستعمال الوثيقة المزورة كوسيلة إثبات، و لكن الوثائق و السجلات أو المستندات المعلوماتية ليست لها أهمية[2] في ميدان الإثبات[3].

و لعل ما يدعم هذا الرأي تلك القوانين المستحدثة المتعلقة بالتجارة الإلكترونية التي جاءت بها القانون التونسي رقم 2000–83 المؤرخ في 9 أوت 2000 و المتعلق بالتجارة الإلكترونية حيث نجد الفصل الرابع منه يشير إلى أنه : "يعتمد قانونا حفظ الوثيقة الإلكترونية كما يعتمد حفظ الوثيقة الكتابية "، و هذا ما يدل على أن هنالك تباين بين الوثيقتين، فإذا نظرنا إلى الوثيقة الورقية و الإلكترونية فإننا نجد فرقا شاسعا بينهما، حيث تأخذ المعلومات في الوثيقة الورقية مظهرا ملموسا، على عكس الوثيقة الإلكترونية التي لا تأخذ مظهر ملموس[4]، و لا تعني دائما نصا كتابيا بل يمكن أن تكون هذه الوثيقة الإلكترونية : سمعية، مرئية، أو معلوماتية[5] .

ثانيا : الفريق المؤيد لتطبيق النصوص التقليدية على التزوير المعلوماتي

يرى هذا الفريق بأن هنالك علاقة وثيقة بين العقاب على التزوير و نظام الإثبات، فطبقا لمبدأ الإثبات الحر في مجال المعاملات التجارية، فإن الوثائق الإلكترونية طالما كانت لها قيمة فإنها تصلح للإثبات، و بالتالي إعتمادها في جرائم التزوير، حيث ذهب الإجتهاد القضائي التونسي إلى أبعد من ذلك من خلال تأكيد محكمة التعقيب في قضية متعلقة بالإعتداءات التي إستهدفت البنك التونسي القطري للإستثمار، على أن : " التدليس في

---

(1)_ أنظر : المومني أنيس، **مرجـــع سابـــق**، صفحة 52.

(2)_ المعطيات المعلوماتية على عكس ما يقوله أصحاب هذا الإتجاه أصبحت تعد وسيلة إثبات في التشريع الفرنسي، كما أن المشرع الجزائري أصبح يعترف بأن النظام المعلوماتي و ما فيه من معطيات عبارة عن مال و لا بد من حمايته جنائيا و هذا ما يجعلنا نفهم بأن المشرع الجزائري سيتبع الطريق التي سلكها المشرع الفرنسي أي تجريم التزوير المعلوماتي و بالتالي الإعتراف بأن المعطيات المعلوماتية على وجه الخاص و الدعامة المعنوية ***"Le support numérique"*** وسيلة إثبات في القانون.

(3)_ أنظر : المومني أنيس، **مرجـــع سابـــق**، صفحة 52.

(4)_ كالمعطيات و البرامج و المستندات الإلكترونية كدعائم معنوية فلا يمكن إستعمالها أي نقلها من مكان إلى آخر إلا إذا سجلت على دعامة مادية كالأقراص المضغوطة أو القرص المرن.

(5)_ أنظر : المومني أنيس، **مرجـــع سابـــق**، صفحة 52 إلى 53.

مفهومه العام من الناحية الجزائية هو كل فعل مغاير للحقيقة نتج عنه ضرر عام أو خاص، و عليه فإن تضمين معطيات مخالفة و مغايرة للحقيقة بجهاز الإعلامية يعد من قبيل التدليس الذهني الذي ينتج عنه ضرر يتمثل في خسارة فادحة للبنك المتضرر "[1].

و في المعنى ذاته أكد الأستاذ جون دفراز ***"Jean Devrèze"*** أنه يمكن التغلب على العقبات و ذلك بتغليب روح النصوص العقابية على ألفاظها و حروفها، و إعتبر أن ما يظهر في شاشة الحاسب الآلي نمطا مستحدثا للمحرر يمكن أن يقع عليه التزوير[2].

و للتغلب على الصعوبات في مجال المحررات المعلوماتية و في سبيل تمديد الحماية من جريمة التزوير في محيط المعلوماتية، عمدت التشريعات في العديد من الدول بإستحداث و تعديل نصوصها العقابية بطريقة تجعلها تتصدى للتزوير المعلوماتي كما هو الحال في التشريع العقابي الفرنسي حيث أن المشرع التونسي إتبع الطريق الذي سلكه المشرع الفرنسي في هذا المجال من خلال إقراره بدوره بجرائم التزوير في الوثائق المعلوماتية، من خلال التعديلات التي طرأت على المجلة الجنائية و ذلك بموجب القانون 1999-89 المؤرخ في 2 أوت 1999، بهدف تجريم كل أنواع التزوير المعلوماتي التي تنشأ أساسا بموجب إستعمال تقنية المعلوماتية و التي قد يقوم بها الموظف العمومي، من خلال : "صنع وثيقة مكذوبة أو تغيير متعمد للحقيقة بأية وسيلة كانت في كل سند كان ماديا أو غير مادي (معنوي ***"Incorporel ou immatériel"***) من وثيقة معلوماتية أو إلكترونية و ميكروفيلم و ميكروفيش، و يكون موضوعه إثبات حق أو واقعة منتجة لآثار قانونية "، أو من خلال قيام أي شخص آخر بـــ : " إدخال تغيير بأي شكل كان على محتوى وثائق معلوماتية أو إلكترونية أصلها صحيح " مع ضرورة حصول ضرر للغير[3].

المطلب الثالث : أركان جريمة التزوير المعلوماتي و العقوبات المقررة بشأنها

في هذا المطلب سنتناول أركان جريمة التزوير في محيط المعلوماتية أي الركن المادي للجريمة في (فرع أول) ثم الركن المعنوي في (فرع ثاني).

---

[1]_ أنظر : المومني أنيس، **المرجـــع نفســـه**، صفحة 53.

[2]_ أنظر : المومني أنيس، **المرجـــع نفســـه**، صفحة 53 إلى 54.

[3]_ أنظر : المومني أنيس، **المرجـــع نفســـه**، صفحة 54 إلى 55.

الفرع الأول : الركن المادي للجريمة

قانون العقوبات الفرنسي لم يعطي المزيد من المعلومات في ما يخص عملية التزوير ***"L'acte de falsification"***، و بالتالي و حسب مفهوم المادة 441-1 ق.ع.فرنسي، التغيير للحقيقة قد يكون مادي ***"Matériel"*** أو معنوي منطقي أو فكري[1] ***"Logique ou intellectuelle"***.

- التزوير المادي : يتعلق الأمر بالتغيير أو التحريف المادي ***"Altération physique"*** للسند المادي ***"Le support matériel"*** أو إنشاء سند مزور كما هو الحال بالنسبة للمحررات الكتابية أو العملات النقدية[2].

- التزوير المعنوي : يتعلق الأمر هنا بتغيير المعلومة المعلوماتية و مثال ذلك في ما يخص النتائج التي يقدمها نظام المعالجة الآلية تابع لإدارة مالية معينة في شكل وثائق أو تقارير معلوماتية (الخزينة العامة مثلا)، أو أن يقوم مثلا المجرم بإظهار رصيد مالي أكبر أو أقل من المبلغ الحقيقي الذي تم حسابه من طرف النظام و ذلك بواسطة تغيير النتيجة الأصلية الواردة في الوثيقة المعلوماتية التي أصدرها هذا النظام [3] عن طريق معالجة آلية غير مشروعة، و تجدر الإشارة إلى أن التزوير المعنوي أي المعلوماتي هو السبيل الوحيد لتزوير مستند منطقي أو معلوماتي ***"Document logique ou informatique"*** [4].

بالرجوع إلى المادة 441-1 ق.ع.فرنسي فإن الدعائم الأخرى محل جريمة التزوير عديدة قد تكون مثلا : بطاقة إلكترونية بنكية ***"Carte magnétique bancaire"***، أو شريط ممغنط ***"Bande magnétique"***، أو قرص مرن أو متنقل ***"Disque dure ou amovible"***، أي تغيير المعلومات المعلوماتية التي تحتويها.

من جهة أخرى التزوير المعلوماتي[5] قد يتم بطرق عديدة حيث أن المشرع الفرنسي لم ينص عليها صراحة و لا على سبيل الحصر، وبالتالي يكفي أن تتحقق النتيجة المتمثلة في إصدار وثيقة معلوماتية مغايرة للحقيقة شريطة أن تكون هذه الوثيقة دليل ينشأ حق أو واقعة لها نتائج قانونية و أن يؤدي إستعمالها إلى إلحاق ضرر بالغير.

---

(1)_ أنظر : Michel Vivant (sous la direction), Christian Le Stanc, Lucien Rapp, Michel Guibal (avec leurs collaboration), Lionel Costes (secrétaire général de la rédaction), ***Lamy - Droit de l'Informatique / Informatique, Télématique, Réseaux***, édition Lamy S.A., France, édition 1991, (France), Page 1260.

(2)_ أنظر : Michel Vivant (sous la direction), Christian Le Stanc, Lucien Rapp, Michel Guibal (avec leurs collaboration), Lionel Costes (secrétaire général de la rédaction), ***Idem***.

(3)_ حتى تقوم الجريمة يشترط أن يكون هذا التقرير أو الوثيقة المعلوماتية معتمدة و معترف بها كوسيلة إثبات.

(4)_ أنظر : Michel Vivant (sous la direction), Christian Le Stanc, Lucien Rapp, Michel Guibal (avec leurs collaboration), Lionel Costes (secrétaire général de la rédaction), ***Op.cit***, Page 1260.

(5)_ حتى نكون بصدد جريمة تزوير معلوماتي يجب أن يقع التزوير على وثيقة معلوماتية (في أغلب الأحيان محمية تقنيا من أي تعديل منطقي أو معلوماتي) يمكن الإطلاع عليها و التي يعترف بها كوسيلة إثبات حق أو واقعة قانونية.

الفرع الثاني : الركن المعنوي للجريمة

و هو نفس الركن المعنوي المعروف في جريمة التزوير التقليدية المتعلقة بالدعائم المادية كالمحررات.

في ما يخص القصد الجنائي العام : و هو توافر لدى المجرم إرادة تغيير الحقيقة مع علمه بأن التغيير قد تم في محرر (محرر معلوماتي)، أي محرر معلوماتي بإعتباره له نفس الأثر الذي يرتبه المحرر الكتابي حسب نص المادة 441-1 ق.ع.فرنسي[1].

القصد الجنائي العام لا يكفي وحده لقيام جريمة التزوير و بالتالي يجب توافر القصد الجنائي الخاص : و هو إتجاه نية المجرم إلى تحقيق غاية معينة من عملية التزوير[2].

---

[1]_ أنظر : أحسن بوسقيعة، "**الوجيز في القانون الجنائي الخاص**"، **الجزء الثاني : جرائم الموظفين، جرائم الأعمال، جرائم التزوير** ، دار هومه، طبعة 2004، (الجزائر)، من الصفحة 245 إلى 246.

[2]_ أنظر : أحسن بوسقيعة، **المرجـــع نفســـه**، من الصفحة 245 إلى 246.

المبحث الثالث :
جريمة السرقة المعلوماتية

يمكن أن نعرف بصفة عامة جريمة السرقة على أنها : "عملية إستيلاء ***"Usurpation"*** أو إختلاس ***"Soustraction"*** إحتيالي غير مشروع لمال مملوك للغير دون رضاه و لا علمه "، و بالتالي فجريمة السرقة بإمكانها أن تتضمن عنصري الخفية أو الإكراه.

هذا التعريف يمكن إستنباطه من نص المواد 311-1 ق.ع.فرنسي و 350 فقرة 1 ق.ع.جزائري[1]، و بالتالي هذه المواد نصت على القاعدة العامة بالنسبة لكل أنواع جرائم السرقة، إلا أن ذلك سيطرح إشكال خاصة و أن المشرع إلى حد الآن سواء الفرنسي أو الجزائري لم يمدد مضمون المواد المذكورة سابقا إلى ما يعرف حاليا بجريمة السرقة المعلوماتية (أي سرقة المعطيات المعلوماتية و بصفة عامة سرقة كل أنواع المعلومات و كذا سرقة وقت الكمبيوتر) و بالتالي الصعوبة التي تطرحها هذه المواد هو المال محل جريمة السرقة، بمعنى آخر تمديد مفهوم المال المملوك للغير (كل ما له وجود مادي) إلى المعلومات بكل أنواعها، بالإضافة إلى سرقة وقت الكمبيوتر (بإعتبارها أشياء منطقية أو معنوية) سواء بإدماجها في هذه المواد بموجب تعديل (كما هو الحال بالنسبة لجريمة سرقة المياه و الغاز و الكهرباء في الفقرة 3 من المادة 350 ق.ع.جزائري و المادة 311 مكرر 2 ق.ع.فرنسي) أو بواسطة الإجتهاد القضائي، إلا أن الأمر غير يسير كما هو في الظاهر لأسباب سنتكلم عنها في هذا المبحث.

سنركز دراستنا في هذا المبحث على جريمة سرقة المعلومات بصفة عامة و المعطيات المعلوماتية بصفة خاصة (مطلب أول) ثم جريمة سرقة وقت الكمبيوتر (مطلب ثاني) بإعتبارها الجرائم الأساسية في ما يخص السرقة المعلوماتية.

المطلب الأول : جريمة سرقة المعطيات المعلوماتية

كما قلنا في مقدمة هذا المبحث، فإن هنالك صعوبة منطقية لتطبيق النصوص العقابية التقليدية على سرقة المعطيات المعلوماتية.

هناك بعض الملاحظات التي يمكن عرضها في هذا الموضوع كما يلي :

---

[1] _ جرائم السرقة في التشريع الجزائري منصوص عليها في المواد من 350 إلى 371 ق.ع.جزائري في القسم الأول من الفصل الثالث من قانون العقوبات تحت عنوان "السرقات و إبتزاز الأموال".

1 - وجوب الأخذ بعين الإعتبار بأن المعطيات المعلوماتية في شتى أنواعها (مثلا : بيانات، برامج معلوماتية) هي عبارة عن معلومات (أشياء معنوية) و بالتالي فهي إبداعات فكرية مستقلة عن الدعامة المادية التي يمكن أن تحملها (أقراص مضغوطة أو مرنة) [1].

2 - هذه الإبداعات الفكرية أي المعلومة بصفة عامة مبدئيا هي ملك لكل الناس (إذ يمكن أن تكون في حيازة عدة أشخاص نظرا لسهولة نقلها، و في بعض الأحيان قد تفلت من أي إمكانية لتملكها و بالتالي تصبح أشياء مباحة) و لكن إستثناءا فإنها قد تكون محل ملكية خاصة [2] (ملكية تامة للمالك على المعلومة التي أنشأها) و حسب ما هو متعارف عليه حاليا فلا يمكن حماية المعلومة إلا في إيطار القانون الخاص بحماية الملكية الفكرية أي حقوق المؤلف كما هو الحال بالنسبة للمؤلفات الكتابية أما مشكلة السرقة المباشرة للمعلومة فلم يجرمها التشريع العقابي إلى حد الآن سواء الجزائري أو المقارن بنص تشريعي واضح.

الفرع الأول : جريمة السرقة الغير مباشرة للمعلومات (سرقة الدعامة المادية الحاملة للمعلومات)

هنا سنتكلم عن جريمة سرقة المعلومات و هي محمولة على دعامة مادية ***"Support Matériel"*** (الفقرة الأولى)، ثم سنستدل في هذه الجريمة بقرار محكمة النقض الفرنسية في قضية لو ڤلبكس "***LOGABAX***" الذي جاء بفكرة سرقة الدعامة المادية خلال المدة الزمنية اللازمة لنسخ ***"Reproduction"*** المعلومات التي تحملها (الفقرة الثانية)، و تجدر الإشارة إلى أن هذه الحيلة القانونية ***"Astuce juridique"*** و إن كانت تجرم أساسا سرقة الدعامة المادية إلا أنها بصفة غير مباشرة تجرم سرقة المعلومات التي تحملها هذه الدعامة المادية.

الفقرة الأولى : مضمون الجريمة

في هذه الحالة الإشكال لا يطرح، و بالتالي إذا قام المجرم بسرقة دعامة مادية (أسطوانة أو أي قرص مضغوط) محمولة بمعلومات في شكل معطيات فجريمة السرقة تعد قائمة كما هو الحال بالنسبة لسرقة كتاب مملوك للغير بإعتباره يحمل معلومات[3].

الإشكال الحقيقي سيظهر في هذه المسألة من الناحية العملية إذ أن القاضي الجزائي في هذه الحالة سيعتبر محل جريمة السرقة هي الدعامة المادية التي تحمل المعطيات و ليس المعطيات المعلوماتية نفسها، و المجرم

---

(1)_ أنظر : Michel Vivant (sous la direction), Christian Le Stanc, Lucien Rapp, Michel Guibal (avec leurs collaboration), Lionel Costes (secrétaire général de la rédaction), ***Op.cit***, Page 1250.

(2)_ أنظر : Michel Vivant (sous la direction), Christian Le Stanc, Lucien Rapp, Michel Guibal (avec leurs collaboration), Lionel Costes (secrétaire général de la rédaction), ***Idem***.

(3)_ أنظر : Michel Vivant (sous la direction), Christian Le Stanc, Lucien Rapp, Michel Guibal (avec leurs collaboration), Lionel Costes (secrétaire général de la rédaction), ***Idem***.

سيعاقب على هذا الأساس و ليس إلا، و إن كان الضرر المادي الناجم عن سرقة المعلومات المعلوماتية غالبا ما يكون أكبر بكثير من ضرر سرقة الدعامة المادية التي تحملها.

و تجدر الإشارة إلى أن تجريم سرقة الدعامة المادية الحاملة للمعطيات المعلوماتية يعد وسيلة ردعية فعال في حالات عديدة إذ أنها ستسمح بمعاقبة عدد كبير من قراصنة المعلوماتية[1].

الفقرة الثانية : قرار محكمة النقض الفرنسية في قضية لوقلبكس *"LOGABAX"*

الأصل أنه و كما سبق ذكره عندما يكون المال المعنوي ***" bien incorporel"*** بما في ذلك المعلومة و هي محمولة على دعامة مادية (مثلا : ورقة ، قرص متنقل ***"Disque Amovible"*** كالقرص المضغوط ***"CD-Rom"*** أو القرص الممغنط ***"Disquette"***)، هنا الإجتهاد القضائي يعترف بدون صعوبة بأن الكل يمكن أن يكون محل جريمة سرقة، وبما أنه لن يكون هنالك فصل ***"Séparation"*** بين الدعامة المادية و مضمونها (المعلومات) فهذه الجريمة ظاهريا لا تختلف عن جريمة السرقة التقليدية إلا أنه في القضية التي سنعرضها الإجتهاد القضائي جاء بفكرة أو حيلة قانونية جديدة تهدف إلى تجريم أساسا و بصفة مباشرة سرقة الدعامة المادية و بصفة غير مباشرة المعلومات التي تحملها هذه الدعامة[2].

قضية لوقلبكس طرحت على محكمة النقض الفرنسية [3]، و تتلخص وقائع القضية في أن عامل قام بنسخ عن طريق التصوير ***"Reproduction par photocopie"*** مسندات تتضمن مخطط إعادة هيكلة شركة لو قلبكس ***"Plan de restructuration"*** ليستعملها لصالحه أمام القسم العمالي***"L'instance prud'homale"*** [4].

في بداية الأمر القاضي الجزائي على مستوى المحكمة ***"1ère instance"*** أدان العامل على أساس جريمة السرقة.

غير أنه عند إستئناف العامل أمام المجلس القضائي ***"2ème instance"***، القاضي الجزائي برئه على أساس أنه لم يتم تبيين بأن هذا العامل الذي قام بنسخ المستندات في إيطار وظيفته قد تملكها إحتياليا[5] .

فيما بعد قررت شركة لوقلبكس تسجيل طعن بالنقض في قرار المجلس، و تبعا لذلك ألغت محكمة النقض قرار المجلس مستدلة في ذلك بأنه : "عند قيام العامل بنسخ المستندات التابعة للشركة لوقلبكس، و لأغراض شخصية

---

(1)_ أنظر : Michel Vivant (sous la direction), Christian Le Stanc, Lucien Rapp, Michel Guibal (avec leurs collaboration), Lionel Costes (secrétaire général de la rédaction), ***Op.cit***, Page 1242.

(2)_ أنظر : Laureen KRAFTCHIK, mémoire de master de recherche mention : droit pénal, ***Les appropriations frauduleuses et le recel de biens incorporels,*** sous la direction du : Professeur Alain DEKEUWER, Lille 2 (Université de droit et de la santé), Faculté des Sciences juridiques, Politiques et Sociales, année 2004-2005 (France), Page 13.

(3)_ ***Arrêt de la cour suprême française chambre pénale du 8 janvier 1979 (Affaire LOGABAX)***

(4)_ أنظر : Laureen KRAFTCHIK, ***Op.cit***, page 13.

(5)_ أنظر : Laureen KRAFTCHIK, ***Idem***.

بدون أي ترخيص و لا علم مالك هذه المستندات، فإن العامل بإعتباره لم يكن حائزا لها ماديا، قد تعرض لها و إستولى عليها إحتياليا خلال المدة اللازمة لإعادة نسخها"[1].

و على هذا الأساس محكمة النقض إعتبرت بأن جريمة السرقة قائمة ما دام أن العامل أثناء المدة اللازمة لقيامه بنسخ المستندات يعد قد تملكها بطريقة غير مشروعة أي دون ترخيص و لا علم مالكها الشرعي (و بالتالي هنالك تعرض إحتيالي للمستندات الأصلية خلال المدة اللازمة لإعادة نسخها)[2].

في ما يخص الركن المادي للجريمة : فيتمثل في الإختلاس القانوني للدعامة المادية ***"Soustraction juridique du support matériel"*** أي المستندات الأصلية بواسطة الإستيلاء على حيازتها، بالإضافة إلى سرقة إستعمال هذه الوثيقة ***"Vol d'usage des documents"*** خلال المدة اللازمة لإعادة نسخها[3].

الفرع الثاني : جريمة السرقة المباشرة للمعلومات (مستقلة عن الدعامة المادية)

المعطيات المعلوماتية و المعلومة بصفة عامة كما سبق ذكره هي إبداع فكري و يمكن إعتبارها مال أو ملك معنوي غير مادي، و بالتالي تكمن الصعوبة هنا في الإعتراف بتكييف المال المعلوماتي على أنه مال بالمعنى التقليدي[4] المنصوص و المجرم على سرقته في المواد 350 فقرة 1 ق.ع.جزائري و 311-1 ق.ع.فرنسي.

إذا أساس الخلاف بين رجال القانون في ما يخص سرقة المعطيات المعلوماتية هو المال محل الجريمة بإعتباره من العناصر الأساسية لجريمة السرقة (المال المعنوي) و كذا الوسيلة المستعملة في هذه الجريمة (الكمبيوتر و المعلوماتية) بإعتبار أن عنصر الإكراه ينتفي في هذه الجريمة[5].

من جهة أخرى مسألة معرفة ما إذا كانت المعطيات المعلوماتية بغض النظر عن دعامتها المادية، هل هي قابلة للسرقة أم لا ؟ يمكن طرحها خاصة إذا إعترفنا بأنها يمكن أن تدخل في عالم الأموال مثلما كان الأمر بالنسبة للطاقة (كهرباء، ماء، غاز)، و بالأدق بإعتبارها يمكن أن تكون موضوع ملكية خاصة، فهنا يطرح إشكال التملك الحقيقي لشيء معنوي غير مادي بالمعنى القانوني[6].

---

(1)_ أنظر : Laureen KRAFTCHIK, ***Op.cit***, page 13.

(2)_ أنظر : Laureen KRAFTCHIK, ***Idem***.

(3)_ أنظر : Laureen KRAFTCHIK, ***Idem***.

(4)_ أنظر : هدى حامد قشقوش، **مرجـــع سابـــق**، صفحة 72.

(5)_ بالإضافة إلى التحليل الذي سيأتي حول سرقة المعطيات المعلوماتية يمكن أيضا الإطلاع لمزيد من المعلومات حول السرقة المعلوماتية على مستند **(PDF)** تحت عنوان : ***« Espionnage économique et droit : l'inutile création d'un bien informationnel »*** المستنسخ Téléchargé من صفحة الأنترنت التالية : **http://www.lex-electronica.org/articles/v7-1/Dupre.pdf (de la Page 4 à 8 du document)**

(6)_ أنظر : André Lucas, Jean Devrèze, Jean Frayssinet, ***Op.cit***, Page 710.

غير أن سرقة المعطيات المعلوماتية لا يمكن مطابقتها على جريمة السرقة التي تستند فيها محل الجريمة أساسا إلى ما هو مادي، لأن جريمة سرقة ما هو معنوي تستضم بإشكالات في ما يخص الركن المادي للجريمة (بإعتبار أن المعلومة من طبيعتها يمكن نسخها إلى ما لا نهاية، فإن مالكها الأصلي و إن كان من المفروض لا يفقد ملكيتها[1] يمكن أن يحتج بحقه في عدم تبليغها للغير، إلا أن الجريمة في هذه الحالة تعد غير قائمة إستنادا إلى النصوص التقليدية)[2].

في ما يخص طبيعة الضرر المادي الناجم عن سرقة المعلومة المعلوماتية :
هنالك فرضية أولى تقول بأن الإستيلاء على هذه المعلومات بعد أن تم نسخها على دعامة مادية أخرى قد يؤدي إلى إحتمال الإفشاء بها إذا كانت هذه المعلومات سرية، إذا الضرر في هذه الحالة هو المساس بسرية المعلومة (كما هو الحل في ما يخص سر الصناعة ***"Secret de fabrication"***)[3].

أما الفرضية الثانية فترى بأنه إذا تعلقت جريمة السرقة بمعلومات معلوماتية غير قابلة للنسخ ***"Non duplicables"*** أو في حالة نسخها على دعامة مادية أخرى ثم حذفها (أي حذف النسخة الأصلية)، في هذه الحالة سرقتها تؤدي إلى إنتقال الملكية التامة للدعامة المعنوية من المجني عليه إلى الجاني مما يؤدي إلى فقدان مثلا معلومات مهمة، إذا الضرر هنا قد يكون مزدوج أي المساس بالملكية التامة للمعلومة و كذا المساس بسريتها إذا كان مالكها الأصلي لا يرغب أن يتطلع عليها الغير[4].

و في هذا الصدد سنرى بأن الإجتهاد القضائي الفرنسي تردد في ما يخص معرفة ما إذا كانت المعلومة وحدها قابلة للسرقة أم لا، كما سنرى بأن الفقه إختلف في هذه المسألة.

الفقرة الأولى : المبررات التي تسمح الإعتراف بهذه الجريمة

في سنة 1989، ظهر هنالك قرارين قضائيين صادرين عن الغرفة الجزائية لمحكمة النقض الفرنسية أحدثا ضجة كبيرة في ما يخص مسألة إمكانية تجريم السرقة المباشرة للمعلومات (أولا)، و لتدعيم هذه القرارات فإن الفقهاء المؤيدين لهذا الرأي لم يترددوا على تقديم تبريرات في سبيل الإعتراف القانوني بجريمة سرقة الأموال المعنوية ***"Le vol de biens incorporels"*** (ثانيا).

---

(1)_ أي أن الملكية التامة للمال المعنوي (المعطيات المعلوماتية مثلا) لا تنتقل من مالكها الأصلي إلى السارق رغم إستيلاء هذا الأخير عليها، بل هناك سرقة لمنفعة الشيء.

(2)_ أنظر : André Lucas, Jean Devrèze, Jean Frayssinet, ***Op.cit***, de la Page 710 à 711.

(3)_ أنظر : X. Linant de Bellefonds, A. Hollande, ***Op.cit***, Page 110.

(4)_ أنظر : X. Linant de Bellefonds, A. Hollande, ***Idem***.

أولا : المبررات القضائية من خلال قضيتي بوركان *"Bourquin"* و أنتنيولي *"Antoniolli"*

في ما يخص قضية بوركان *"Bourquin"* فإن قرار محكمة النقض الفرنسية [1] كان أول قرار يفتح المجال للمناقشات و الخلافات النظرية حول مسألة سرقة المال المعنوي، أي المعلومة و هي مستقلة عن أي دعامة مادية[2].

تتلخص وقائع القضية الأولى في أن عاملين أخذى معهما 70 أسطوانة ممغنطة *"Disquettes"* إلى منازلهم بهدف إعادة نسخها، ثم أعادها إلى مكان عملهم أين قاموا بنسخ 47 أسطوانة ممغنطة أخرى[3].

في بداية القضية القاضي الجزائي على مستوى المحكمة إعتبر العاملين المتابعين على أساس جريمة السرقة بريئين.

غير أن القاضي الجزائي لدى المجلس القضائي إعتبر أن العاملين مذنبين على أساس سرقة 70 أسطوانة ممغنطة أي سرقة الدعامات المادية *"Les supports matériels"* و كذا سرقة مضمون 47 أسطوانة ممغنطة أخرى (أي المعلومات المعلوماتية المحتواة فيها *"Les Informations informatiques"*) التي لم يخرجها العاملين من مكان عملهم (أي شركة الأسهم بوركان *"Société par action Bourquin"*)[4].

و عليه فإن العاملين سجلا طعن بالنقض في قرار المجلس، إلا أن هذه الأخيرة أخذت من جديد بنفس المبررات التي جاء بها قاضي الإستئناف قائلة : "بأنه يتضح من القرار المستأنف فيه بأن السيد ڤينني *"M. Guenu"* و السيد بوبار *"M. Boyer"* مذنبين على أساس سرقة 70 أسطوانة ممغنطة و كذا سرقة مضمون 47 أسطوانة ممغنطة أخرى و ذلك خلال المدة اللازمة لإعادة نسخ المعلومات التي كانت على متنها، الكل إضرارا بشركة الأسهم بوركان التي كانت مالكة لها (أي الأسطوانات الممغنطة و المعلومات التي تحملها)"[5].

و على هذا الأساس قررت محكمة النقض بدورها التمسك بقيام جريمة السرقة، و بالتالي رفض الطعن[6].

---

(1) _ ***Arrêt de cour suprême Française chambre pénale du 12 janvier 1989 (Affaire BOURQUIN)***

(2) _ أنظر : Laureen KRAFTCHIK, ***Op.cit***, Page 16.

(3) _ أنظر : Laureen KRAFTCHIK, ***Idem***.

(4) _ أنظر : Laureen KRAFTCHIK, ***Idem***.

(5) _ أنظر : Laureen KRAFTCHIK, ***Ibid***, de la Page 16 à 17.

(6) _ أنظر : Laureen KRAFTCHIK, ***Ibid***, Page 17.

في ما يخص قضية أنتونيولي ***"Antoniolli"*** فإن قرار محكمة النقض الفرنسية [1] في فتح بدوره هو الآخر من جديد المجال للمناقشات و الخلافات النظرية[2].

تتلخص وقائع هذه القضية الثانية، في أن عامل تحت تسمية أنتونيولي إستعمل مستندات محاسبة ***"Des documents comptables"*** تابعة للمؤسسة التي يعمل بها، لينشأ من خلالها جداول ***"Tableaux"*** و بيانات ***"Graphiques"*** و التي وفرها فيما بعد لمؤسسة أخرى منافسة ***"Entreprise concurrente"*** [3].

أمام المحكمة الإبتدائية العامل المتابع لم يتم إدانته على أساس جريمة السرقة، إلا أن القاضي الجزائي للمجلس القضائي أدانه على هذا الأساس[4].

نتيجة لذلك قام العامل بتسجيل الطعن النقض في هذا القرار و من بين مبرراته أنه كان على قاضي الغرفة الجزائية أن يكيف محل الجريمة بأنها مال معنوي ***"Bien incorporel"*** (أي إبلاغ معلومات ***"Communication de renseignements"***) بدون إثبات فعل الإستلاء الإحتيالي (الإختلاس) ***"La soustraction frauduleuse"*** و بالتالي قاضي المجلس كان خاطئ عندما جرم فعل إختلاس المعلومات ما دام أن التشريع العقابي لا يمتد إلى هذا النوع المستحدث من الجرائم، و من هنا حاول العامل تبيين بأن الأشياء المادية وحدها قابلة للإختلاس دون الأشياء المعنوية[5].

غير أن محكمة النقض لم تأخذ بعين الإعتبار هذا التبرير الذي جاء به محامي المتهم و قضت بأن : "المتهم أنتونيولي إستولى على حيازة المستندات و بالتالي إرتكب فعل الإستيلاء الإحتيالي على المعطيات الحسابية و التجارية ***"Les données comptables et commerciales"*** الموجودة على متن المستندات و التي سلمها للغير، إذا جريمة السرقة مؤسسة إذ المعطيات الحسابية و التجارية التي تشكل أموال معنوية تعد قانونيا الملكية الخاصة للمؤسسة إستاينو ***"L'entreprise ESTAYNOU "*** ..."[6].

---

[1] _ ***Arrêt de cour suprême Française chambre pénale du 1 mars 1989 (Affaire ANTONIOLLI)***

[2] _ أنظر : Laureen KRAFTCHIK, ***Op.cit***, page 17.

[3] _ أنظر : Laureen KRAFTCHIK, ***Idem***.

[4] _ أنظر : Laureen KRAFTCHIK, ***Idem***.

[5] _ أنظر : Laureen KRAFTCHIK, ***Idem***.

[6] _ أنظر : Laureen KRAFTCHIK, ***Idem***.

ثانيا : المبررات الفقهية التي تسمح الإعتراف بالسرقة المباشرة للأموال المعنوية

في ما يخص القرارات الصادرة في 1989، فإن فقهاء القانون فسروها بأنها إعتراف صريح من طرف العدالة الجزائية لكون أن السرقة المباشرة للمعلومات تشكل جريمة مثلها مثل جريمة السرقة للأموال المادية، و بالتالي تبريرات الفقهاء في ما يخص تجريم هذا النوع من السرقات كان على أساس العقوبات المقررة بشأنها (1)، و كذا القيمة و الأهمية أو الوظيفة الإقتصادية المسندة إليها (2).

1- من حيث العقوبات (الغرامات المالية) المقررة بشأنها

الحكمة من هذا التبرير هو أن القاضي الجزائي كقاعدة عامة يأخذ بعين الإعتبار قيمة المال المعنوي ***"La valeur du bien incorporel"*** أي المعلومة ***"L'information"*** [(1)].

و ما يدل على ذلك قضية إربيرتو ***"Herberteau"*** [(2)] التي طرحت على مستوى محكمة النقض الفرنسية، ملخص هذه القضية هو أن عاملين أحدهما تحت تسمية إربيرتو قاما بنسخ مخططات لآلات تابعة للمؤسسة التي يعملون بها بهدف المتاجرة بها، و تجدر الإشارة إلى أن قضاة محكمة النقض أيدوا القرار الذي جاء به قاضي الإستئناف لمجلس قضاء بواتيي ***"Poitiers"***، أي جريمة سرقة المخططات خلال المدة اللازمة لإعادة نسخها (نفس الحل الذي جاءت به محكمة النقض في قضية لو ڤلبكس ***"LOGABAX"***)، و لكن ما جلب نظرنا في هذه القضية و إن كانت في الأصل تتعلق بسرقة دعامة مادية خلال المدة اللازمة لإعادة نسخها هو أن التعويض المقرر من طرف قاضي الإستئناف و المؤيدة من طرف محكمة النقض قدرة بـــ 6 آلاف فرنك فرنسي، و بالتالي يتضح من هذه القضية أن القاضي الجزائي أراد تجريم بصفة غير مباشرة سرقة المعلومات و ليس مجرد سرقة أوراق التي تحتوي على المخططات التي تعد ذات قيمة مالية تافهة[(3)].

و هذا الحل سنجده أيضا في قضية أونتونيولي ***"Antoniolli"***، حيث أن قرار المجلس القضائي و المؤيد من طرف محكمة النقض أدان العامل المتهم و قدر التعويض بـــ 30 ألف فرنك فرنسي و تجدر الإشارة إلى أن هذا التعويض مثل ما هو الحال في القضية السالفة الذكر يعد عقوبة مدنية مشددة، و بالتالي القاضي الجزائي لم يؤخذ فقط في تقدير التعويض بقيمة الدعامة المادية الحاملة للمعلومة بل زيادة على ذلك أخذ بعين الإعتبار قيمة المعلومات التي كانت هي الأخرى في نظره محل الجريمة[(4)].

---

(1)_ أنظر : Laureen KRAFTCHIK, ***Op.cit,*** Page 18.

(2)_ ***Arrêt de cour suprême Française chambre pénale du 29 avril 1986 (Affaire HERBERTEAU)***

(3)_ أنظر : Laureen KRAFTCHIK, ***Op.cit***, page 18.

(4)_ أنظر : Laureen KRAFTCHIK, ***Idem***.

و بالتالي ما يمكن أن نستنتجه هو أن القاضي الجزائي الفرنسي لا يؤخذ فقط بعين الإعتبار الضرر الناتج عن سرقة الدعامة المادية و التي هي في أغلب الأحيان ذات قيمة تافهة بل يؤخذ أيضا بعين الإعتبار القيمة المالية للمعلومات المحتواة في الدعامة و التي تعد في أغلب الأحيان ذات قيمة باهضة.

2- من حيث القيمة و الأهمية المالية للمال المعنوي (المعلومة)

اليوم بعض الأموال المعنوية (أي المعلومات) لها قيمة مصرفية و مالية حقيقية، و لهذا الفقهاء المؤيدين لهذه الفكرة وضعوا كقاعدة أنه لسبب قيمتها المالية فالمعلومة يجب أن يكون لها نظام قانوني خاص بها، و إذا كانت المعلومة لها نفس القيمة المالية التي نجدها في الأموال المادية فعلى هذا الأساس تستحق أن تكون محمية جنائيا على نفس مستوى المال المادي، كما أن الإعتراف بأن المعلومة لها قيمة مالية سيدفع بالمشرع و القضاء إلى الإعتراف بأنه يمكن أن تكون محل ملكية و بالتالي يمكن أن تكون محل جريمة السرقة[1].

وفقا لما ذهب إليه هؤلاء الفقهاء في هذا التحليل فإن المال المعنوي (المعلومات) لا يمكن أن تكون محل ملكية إلا إذا كانت ذات قيمة إقتصادية حقيقية ***"Valeur économique réelle"*** [2] و بالتالي من الناحية العملية في غياب نصوص في هذا الصدد فإن القاضي هو الذي يقدر ذلك مثلما حدث في قضية إربيرتو ***"Herberteau"*** و أونتونيولي ***"Antoniolli"***.

هنالك تسائل يمكن أن نطرحه بشأن مدى إمكانية الإعتراف للمعلومات المعلوماتية بأن لها قيمة مالية مثل الماء أو الكهرباء المعلومات المعلوماتية المسروقة يمكن قياس كميتها بسهولة (مثلا : طول الشريط الممغنط، أو مدة الإتصال ***"Durée de transmission"***، أو حجم المعطيات المعلوماتية)، إلا أن القيمة المالية للمعلومة لا يمكن ربطها مباشرتا بكميتها التي تم الإستيلاء عليها، إلا أن هذا الأمر لا يمنع وجود حالات إستثنائية يمكن أن تقدر فيها قيمة المال المعنوي المسروق كما هو الحال بالنسبة للبرامج المعلوماتية المصممة خصيصا لشركة ما (قيمتها المالية يحددها مصممها ***"Le programmeur"***)، أو قاعدة معطيات ***"Banque de données"*** التي تطلبت مدة زمنية معينة لإنجازها و عدد من المختصين في المعلوماتية لتصميمها، في هذه الحالة قيمتها المالية تقاس وفقا لهذه المدة بالإضافة إلى تكلفة توظيف هؤلاء المختصين لإنجازها[3].

---

(1)_ أنظر : Laureen KRAFTCHIK, ***Op.cit***, Page 19.

(2)_ أنظر : Laureen KRAFTCHIK, ***Idem***.

(3)_ أنظر : X. Linant de Bellefonds, A. Hollande, ***Op.cit***, Page 110.

الفقرة الثانية : المبررات التي تنفي الإعتراف بهذه الجريمة

الفقهاء المعارضين لفكرة إمكانية تملك المعلومات كمال معنوي و بالتالي إمكانية إختلاسها، يستدلون في ذلك بالشروط الواجب توافرها لقيام جريمة السرقة و منها شرط وجود شيء قابل للإختلاس (أولا)، و كذا شرط وجود فعل الإختلاس كركن مادي أساسي لقيام الجريمة (ثانيا).

أولا : شرط أن يكون الشيء قابل للإختلاس

هنا سنرى بأن الإعتراف بإمكانية السرقة المباشرة للمعلومات كمال معنوي تتنافى مع طبيعة تكييف الجريمة بأنها سرقة (1)، و من جهة أخرى يرى هؤلاء الفقهاء بأن القرارات القضائية الفرنسية الصادرة في 1989 لا تعترف في الحقيقة بسرقة المعلومة وحدها منفصلة عن دعامتها المادية (2)، كما سنلاحظ بأن النصوص التقليدية بخصوص جريمة السرقة لا تسمح منطقيا بحكم صياغتها من تجريم سرقة المعلومات (3).

1- تعارض الإعتراف بسرقة المعلومات بالمفهوم التقليدي لجريمة السرقة

أي أن طبيعة جريمة السرقة تمنع تمديد فعل الإختلاس إلى ما هو معنوي (المعلومات)، إذ أن جريمة السرقة و كما قلناه في مقدمة هذا المبحث تتضمن عنصري الخفية و الإكراه الذي يهدد الشخص المالك للشيء، بإعتبار جريمة السرقة من طبيعتها أنها تستعمل فيها العنف الذي يهدد مالك الشيء، هذا إذا كنا بصدد إختلاس مال مادي[1].

إلا أن التكييف سيختلف إذا إعترفنا بإمكانية إختلاس المعلومات كمال معنوي، إذ أن سرقة المعلومات هي عبارة عن جريمة تستعمل فيها الحيلة و إن كانت تتم في الخفاء مثل ما هو الحال بالنسبة لسرقة المال المادي إلا أنه لا يمكن إستعمال فيها الإكراه أي بدون إمكانية خلق خطر جسماني للمالك الشرعي للمال المعنوي (المعلومات)[2].

---

(1)_ أنظر : Laureen KRAFTCHIK, ***Op.cit***, Page 21.

(2)_ أنظر : Laureen KRAFTCHIK, ***Idem***.

2- القرارات القضائية الفرنسية لسنة 1989 لا تعترف في الحقيقة بسرقة المعلومات مستقلة عن دعامتها المادية

بالنسبة للفقهاء المؤيدين لفكرة شرط الوجود المادي للمال محل الجريمة، فإن القرارات الصادرة في 1989 كانت في الأصل لن تعترف صراحة بقيام جريمة سرقة المال المعنوي إذا لم يكن هنالك سرقة للدعامة المادية (أسطوانات ممغنطة أو وثائق مثلا)[1].

فالمضمون المعلوماتي للأسطوانات الممغنطة كان من غير الممكن التعرض لها إذا لم يكن هنالك إختلاس للدعامة المادية التي تحملها، و بالتالي الدعامة المادية تم إختلاسها قبل إختلاس مضمونها أي المعلومات، و بالتالي حسب هؤلاء الفقهاء فإننا عدنا إلى الحالة الكلاسيكية في ما يخص سرقة الأسطوانات الممغنطة كمال مادي الشيء الذي قيد القاضي الجزائي و دفع به إلى الإعتراف بوجود جريمة سرقة بمفهومها التقليدي لا أكثر[2].

و بالتالي سرقة المعلومات لم يأخذها القاضي الجزائي بعين الإعتبار إلا في ما يخص الركن المعنوي للجريمة أي الدافع[3].

3- الصعوبات في ظل النصوص العقابية التقليدية

كقاعدة عامة يجب أن يكون المال محل جريمة السرقة سواء في القانون الفرنسي أو الجزائري مال مملوك للغير و بالتالي شيء قابل لتملكه[4].

حسب هذه القاعدة العامة، الفقه و الإجتهاد القضائي يفرض أن يكون هنالك وجود مال مادي قابل للتملك و تصرف مادي أي فعل الإختلاس أي قيام جريمة سرقة بمفهومها التقليدي، و بالتالي يشترط أن يكون محل جريمة السرقة مال مادي ***"Bien corporel"***، و حسب هذه القاعدة الأساسية يستبعد تجريم سرقة الأموال المعنوية (المعلومات) و تجدر الإشارة في هذا الصدد بأن الأستاذ كاربونيي ***"M. Carbonnier"*** قال : "الأموال عبارة عن أشياء يراها القانون "، حسب هذه المقولة فالأشياء حتى تكون محل حماية قانونية يجب أولا أن يعترف بها

---

(1)_ أنظر : Laureen KRAFTCHIK, ***Op.cit***, page 21.

(2)_ أنظر : Laureen KRAFTCHIK, ***Ibid***, de la Page 21 à 22.

(3)_ أنظر : Laureen KRAFTCHIK, ***Ibid***, Page 22.

(4)_ أنظر : Laureen KRAFTCHIK, ***Idem***.

القانون صراحة أي بنص، و بالتالي ما دام لم ينص المشرع على الأموال المعنوية كمحل للجريمة في قانون العقوبات فإنه منطقيا لا يمكن متابعة من إختلس المعلومات أيا كان نوعها[1].

ثانيا : شرط وجود فعل إختلاس

هنا يمكن أن نلاحظ عارضين لإمكانية الإعتراف بأن فعل الإستيلاء على المعلومات يشكل جريمة.

1- إحتمال الإنحراف إلى إختلاس فكري بحث

فعل الإختلاس يشكل الركن المادي الأساسي في جريمة السرقة، إلا أن المشرع بصفة عامة لم يعرف فعل الإختلاس و بالتالي الفقه و الإجتهاد القضائي هما اللذان عرفا و حددا مضمونه، حيث أنه أعطي له تعريفين [2] :

التعريف الأول وضع كمفهوم ما يسمى بالإختلاس المادي ***"La soustraction Matériel"*** و حسب هذا التعريف يفهم من كلمة إختلاس نقل حيازة الشيء من المجني عليه إلى الجاني[3].

التعريف الثاني جاء بمصطلح الإختلاس القانوني ***"La soustraction juridique"***، الأساس الفقهي لهذا التعريف يرجع إلى الأستاذ إيميل قلوسون ***"Emile Garçon"*** الذي يرى بأن الإختلاس هو الإستيلاء على الملكية بعنصريها المادي و المعنوي و بالتالي فعل الإختلاس لم يعد يفهم على أساس أنه مجرد تصرف بل هو أيضا إستنتاج بأن الشخص سلب من ملكيته ماديا و معنويا[4].

الآن السؤال الذي يمكن طرحه هو هل يمكن تطبيق صورتي فعل الإختلاس على المال المعنوي (المعلومة) ؟ حاليا لا يمكن تصور وجود إستيلاء لمال معنوي لسبب بسيط هو عدم توافر فعل مادي في الجريمة و لا شيء مادي قابل للإستيلاء، وتجدر الإشارة إلى أن الإعتراف بمثل هذا التصرف يؤدي بنا إلى الإعتراف بأنه يمكن أن تقوم جريمة السرقة دون توافر فعل أو تصرف مادي و لا شرط وجود شيء مادي قابل لسلبه من حيازة مالكه الشرعي و هذا ما يسمى بالإختلاس الفكري ***"Soustraction intellectuelle"*** الذي في نظر الفقهاء يتناف مع التعريفين السابقين[5].

---

(1)_ أنظر : Laureen KRAFTCHIK, ***Op.cit***, Page 23.

(2)_ أنظر : Laureen KRAFTCHIK, ***Ibid***, Page 27.

(3)_ أنظر : Laureen KRAFTCHIK, ***Idem***.

(4)_ أنظر : Laureen KRAFTCHIK, ***Ibid***, de la Page 27 à 28.

(5)_ أنظر : Laureen KRAFTCHIK, ***Ibid***, Page 30.

2- إنعدام وجود إختلاس تام للمال المعنوي (المعلومة)

كلاسيكيا فعل الإختلاس يتمثل في سلب ملكية شخص حتى و إن كان ذلك لمدة زمنية معينة ثم تعود إليه، إلا أنه إذا إعترفنا بوجود إمكانية إختلاس معلومات فإن هذه المعلومات في الحقيقة رغم إختلاسها فإنها تبقى أيضا في حيازة مالكها الشرعي و بالتالي ليس هنالك سرقة، و ما يبين ذلك قرار مجلس قضاء باريس في قضية قناة + *CANAL* في 24 جوان 1987، الذي رفض فيه القاضي الجزائي تطبيق جريمة السرقة على قرصنة الموجات الهوائية الهرتزية المحمية برموز أو شفرة سرية ***"Les ondes hertziennes codées"*** بإعتبارها أموال معنوية، على أساس أن الإتصال الإحتيالي لم يهدف إلى سلب مالك القناة + من برامجه الذي يواصل رغم ذلك في بثها و لا سلب المتفرج من حقه في المشاهدة و الذي لم يتعرض لأي خلل في تلقيه لبرامج قناة +[1].

الحيلة في سرقة المعلومات هو قيام السارق بنسخها ***"Reproduction"*** دون سلبها من مالكها الشرعي و بالتالي فعل الإختلاس ينتفي. لكن هذا لا يعني أن قرصنة الأرقام السرية أو شفراة قناة التلفزة المدفوعة الأجر لا تشكل جريمة.

المطلب الثاني : جريمة سرقة وقت الكمبيوتر

سرقة وقت الكمبيوتر ***"Le vol du temps ordinateur"*** أو الإستغلال الغير مشروع للكمبيوتر ***"L'utilisation ou l'exploitation illégale de l'ordinateur"*** [2] يقصد به إستخدام الحاسب الآلي بطريقة غير مصرح بها للمعالجة الآلية لمعطيات، بيانات، حسابات منطقية مثلا، أي إستخدام وقت الحاسب الآلي أو وقت الآلة لأغراض شخصية دون تصريح و لا ترخيص من صاحب الحاسب الآلي، وتجدر الإشارة إلى أن سرقة وقت الحاسب الآلي من الجرائم الشائعة في مجال المعلوماتية[3].

من جهة أخرى سرقة وقت الكمبيوتر قد تتجسد في جملة من التصرفات المادية كتشغيل جهاز الكمبيوتر مثلا و عادة تليها أفعال معنوية أو معلوماتية تتمثل مثلا في تشغيل برامج أو فتح مستندات معلوماتية و كل هذا يشكل وقت و منفعة مأخوذة على حساب صاحب جهاز أو أجهزة الكمبيوتر كما هو الحال في نوادي الأنترنت ***"Les cybercafés"***، و بالتالي وقت الكمبيوتر هو مال ***"Un bien économique"*** يمكن قياسه[4].

---

(1) _ أنظر : Laureen KRAFTCHIK, ***Op.cit***, Page 32.

(2) _ أنظر : محمد أمين الرومي، "**جرائم الكمبيوتر و الأنترنت**"، دار المطبوعات الجامعية، طبعة 2004، الإسكندرية (مصر)، صفحة 49.

(3) _ أنظر : محمد سامي الشوا، "**ثورة المعلومات و إنعكاساتها على قانون العقوبات**"، دار النهضة العربية، سنة 1993، القاهرة (مصر)، صفحة 85.

(4) _ أنظر : Hollande Alain, De Bellefonds Linant Xavier, ***Op.cit***, Page 257.

وتجدر الإشارة إلى أن الإستغلال الغير مشروع لوقت الكمبيوتر يجعل قدرات الكمبيوتر جزئيا أو كليا مجمدة ***"Mobilisé"*** لحساب السارق وحده على حساب حق المستعملين الشرعيين الآخرين[1].

يمكن أن نلاحظ بأن الإستغلال الغير مشروع للكمبيوتر أو وقت الكمبيوتر يظهر من خلال سرقة الطاقة الكهربائية، مع العلم أن سرقة الطاقة الكهربائية معاقب عنها قانونا إلا أنه يجب أن نحذر إذ أن المتابعة الجزائية في حالة إستعمال الغير مشروع للكمبيوتر لا تتم إلا إذا كان هنالك إستهلاك مبالغ في الطاقة الكهربائية أي حجم كبير من الطاقة و غير عادي، إلا أن ذلك قد يكون غير ممكن لأن الوحدة المركزية للكمبيوتر بعد تشغيلها تستهلك كمية منتظمة و غير مبالغ فيها من الطاقة الكهربائية مما يجعل إمكانية المتابعة الجزائية مستحيلة[2].

---

(1)_ أنظر : Hollande Alain, De Bellefonds Linant Xavier, ***Op.cit***, page 257.

(2)_ أنظر : Michel Vivant (sous la direction), Christian Le Stanc, Lucien Rapp, Michel Guibal (avec leurs collaboration), Lionel Costes (secrétaire général de la rédaction), ***Op.cit***, Page 1242.

المبحث الرابع :

جريمة النصب المعلوماتي

في هذا المبحث سنتكلم عن النصب المعلوماتي، لكن هذا لا يعني أن هنالك في القانون جريمة نصب خاصة بمجال المعلوماتية، و بالتالي لا يوجد إلا جريمة النصب وفقا لما هو متعارف عليه في النصوص التقليدية [1]، أما السؤال الذي يجب طرحه هنا هو ما مدى إمكانية تطبيق النصوص العقابية التقليدية على حالة التصرفات ذات هدف إحتيالي بإستعمال المعلوماتية ضد مال الغير ؟

سنتكلم أولا عن جريمة النصب كجريمة تقليدية من حيث العموميات (المطلب الأول)، ثم نرى بخصوص جريمة النصب في محيط المعلوماتية ***"En milieu informatique ou virtuel"*** مدى إمكانية الإستلاء على مال الغير بواسطة التقنية المعلوماتية (المطلب الثاني)، و هل يمكن تسليم المال عن طريق التحويل الإلكتروني ؟ و هل تقوم الجريمة إذا كان المال المستولى عليه مال معنوي ؟ (المطلب الثالث).

المطلب الأول : عموميات حول جريمة النصب كجريمة تقليدية في الأصل

جريمة النصب بصفة عامة هي "الإستيلاء ***"Usurpation"*** على الحيازة الكاملة لمال الغير بوسيلة يشوبها الخداع ***"Par un moyen frauduleux"*** تسفر عن تسليم ذلك المال"[2]، أو هو "الإستيلاء بطريقة الإحتيال على شيء مملوك للغير بنية تملكه".

المشرع الفرنسي نص على هذه الجريمة بموجب المادة 313-1 ق.ع، المشرع المصري نص عليها في المادة 336 ق.ع أما المشرع الجزائري فنص عليها في المادة 372 ق.ع.

من خلال التطلع على هذه المواد يمكن أن نلاحظ بأن جريمة النصب تقوم على ركنين أساسيين أي الركن المادي الذي يتألف من فعل هو الكذب و وسيلة الإحتيال أو التدليس ثم نتيجة تتمثل في الإستيلاء على مال الغير و علاقة سببية بين الإحتيال و الإستيلاء و هو ما يقتضي أن يكون التسليم مرحلة لاحقة لإستعمال التدليس و يجب أيضا أن تكون الوسائل الإحتيالية من شأنها أن تؤدي إلى تسليم المال نتيجة إنخداع الضحية بها[3]، وقد حدد المشرع الجزائري و المصري وسيلة الإحتيال بإحدى الطرق التي نص عليها على سبيل

---

(1)_ أنظر : Michel Vivant (sous la direction), Christian Le Stanc, Lucien Rapp, Michel Guibal (avec leurs collaboration), Lionel Costes (secrétaire général de la rédaction), ***Op.cit***, Page 1218.

(2)_ أنظر : هشام محمد فريد رستم، **مرجـــع سابـــق** ، صفحة 268.

(3)_ أنظر : أحسن بوسقيعة، "**الوجيز في القانون الجزائي الخاص** "، **الجزء الثاني : جرائم الموظفين، جرائم الأعمال، جرائم التزوير** ، **مرجـــع سابـــق**، صفحة 314.

الحصر، وبالتالي إذا وقع الإحتيال بوسيلة غير الوسائل التي نص عليها المشرع و لو ترتب عنها تسليم المجني عليه المال إلى الجاني فهنا تنتفي جريمة النصب[1].

و من هنا الوسائل المذكور على سبيل الحصر تتمثل في : إستعمال وسيلة من وسائل التدليس و الإحتيال[2] بالإضافة إلى الكذب من شأنها أو من طبيعتها إيقاع المجني عليه في خطأ ***"De nature a induire la victime en erreur"***، هذه الوسائل التدليسية مختلفة قد تتمثل في إتخاذ الجاني إسم كاذب أو صفة كاذبة، أو في مناورات إحتيالية المتمثلة في : إيهام الناس بوجود سلطة خيالية أو إعتماد مالي خيالي أو وجود مشاريع كاذبة (هذه الحالة موجودة في النص المادة الفرنسي) أو إحداث الأمل في الفوز أو الخشية من وقوع حادث أو واقعة وهمية يترتب عنها تسليم المال إلى الجاني الذي يتصرف فيه رغم أنه غير مملوك له و ليس له الحق للتصرف فيه[3].

المشرع الفرنسي في المادة 313-1 ق.ع أضاف وسيلة أخرى من بين الوسائل الأخرى السالفة الذكر لم يذكرها لا المشرع الجزائري و لا المصري و المتمثلة في التعسف في إستعمال صفة حقيقية ***"L'abus d'une qualité vraie".***

من جهة أخرى المشرع الجزائري على خلاف المشرع المصري و الفرنسي نص على الشروع في جريمة النصب أي وجود جملة من الأفعال و المناورات الإحتيالية تحيل الفهم إلى أن الجاني سيرتكب الجريمة و لكن لسبب خارج عن إرادته لا تتحقق النتيجة أي سلب مال الغير بالتسليم، و بالتالي عاقب عليها من خلال المادة 372 ق.ع.

في ما يخص المناورات الإحتيالية : فجاءت في المادة 372 ق.ع.جزائري على سبيل الحصر كما ذكر سابقا، و تجدر الإشارة إلى أن المشرع الفرنسي على عكس المشرع الجزائري لم يحدد في المادة 313-1 ق.ع على سبيل الحصر المناورات الإحتيالية.

---

(1)_ أنظر : هشام محمد فريد رستم، **مرجـــع سابـــق**، صفحة 269.

(2)_ الهدف الأساسي من وسائل التدليس هو إعطاء للأقوال الكاذبة للجاني قوة إقناع وإزالة الشك لدى المجني عليه و التي تجعله في ما بعد يسلم إراديا ماله إلى الجاني.

(3)_ أنظر : هشام محمد فريد رستم، **مرجـــع سابـــق**، صفحة 269.

في ما يخص الركن المعنوي : لجريمة النصب فيتخذ صورة القصد العام بالإضافة إلى القصد الخاص الذي هو عبارة عن نية المتهم في الإستيلاء على مال الغير، فإذا كان الهدف من الإحتيال مجرد المزاح أو مجرد منفعة عابرة فلا تقوم الجريمة[1].

المطلب الثاني : مدى إمكانية الإحتيال في محيط المعلوماتية

بعد تطرقنا لجريمة النصب بصفة عامة كيفما هو متعارف عليه، الآن يأتي الإشكال الذي ثار و لا زال يثور إلى حد الآن في الفقه و هو مدى توافر أركان جريمة النصب في الحالات التي يتوصل فيها الجاني بواسطة التلاعب بالأنظمة المعلوماتية إلى الإستيلاء على مال الغير : و مثال ذلك الشخص الذي يتلاعب في المعطيات المخزنة في ذاكرة جهاز الكمبيوتر أو في برامجه لإستخراج شيكات أو أرصدة تدفع له، أو حالة تحويل الجاني بواسطة المعلوماتية كل أو بعض أرصدة الغير أو الفوائد المستحقة لهم إلى حسابه، كذلك حالة التلاعب في الإشارات الإلكترونية التي يوجهها الحاسب المركزي للبنك إلى الموزع الآلي للنقود لإختلاس أموال من أرصدة العملاء أو من رصيد الموزع الآلي للنقود[2].

كل هذه الحالات جديدة بالنسبة للمشرع الحالي و القضاء و بالتالي تولى الفقه مسؤولية الفصل في هذه المسائل و الذي إختلفت أرائه فيها.

ففي ما يخص المقصود من المناورات الإحتيالية في ما يخص جريمة النصب المعلوماتي :
المناورات الإحتيالية يقصد بها هنا الأفعال و التصرفات المعلوماتية (كتلاعب الجاني بالبرامج و المعطيات بهدف إيقاع المجني عليه في غلط) و التي تشكل العنصر الخارجي لعملية الكذب، و في هذا المجال يقول الفقيهين سارڤو و ماسي ***"M. Sargos et Massye"*** بأنه لا يشترط تعديل النصوص التقليدية لجريمة النصب في ما يخص النصب المعلوماتي إذ أن إستعمال الكمبيوتر كممثل أو مؤثر بالإضافة إلى الكذب تشكل مناورات إحتيالية و بالتالي النصوص التقليدية قابلة للتطبيق[3].

في ما يخص إشكالية ما إذا كان بإمكان الجاني الإحتيال على النظام المعلوماتي و إيقاعه في غلط أم أن الإحتيال رغم إستعمال تقنية المعلوماتية لا يكون إلا ضد مال شخص آخر :

---

(1)_ أنظر : أحسن بوسقيعة، "**الوجيز في القانون الجزائي الخاص** "، **الجزء الثاني : جرائم الموظفين، جرائم الأعمال، جرائم التزوير ، مرجـــع سابـــق**، صفحة 315.

(2)_ أنظر : هشام محمد فريد رستم، **مرجـــع سابـــق**، من الصفحة 269 إلى 270.

(3)_ أنظر: Michel Vivant (sous la direction), Christian Le Stanc, Lucien Rapp, Michel Guibal (avec leurs collaboration), Lionel Costes (secrétaire général de la rédaction), ***Op.cit***, Page 1219.

أولا و قبل كل شيء تجدر الإشارة إلى أن نطاق المعلوماتية لم يضيف شيئا جديدا إلى جريمة النصب من الناحية النظرية و بالتالي التشريع العقابي الجزائري و المقارن حول جريمة النصب قابلة للتطبيق في مجال المعلوماتية، أما الشيء الجديد الذي جاء به نطاق المعلوماتية هو من الناحية العملية أي الوسيلة المستعملة لإرتكاب جريمة النصب (الحاسب الآلي).

من جهة أخرى تجدر الإشارة إلى أن إمكانية الإحتيال على النظام المعلوماتي و إيقاعه في الغلط كان محل خلاف كبير بين فقهاء القانون، إذ كقاعدة عامة معظم التشريعات الجنائية بالإضافة إلى الجزائري تحدد السلوك المادي لجريمة النصب و المتمثل في الكذب البالغ درجة الإحتيال الذي ينتج عنه تسليم المجني عليه إراديا مالا من أمواله إلى الجاني، و يستفاد من نموذج الجريمة كما حددته قاعدة التجريم في عدد كبير من التقنينات أن " شخصا " طبيعيا أو معنويا هو الذي يجب أن يقع عليه فعل الإحتيال، و مفاد ذلك أن قابلية تطبيق النصوص العقابية لجريمة النصب على الإحتيال الذي يباشر على الأنظمة المعلوماتية تتوقف على شرط أن يكون الجاني قد خدع أيضا الشخص الذي يستعمل المعلوماتية كفحص أو مراجعة المعطيات المرسلة من طرف الجاني[1].

يرى القاضي جاي ڤو ***"M. Jaeger"*** أحد الفقهاء في القانون، بأنه لا يمكن أن يطبق قانون العقوبات اللوكسمبرجوازي في ما يخص جريمة النصب على الجهاز المعلوماتي لأن جهاز المعلوماتية يستعملها في الأصل شخص جاني ضد المجني عليه الذي يكون قد خدع و ليس الجهاز المعلوماتي الذي في حقيقة الأمر لا يلعب في هذه الجريمة إلا دور الوسيط[2].

في حين أن جانب من الفقه الفرنسي يرى بأن خداع الأنظمة المعلوماتية لسلب المال تتحقق به الطرق الإحتيالية بمفهومها المستقر أي الكذب مدعم بمناورات إحتيالية تتمثل في جملة من الأعمال المادية أو الوقائع الخارجية المتمثلة في تقديم الجاني معطيات معلوماتية بواسطة إدخالها إلى نظام المعلوماتية التي سيطلع عليها في ما بعد المجني عليه، كما قد تتحقق المناورات الإحتيالية بإستخدام الجاني معطيات غير صحيحة أو خاطئة التي يخرجها من الجهاز المعلوماتي بعد أن تلاعب بالبرامج أو المعطيات المعلوماتية المخزنة فيه، و ذلك بهدف الإستيلاء على أموال لا حق له فيها، و بالتالي يكفي أن يستولي الجاني بواسطة المعلوماتية كوسيلة مناورات إحتيالية على أموال ليس له حق فيها حتى تعد جريمة النصب قائمة[3] .

إلا أن جانب آخر من الفقه الفرنسي يرى عدم إمكانية إرتكاب جريمة النصب إلا إذا كانت تنطوي على علاقة مباشرة بين شخصين (المحتال و المخدوع)، و هو ما ينتفي في حالة مباشرة الطرق الإحتيالية ضد جهاز

---

[1]_ أنظر : هشام محمد فريد رستم، **مرجـــع سابـــق**، من الصفحة 270 إلى271.

[2]_ أنظر : هشام محمد فريد رستم، **المرجـــع نفســـه**، صفحة 272.

[3]_ أنظر : هشام محمد فريد رستم، **المرجـــع نفســـه**، من الصفحة 274 إلى 275.

معلوماتي، إلا أنه يمكن تفادي هذا العارض بالنظر إلى دور الكمبيوتر في عملية الإحتيال بإعتباره مجرد وسيط شفاف ***"Intermédiaire transparent"*** و القول بناءا على ذلك بأن صاحب الكمبيوتر هو الذي تم خداعه و سلب أمواله، أي بمعنى آخر خادع النظام المعلوماتي للكمبيوتر يمكن تقبله على أساس أنه أصبح يحل محل المجني عليه[1].

كملخص لهذا التحليل : إذا تمت جريمة النصب بواسطة جهاز المعلوماتية كوسيلة مناورات إحتيالية ضد مال شخص آخر فهنا تقوم الجريمة طبقا للتشريعات العقابية الخاصة بجريمة النصب، أما إذا تمت جريمة النصب بواسطة جهاز المعلوماتية كوسيلة مناورات إحتيالية ضد الجهاز المعلوماتي ذاته، فهنا هنالك من يرى عدم قابلية تطبيق قانون العقوبات على أساس أن المستهدف بجريمة النصب هو الآلة و ليس الإنسان، و هناك من يرى إمكانية تطبيق قانون العقوبات على أساس أن مالك و مستعمل الجهاز المعلوماتي هو الذي كان في الأصل مستهدف بالجريمة، و نحن من جهتنا يمكن أن نظيف بأن المال المستولى عليه مملوك حتما لشخص آخر غير الآلة و بالتالي جريمة النصب تقوم في كل الأحوال.

من جهة أخرى يمكن أن تحقق جريمة النصب في محيط المعلوماتية بإتخاذ الجاني إسم أو صفة كاذبة بواسطة المعلوماتية و مثال ذلك : الدخول غير المشروع إلى نظام معلوماتي بإستعمال إسم المستعمل***"Nom d'utilisateur"*** و كلمة السر ***"Mot de passe"*** الخاصة في الأصل بمستخدمه الشرعي بقصد الإستيلاء على ماله أو مال الغير، أو حالة إستخدام الجاني بطاقة إلكترونية بنكية سرقها أو عثر عليها، بإدخالها في الموزع الآلي للنقود و إستعمال الأرقام السرية بعد أن تعرف عليها بطريقة الغش لسحب أموال من رصيد المجني عليه، و بالتالي كل هذه الحالات تعتبر جرائم نصب معلوماتية بإستعمال إسم أو صفة كاذبة ***"Nom ou qualité fausse"*** [2].

المطلب الثالث : المال محل جريمة النصب المعلوماتي

في الأصل النشاط الإجرامي المرتبط بجريمة النصب ليس بسيط بل مركب فهو يتكون من فعلين أساسيين هما : الكذب مصحوب بالمناورات الإحتيالية و الإستيلاء على مال المجني عليه، و أول الفعلين يسبق الثاني في الزمن، و بالتالي الفعل الأول يمثل الوسيلة و الفعل الثاني النتيجة المرجوة، إذا تحققت النتيجة بناءا على المناورات الإحتيالية هنا تقوم جريمة النصب من الناحية المادية، وبالتالي الركن المادي للجريمة حسب رأينا يعد محقق إذ أن المناورات الإحتيالية التي ستتم في محيط المعلوماتية ستكون غلبا بواسطة جهاز الكمبيوتر، و

---

[1] _ أنظر : هشام محمد فريد رستم، **المرجـــع نفســـه**، من الصفحة 276 إلى 277.

[2] _ أنظر : هشام محمد فريد رستم، **المرجـــع نفســـه**، من الصفحة 278 إلى 279.

يشترط في الأصل حتى تقوم الجريمة أن يكون المال الذي تم الإستيلاء عليه مال مادي (مثلا : منقولات، سندات، أوراق مالية)[1].

إذا لا يثير الإستيلاء بواسطة المعلوماتية إشكالا إذا كان المال المستولى عليه مال مادي ملموس كأن يتوصل الجاني إلى معرفة الرقم السري لصاحب البطاقة الإلكترونية البنكية المسروقة أو التي عثر عليها و يستخدمها لسحب من الموزع الآلي للنقود رصيد المجني عليه و مثل هذه الحالة المال الذي إستولى عليه الجاني مال مادي في شكل نقود[2] .

الإشكال على عكس الحالة السابقة يتمثل في حالة ما إذا كان محل الجريمة مال في شكل نقود كتابية ***"Monnaie scripturale"*** أو ما يسمى أيضا بالنقود الإلكترونية أو الخيالية ***"Monnaie électronique ou virtuelle"***، و بالتالي إذا تم الإستيلاء على المال عن طريق القيد الإلكتروني أو المعلوماتي، كما لو تلاعب الجاني في المعطيات المخزنة في الكمبيوتر أو في برامجه كي يحول كل أو بعض أرصدة الغير أو فوائدها إلى حسابه الخاص، فإن التساؤل الذي يطرح في هذه الحالة هو هل هنالك إستيلاء مادي حقيقي على مال الغير بإعتباره مبدئيا في شكل مال معنوي غير ملموس ؟

موقف محكمة النقض الفرنسية، و الفقه في هذه المسألة هو أن التسليم في جريمة النصب محقق ما دام الشيء وضع تحت تصرف الجاني بحيث يتمكن من حيازته بغير عائق و لو لم يستول عليه إستيلاء ماديا[3].

أيضا أكد القضاء الفرنسي موقفه في هذه المسألة بناء على نظرية التسليم المعادل ***"la Théorie de la remise par équivalent"*** التي أشارت إليها بمناسبة جرائم النصب على الضريبة على القيمة المضافة ***"T.V.A (taxe sur la valeur ajoutée)"***، و على عداد موقف السيارات أمام الأرصفة ***"Le Parcmètre"***، و الهاتف و الهدف من هذه النظرية التي وضعها فقهاء القانون هي ملاحقة كافة أشكال النصب و بالإضافة إلى التي تتم بإستخدام الحاسب الآلي[4].

في ما يخص هذه النظرية، أقرت محكمة النقض الفرنسية بأن مجرد القيد الكتابي و الذي لا يشترط فيه تسليم مادي مهما كان نوعه يعد بمثابة التسليم المعادل، و هكذا عدلت محكمة النقض الفرنسية المفهوم التقليدي لفكرة

---

(1)_ أنظر : هشام محمد فريد رستم، **المرجـــع نفســـه**، من الصفحة 279 إلى 280.

(2)_ أنظر : هشام محمد فريد رستم، **المرجـــع نفســـه**، صفحة 281.

(3)_ أنظر : هشام محمد فريد رستم، **المرجـــع نفســـه**، من الصفحة 282 إلى 284.

(4)_ أنظر : محمد سامي الشوا، **مرجـــع سابـــق**، صفحة 133.

التسليم حيث رأت بأن الوقت قد حان لتعديل هذا المفهوم، بما لا يتعارض و مبدأ التفسير الضيق للنصوص الجنائية[1].

من بين الأمثلة العملية لجريمة النصب في محيط المعلوماتية و عبر شبكة الأنترنت، جريمة النصب المعلوماتية بواسطة تقنية الفيشيرڤ ***"The phishing"*** :

حيث أنه حسب تقرير مكتب ***"(HSC)"*** (شركة مختصة في الإستشارات و الخبرة في مجال الحماية المعلوماتية)، وقعت هنالك هجمات بواسطة تقنية الفيشين ڤ[2] ***"The Phishing"*** سنة 2005، و تمثلت هذه التقنية في قيام المحتالين بإرسال رسائل إلكترونية ***"e-Mail"*** إلى عملاء أو مشتركين في 4 بنوك فرنسية ***"(Société Générale, BNP Paribas, CIC Banque et CCF)"***.

في نظر توماس سايرات ***"Thomas Sayrat"*** مستشار في مكتب ***"(HSC)"***، يتعلق الأمر بمراسلة الغير بواسطة بريد إلكتروني غير مرغوب فيه ***"SPAM - e-Mail non sollicités"*** إلى عملاء هذه البنوك و بهدف توجيههم إلى صفحات أنترنت خاطئة و مزيفة غير مواقع الأنترنت البنكية الرسمية التابعة للبنوك الأربعة، و هذه الصفحات المزيفة تحتوي على إستمارة إلكترونية مزيفة التي يطلب فيها من العملاء كتابة أسمائهم للإستعمال***"Leurs noms d'utilisateurs"*** و أرقامهم السرية للإتصال بحساباتهم الخاصة***"Leurs identifiants de connexion à leurs comptes"***.

هذه المناورة الإحتيالية المستحدثة سمحت للمحتالين في ميدان المعلوماتية إستعمال أسماء إستعمال و الأرقام السرية لعملاء البنوك الأربعة السالفة الذكر للتسلل إلى حساباتهم في هذه البنوك و إختلاس كل رصيدهم المالي الموجود فيها.

---

(1)_ أنظر : محمد سامي الشوا، **المرجـــع نفســـه**، صفحة 133.

(2)_ و هي إحدى أنواع جرائم المعلوماتية عبر شبكة الأنترنت المنصوص عليها في تقرير الصحافي لنتائج المؤتمر الحادي عشر للأمم المتحدة حول "الوقاية من الجريمة و العدالة الجنائية" أيام 18 إلى 25 أفريل 2005 ببنكوك (تايلاند) : **الملحق رقم 1**.

المبحث الخامس :
جريمة خيانة الأمانة المعلوماتية

في هذا المبحث سنتكلم عن العموميات التي تدور حول جريمة خيانة الأمانة كجريمة تقليدية في الأصل ؟ (المطلب الأول)، ثم سنحاول مطابقة هذه الجريمة على محيط المعلوماتية من خلال إشكاليتين أولها تحديد الطبيعة التعاقدية في محيط المعلوماتية ؟ (المطلب الثاني)، و ثانيها عملية أي هل فصل الإجتهاد القضائي في هذه المسألة بمعنى إمكانية وقوع جريمة خيانة الأمانة بواسطة المعلوماتية على مال معنوي ؟ (المطلب الثالث).

و بالتالي إذا حاولنا تطبيق جريمة خيانة الأمانة على المعاملات في محيط المعلوماتية فإننا سنجد بعض التصرفات التي تدخل فيها تقنية المعلوماتية كوسيلة و التي تشكل جريمة خيانة أمانة .

المطلب الأول : عموميات حول جريمة خيانة الأمانة كجريمة تقليدية في الأصل

جريمة خيانة الأمانة عبارة عن : "عملية إختلاس[1] ***"Détournement"*** أو تبديد ***"Dissipation"*** أو إستعمال مال الغير الذي سلم إلى الجاني بموجب عقد من عقود الأمانة إضرارا بمالكه أو حائزه الشرعي ***"Possesseur légale"*** أو واضع اليد عليه ***"Détenteur"*** مع توافر القصد الجنائي"[2].

نص على هذه الجريمة المشرع الجزائري في المادة 376 ق.ع و المصري في المادة 341 ق.ع و الفرنسي في المادة 314-1 ق.ع.

و تجدر الإشارة في هذا الصدد إلى أن المشرع الجزائري حدد على سبيل الحصر نوع المال محل الجريمة بقوله : "... أوراقا تجارية أو نقودا أو بضائع أو أوراقا مالية أو مخالصات أو أية محررات أخرى تتضمن أو تثبت إلتزاما أو إبراء ... "، كما حدد على سبيل الحصر أنواع عقود الإئتمان التي يمكن أن ترتكب بموجبها الجريمة بقوله : "... على سبيل الإجازة أو الوديعة أو الوكالة أو الرهن أو عارية الإستعمال أو لأداء عمل بأجر أو بغير أجر ..."، و المشرع المصري بصفة عامة سلك نفس المنهج الذي سلكه المشرع الجزائري في ما يخص هذه الجريمة.

---

[1]_ المصطلح إختلاس في جريمة خيانة الأمانة يؤخذ معنى تحريف ***"Détournement"***، بينما في جريمة السرقة يؤخذ معني إستيلاء ***"Soustraction ou usurpation"***.

[2]_ أنظر : محمد سامي الشوا، **مرجـــع سابـــق**، صفحة 135.

أما المشرع الفرنسي على عكس المشرع الجزائري و المصري فلقد سلك طريقا مخالفا و ذلك بإعطائها تعريف عام أوسع، إذ لم يحدد في نص المادة 314-1 ق.ع أنواع عقود الإئتمان و بالتالي كل العقود الخاصة صالحة لأن تكون وسيلة لإرتكاب الجريمة، و من جهة أخرى المشرع الفرنسي أعطى تعريف عام غير دقيق في ما يخص المال محل الجريمة، مما يحيل الفهم إلى أنه مدد تعريف المال إلى ما يسمى بالمال المعنوي و هذا يعد سبيل و مجال متاح للقاضي الجزائي في تجريم إختلاس الأموال المعنوية في أنواعها المختلفة كالنقود إلكترونية أو البرامج معلوماتية، حيث إكتفى المشرع بتعريف المال كما يلي :

"... أموال، قيم، أو أي ملك ... "[1]، و بالتالي يستنتج من عمومية المشرع الفرنسي في ما يخص المال محل الجريمة إعطاء سلطة تقديرية أكبر للقاضي الجزائي في هذه النقطة، مع العلم بأن المعاملات بين الأشخاص تطورت مع ظهور المعلوماتية و شبكات الإتصال المعلوماتية (كالتجارة الإلكترونية، التحويل الإلكتروني أو المعلوماتي للأموال بشتى أنواعها مادية أو معنوية، و كذا حلول بطاقات الإئتمان البنكية محل النقود التقليدية) كل هذه العوامل دفعت المشرع الفرنسي إلى تعديل نصوصه أي المادة 408 ق.ع.قديم التي كانت محررة بنفس أسلوب المواد 376 ق.ع.جزائري و 341 ق.ع.مصري بموجب الأمر رقم 2000-916 المؤرخ في 19 سبتمبر 2000، المادة 3 من الجريدة الرسمية لـــ 22 سبتمبر 2000 دخل حيز النفاذ في 1 جانفي 2002.

المطلب الثاني : طبيعة العلاقة التعاقدية في مجال المعلوماتية

أي هل هذه العلاقات بين الخواص موجودة فعلا ؟ و هل هي من نوع آخر جديد أم أنها نفس العلاقات التقليدية المتعارف عليها ؟

لقد تم الإجماع في الفقه و الممارسة القضائية على أنه يشترط في التسليم المال الذي تتوافر به جريمة خيانة الأمانة أن يكون بموجب عقد، و أن يكون هذا العقد من قبيل العقود التي وردت في القانون على سبيل الحصر فإذا لم يكن العقد الذي تم التسليم بمقتضاه من هذه العقود أو كان التسليم يتم بناءا على عقد آخر فإن إختلاس المال أو تبديده لا يعد منشأ لجريمة خيانة الأمانة (هذا بالنسبة للتشريع الجزائري و المصري) [2]، أما بالنسبة للتشريع العقابي الفرنسي بموجب المادة 314-1 ق.ع فلم يشترط نوع معين من عقود الإئتمان على سبيل الحصر حتى تقوم الجريمة.

من جهة أخرى تجدر الإشارة إلى أن عقود الأمانة تفترض بالضرورة قيام علاقة تعاقدية خاصة بين أشخاص القانون الخاص، و بالتالي فلا تطبق الجريمة على العقود التي يحكمها القانون العام، فالموظف في علاقته

---

[1] _ أنظر نص المادة 314-1 ق.ع.فرنسي باللغة الفرنسية :

Art 314-1 du code pénal français : « ... des fonds, des valeurs ou un bien quelconque ... »

[2] _ أنظر : محمد سامي الشوا، **المرجـــع نفســـه**، صفحة 136.

بالإدارة لا يعد طرفا في علاقة تعاقدية أيا كان نوعها بل يشغل وظيفة تنظيمية إزاء الإدارة تنظمها أحكام القانون الإداري بما في ذلك قانون الوظيف العمومي[1].

إذا العلاقة التعاقدية في جريمة خيانة الأمانة يجب أن تكون من قبيل العقود الخاصة و بين أفراد القانون الخاص، و هذه القاعدة تمتد أيضا إلى محيط المعلوماتية الذي في حقيقة الأمر لا يعد إستثناء على القاعدة العامة، و بالتالي فأن تقنية المعلوماتية ليست إلا وسيلة في الجريمة و بالتالي ليس لها تأثير على العلاقة التعاقدية بمعناها التقليدي، إلا أن الصعوبة الوحيدة في هذا المجال هو حالة إبرام عقد الأمانة مباشرة عبر الشبكة المعلوماتية مما يستدعي في بعض الأحيان أن يكون هنالك إمضاء إلكتروني على عقد معلوماتي و هذه الحالة تستضم بمشكلة الإعتراف بهذا العقد من الناحية القانونية كوسيلة إثبات بالإضافة إلى مشكلة الإعتراف القانوني بالمال المعنوي إذا كان هذا الأخير محل الجريمة، و ما عدى هذه الحالة فإن محيط المعلوماتية لا يطرح إشكالا كبيرا في ما يخص تطبيق قانون العقوبات بخصوص جريمة خيانة الأمانة و لكي نثبت ذلك سنعرض بعض القضايا التي طرحت في هذا المجال أمام القضاء الجزائي الفرنسي (و إن كانت نادرة إلى حد الآن)، حيث أن موقف القضاء الفرنسي في ما يخص تطبيق جريمة خيانة الأمانة على المحيط المعلوماتي كان إيجابيا.

المطلب الثالث : الإجتهادات القضائية في مجال جريمة خيانة الأمانة المعلوماتية

و الجديد في هذه الجريمة أن القضاء الفرنسي هو الذي سيصنع الحدث و ذلك بإعترافه صراحة على إمكانية إرتكاب جريمة خيانة الأمانة في محيط المعلوماتية و سنستدل في ذلك بثلاثة قضايا.

أولا و قبل كل شيء تجدر الإشارة إلى أن قانون العقوبات الفرنسي لسنة 1994 أعطى تعريف جديد أوسع لجريمة خيانة الأمانة و ذلك بقطع الرابطة التي كانت موجودة بين تطبيق الجريمة و إجبارية وجود عقد إئتمان محدد و بالتالي و ما دام التعريف الجديد لم يحدد على سبيل الحصر العقود التي بموجبها تتم جريمة خيانة الأمانة فإنه يكفي توافر أي عقد حتى تقوم الجريمة[2].

من جهة أخرى في ما يخص المال محل جريمة خيانة الأمانة فإنه من المنطقي أن القاضي الجزائي كان سيرفض تطبيق النصوص العقابية إذا وقعت الجريمة على مال معنوي، و أساس هذا الرفض هو عدم دخول الأموال المعنوية في حيز نفاذ المادة 314-1 ق.ع.فرنسي و رغم ذلك فإنه عمليا يمكن تجريم إختلاس أو تبديد المال المعنوي نظرا لعدم وجود مصطلح " شيء " و إنما جاءت الصياغة كالتالي " ... أي ملك ... "، و

---

[1] _ أنظر : محمد سامي الشوا، **المرجـــع نفســـه**، صفحة 137.

[2] _ أنظر : Laureen KRAFTCHIK, ***Op.cit***, Page 49.

بالتالي هذه الصياغة كان من الممكن أن تحيل فهم للقاضي الجزائي على أن الأموال المعنوية تدخل أيضا في تعريف الجريمة، و هو ما قررته فيما بعد محكمة النقض الفرنسية[1].

و من هذا المنطلق تم الإعتراف بأن جريمة خيانة الأمانة يمكن أن تتم على مال معنوي و كان ذلك لأول مرة بموجب قرار محكمة النقض الفرنسية، الغرفة الجزائية المؤرخة في 14 نوفمبر 2000 (الفرع الأول)، بعد صدور هذا القرار التجريم بخصوص خيانة الأمانة الواردة على مال معنوي تم تمديدها و توسيع نطاقها، و من بين قرارات محكمة النقض الفرنسية المستحدثة في هذا المجال أيضا، ذلك المؤرخ في 22 سبتمبر 2004 (الفرع الثاني)، و كذا القضية التي طرحت في فرنسا بخصوص جريمة خيانة الأمانة المرتكبة عبر شبكة الأنترنت سنة 2005 (الفرع الثالث).

الفرع الأول : قرار محكمة النقض الفرنسية لـــ 14 نوفمبر 2000

تجدر الإشارة إلى أنه منذ إعتراف محكمة النقض الفرنسية بإمكانية إختلاس ***"Détournement"*** أرقام بطاقات الإئتمان البنكية ***"Les numéros des cartes bancaires"***، ظهرت قرارات أخرى في فرنسا و التي إعترفت بدورها بأن المال المعنوي يعد هو الآخر محل لجريمة خيانة الأمانة[2].

في ما يخص قرار محكمة النقض[3]، فالقضية تمثلت في أن مؤسسة تجارية عن بعد إستعملت رقم بطاقة بنكية مملوكة لزابونة قديمة لقيامها بسحب نقدي جديد على حساب هذه الزابونة تسديدا لقيمة بضاعة أرسلتها المؤسسة التجارية فيما بعد لهذه الزابونة دون رضاها و التي رفضتها فيما بعد[4].

تبعا لذلك الشخص الذي قام بهذا السحب الغير مشروع تم إدانته على أساس جريمة خيانة الأمانة من طرف قاضي الغرفة الجزائية بالمجلس القضائي.

بعد ذلك قام المتهم بتسجيل طعن بالنقض في القرار على أساس أن الإختلاس لم يكن على مال مادي بل تم على مال معنوي و بالتالي لا يمكن تطبيق نص المادة 314-1 ق.ع.فرنسي.

غير أن محكمة النقض رفضت الأساس القانوني الذي جاء به محامي المتهم معتبرة بأن المادة 314-1 ق.ع تطبق على أي ملك أو مال كما هو وارد في النص و ليس فقط على المال المادي[5].

---

(1)_ أنظر : Laureen KRAFTCHIK, ***Op.cit***, de la Page 49 à 50.

(2)_ أنظر : Laureen KRAFTCHIK, ***Ibid***, Page 50.

(3)_ ***Arrêt de cour suprême Française chambre pénale du 14 novembre 2000***

(4)_ أنظر : Laureen KRAFTCHIK, ***Op.cit***, page 50.

(5)_ أنظر : Laureen KRAFTCHIK, ***Idem***.

و بالتالي يمكن أن نستنتج بأن قرار محكمة النقض كان مؤسسا على ما نصت عليه المادة 314-1 ق.ع : "... أي ملك ...".

الفرع الثاني : قرار محكمة النقض الفرنسية لـــ 22 سبتمبر 2004

حيث تجدر الإشارة إلى أن قرار محكمة النقض الفرنسية بدوره أخذ بنفس الحل القانوني الذي جاء به القرار الصادر في 14 نوفمبر 2000 [1] حيث إعتبرت محكمة النقض بأن إختلاس مشروع غير متصل بأي دعامة مادية ***"Projet sans aucun support matériel"*** يشكل جريمة خيانة أمانة[2].

في هذه القضية الغرفة الجزائية إعتبرت بأن العامل إختلاس مشروع غير متصل بأي دعامة مادية، نظرا لكون أنه لم تكن له إلا مجرد حيازة عارضة مؤقتة لهذا المشروع، فإنه منذ اللحظة التي تصرف فيها في هذا المشروع كأنه مالك لها و لحساب الغير، فإنه يعد مرتكب جريمة خيانة الأمانة[3].

في هذه القضية المشروع محل الجريمة لم يكن في البداية موجود في إيطار مادي ***"Matérialisé"***، و لكن فيما بعد تم تحميله على وثيقتين إحداهما تحت تسمية الشركة الموظفة لهذا العامل و الأخرى تحت تسمية الشركة التي كان العامل سيلتحق بها، إذا الأساس القانوني للجريمة هو الإختلاس أو التحريف ***"Détournement"*** الذي قام به العامل للمشروع من خلال نسخ المشروع من جديد في وثيقة ثانية تحت تسمية الشركة التي كان سيلتحق بها، و تجدر الإشارة إلى أن محكمة النقض في قرارها لم توضح بأنه تم إختلاس أو تحريف الوثيقة التي تحمل على متنها المشروع و إنما إكتفت بالإشارة إلى أن الإختلاس تم على مشروع و هذا ما يعطي قرارها كل الأهمية و الإنتباه[4].

و تجدر الإشارة إلى أن الطعن بالنقض الذي سجله العامل في قرار المجلس أسس على أن الوثيقة الثانية و في نظر المادة 314-1 ق.ع لا تعتبر مال بمفهومه المادي و بالتالي جريمة خيانة الأمانة غير مؤسسة[5].

---

(1) _ ***Arrêt de cour suprême Française chambre pénale du 22 septembre 2004***

(2) _ أنظر : Laureen KRAFTCHIK, ***Op.cit***, Page 54.

(3) _ أنظر : Laureen KRAFTCHIK, ***Idem***.

(4) _ أنظر : Laureen KRAFTCHIK, ***Ibid***, Page 55.

(5) _ أنظر : Laureen KRAFTCHIK, ***Idem***.

إلا أن محكمة النقض إستبعدت هذا التأسيس و إعتبرت بأن المشروع في حد ذاته يعد مال على نفس مستوى المال المادي الذي أصبح ملك للشركة المستخدمة لهذا العامل منذ لحظة إنتهائه من إنجاز هذا المشروع و بالتالي فإنه لم يعد إلا مجرد حائز لها حيازة عارضة أي مؤقتة[1].

الفرع الثالث : جريمة خيانة الأمانة عبر شبكة الأنترنت

القضية التي سنتكلم عنها الآن تتعلق بجريمة خيانة الأمانة مرتكبة عبر شبكة الأنترنت ضد 700 مستعمل لها، تتمثل وقائع القضية في أن شخصين محتالين يستعملان شبكة الأنترنت للإستيلاء على أموال العملاء المتعاقدين معهم، ألقي القبض عليهم في 13 سبتمبر 2005 في أوريول ***"Auriol (Bouches-du-Rhône)"*** حيث أن الإبن البالغ من العمر 23 سنة وضع في الحبس المؤقت و أمه البالغة من العمر 40 سنة وضعت تحت الرقابة القضائية، و المتهمين تم إحالتهم من طرف قاضي تحقيق باستيا ***"Bastia"*** على قسم الجنح على أساس جريمة خيانة الأمانة، و تجدر الإشارة إلى أنه في هذه القضية الإبن هو الفاعل الأصلي للأعمال الإحتيالية، حيث أنه أنشأ شركة تحت تسمية ***"New Import Club"*** هذه الشركة تقترح بفضل موقعي الأنترنت التابعين لها و الموجودتين في الولايات المتحدة الأمريكية ***" librshop.com et libertoi.com"*** خدمات في ما يخص توظيف أموال المتعاملين مع الشركة في سوق المالية و بنسبة فوائد يمكن أن تصل إلى 28 %، و بالمقابل العملاء يلتزمون بدفع قيمة 580 € للمشاركة و فتح حساب في الشركة، المجرم في هذه الحالة بعد إبرام العقد مع العملاء كان يمنح لهم مبالغ مالية صغيرة في كل عملية توظيف لأموال العملاء بواسطة هذه الشركة و التي إتضحت فيما بعد بأنها مناورة كان يستعملها المجرم لوضع الثقة عند العملاء و دفعهم إلى توظيف نسبة أكبر من الأموال، حسب تصريح وكيل جمهورية باستيا ***"Jean-Jaques Fagni"*** [2].

حيث أنه خلال أفريل 2005 قدم أحد العملاء شكوى ضد شركة ***"New Import Club"*** التي لم تعد في الخدمة، و أن هذا الأخير قلق على أساس أنه لم يتلقى الفوائد من الأموال التي قدمها للشركة و على هذا الأساس إنطلقت مرحلة التحقيق في القضية[3].

و تجدر الإشارة إلى أن الجمارك المتخصصين في الجرائم الإقتصادية و المالية لمدينة أجاكسيو ***"Ajaccio"*** عثروا بعد 5 أشهر من التحقيق التقني على المتهم الذي بعد أن سلب أموال العملاء قام بغلق مواقع الأنترنت الموجودة في الولايات المتحدة الأمريكية تاركا حوالي 700 ضحية في العالم بدون أي إجابة ***"(France,***

---

(1)_ أنظر : Laureen KRAFTCHIK, ***Op.cit***, page 55.

(2)_ أنظر صفحة الأنترنت التالية (مقال تحت عنوان : ***700 internautes victimes d'abus de confiance : 2 français interpellés***، من ***Michel robert***، ***http://www.njuris.com/***، 07 / 10 / 2005) : **http://www.njuris.com/ShowBreve.aspx?IDBreve=704**

(3)_ أنظر نفس صفحة الأنترنت السابقة : ***Idem* : http://www.njuris.com/ShowBreve.aspx?IDBreve=704**

"Allemagne, Espagne, Belgique, Suisse, Etats-Unis, Canada)، و قدر الضرر الإجمالي بحوالي أكثر من 1,2 مليون أوروا €، و إتضح كذلك بأن أم المتهم كانت تدير شركة تلعب نفس دور شركة الإبن و هذه الشركة كانت موجودة في فرنسا تحت تسمية ***"Whale Trade France"*** ، و إلى حد الآن عدد كبير من الضحايا لم يتم العثور عليهم، و تجدر الإشارة إلى أن هذا النظام الذي وضع من طرف المتهمين الفرنسيين من أهم الأنظمة الإحتيالية لمال الغير عبر شبكة الأنترنت لهذه السنوات الأخيرة في فرنسا، و بالتالي المتهمين تبعوا على أساس تهمة جنحة خيانة الأمانة و ذلك بمناداتهم إلى الجمهور أي ظرف مشدد للجريمة معاقب عليه بسبعة سنوات حبس و غرامة تقدر بـــ 750 ألف €، و تهمة الممارسة الغير مشروعة لوظيفة البنكيين و كذا تهمة الغش إزاء الضريبة على القيمة المضافة [1].

---

(1)_ أنظر نفس صفحة الأنترنت السابقة : ***Op.cit*: http://www.njuris.com/ShowBreve.aspx?IDBreve=704**

الفصل الثاني :
جرائم المعلوماتية الماسة بالأشخاص و الحريات

- المبحث الأول : حرية التعبير في محيط المعلوماتية و الأنترنت
- المبحث الثاني : جرائم المعلوماتية المتعلقة بالمعطيات المعلوماتية الشخصية
- المبحث الثالث : جرائم المعلوماتية الماسة بالحريات الفردية عبر شبكة الأنترنت
- المبحث الرابع : جرائم المعلوماتية الماسة بالقاصر عبر شبكة الأنترنت
- المبحث الخامس : جريمة الإرهاب المعلوماتي عبر شبكة الأنترنت

الـــفـــصـــل الـــثـــانـــي :
جرائم المعلوماتية الماسة بالأشخاص و الحريات

في هذا الفصل سنتطرق إلى أهم الجرائم المرتكبة ضد الأشخاص و الحريات الفردية في محيط المعلوماتية و بالأخص عبر الشبكة المفتوحة "أنترنت"، إذ أنه حتى و إن كانت جل الجرائم المرتكبة ضد هذه الفئات هي في الأصل جرائم تقليدية، إلا أنه بظهور وسائل الإتصال و الإعلام مستحدثة (الكمبيوتر ***"Ordinateur"***، الشبكات المعلوماتية و بما فيها شبكة الأنترنت ***"Réseau « Internet »"***، وسائل الإتصال عن بعد المستحدثة ***"Les moyens de télécommunications modernes"*** مثلا) أصبح بإمكان المجرم تحت تسمية مستحدثة (أي المجرم المعلوماتي ***"Le cyber-criminel ou le hacker"***) إرتكاب مثل هذه الجرائم التقليدية بموجب هذه الوسائل و في أغلب الأحيان عن بعد، مما يطرح إشكال كيفية إتيان دليل إرتكاب هذه الجرائم و كذا القيمة القانونية للدليل الإلكتروني كنوع جديد من الأدلة في المواد الجزائية و هو موضوع مستقل عن دراستنا يستدعي التمعن و البحث فيه لما له من أهمية تكميلية لموضوع البحث.

حرية التعبير تعد مبدأ أساسي كرسه القانون الدولي و كذا معظم التشريعات الوطنية (أي الدساتير) خاصة في الدول ذات نظام ديموقراطي، لذا كان من الضروري التطرق لهذه النقطة لتحديد حدود هذه الحرية في نظر مختلف التشريعات و في ما يخص شبكة الأنترنت، بالإضافة إلى الإجراءات القانونية و الإدارية التي إتخذتها الدول في هذا المجال (المبحث الأول)، ثم بعد ذلك سنتطرق إلى كلا من الجرائم ضد المعطيات المعلوماتية الشخصية (المبحث الثاني)، الجرائم ضد إعتبار الأشخاص و حرمة حياتهم الشخصية عبر شبكة الأنترنت (المبحث الثالث)، ثم سنتكلم عن الجرائم المعلوماتية المرتكبة ضد القصر و هذا بطبيعة الحال عبر شبكة الأنترنت (المبحث الرابع)، و أخيرا سندرس جريمة الإرهاب المعلوماتي بإستعمال تقنية المعلوماتية (المبحث الخامس).

المبحث الأول :
أبعاد حرية التعبير عبر شبكة الأنترنت

تعتبر حرية التعبير مبدأ أساسي في كل مجتمع ديموقراطي ، غير أنه يجب أن لا تمس هذه الحرية بالشخص في حرمة حياته الشخصية أو في شرفه كما وجب أن لا تمس هذه الحرية بالنظام العام، الآداب العامة و الأمن العام في الدولة[1].

لهذا السبب يمكن أن نطرح تساؤل ذات أهمية بالغة في هذا المجال هو، كيف يمكن التوفيق بين الشبكة المفتوحة[2] "أنترنت" و حرية التعبير و الحريات الفردية مع العلم بأن هذه المفاهيم تختلف من دولة إلى أخرى ؟

سندرس في هذا المبحث حرية التعبير بإعتبارها مبدأ أساسي دستوري في كل دولة ذات نظام ديموقراطي (المطلب الأول)، ثم سنرى حدود هذه الحرية في ميدان الأنترنت (المطلب الثاني)، و أخيرا سنرى الإجراءات القانونية و الإدارية التي إتخذت في هذا المجال من طرف الدول (المطلب الثالث).

المطلب الأول : حرية التعبير كمبدأ أساسي دستوري

من بين أهم النصوص التي نصت على مبدأ حرية التعبير قبل أن تصبح مبدأ دستوري هو الإعلان العالمي لحقوق الإنسان لـــ 10 ديسمبر 1948[3] :

المادة 19 : "كل شخص له الحق في حرية الرأي والتعبير، ويشمل هذا الحق حرية اعتناق الآراء دون أي تدخل، واستقاء الأنباء والأفكار وتلقيها وإذاعتها بأية وسيلة كانت دون تقيد بالحدود الجغرافية"[4].

حيث تم التأكيد على هذا النص من جديد بموجب الميثاق أو البروتوكول الدولي المتعلق بالحقوق المدنية و السياسية لسنة 1966.

---

(1) _ أنظر : Féral-schuhl Christiane, ***Cyber Droit (le droit à l'épreuve de l'Internet)***, édition Dalloz (2e édition), septembre 2000, page 86

(2) _ أي الشبكة المفتوحة لكافة الجمهور على عكس الشبكات الخاصة المغلقة ***"Réseaux privés fermés ou verrouillés"*** كشبكة الأنترانت ***"Intranet"*** المفتوحة لعدد محدود من الجمهور و التي تستدعي في أغلب الأحيان رقم سري أو شفرة سرية للدخول إليها.

(3) _ أنظر : **الملحق رقم 14**

(4) _ أنظر نص المادة باللغة الفرنسية :

Art 19 : « Tout individu a droit à la liberté d'opinion et d'expression, ce qui implique le droit de ne pas être inquiété pour ses opinions et celui de chercher, de recevoir et de répandre, sans considération de frontières, les information et les idées par quelque moyen d'expression que ce soit ».

بمعنى أنه "يدخل في صميم حرية التعبير حرية البحث، تلقي و نشر معلومات و أفكار مهما كان نوعها دون الأخذ بعين الإعتبار عنصر الحدود الجغرافية كعائق، في صورة صوتية، مكتوبة، مطبوعة أو فنية و بأي طريقة كانت مختارة من طرفه"[1].

و تجدر الإشارة إلى أن هذه النصوص الدولية لن يكون لها دورا فعال إذا لم تجسد على المستوى الوطني بعد المصادقة عليها، بإدخالها في الدستور و القوانين التي ستطبق على المستوى الداخلي، و لقد إستجاب لهذه النصوص الدولية معظم الدول ذات نظام ديموقراطي في العالم و بما فيها الجزائر (الفصل الرابع من دستور 1996 تحت عنوان : "الحقوق و الحريات" المواد من 29 إلى 51) التي جاءت بصفة عامة معبرة عن المبادئ و القيم التي جاء بها الإعلان العالمي لحقوق الإنسان.

من المعلوم أنه لا توجد طريقة واحدة للتعبير عن الآراء و الأفكار بل عدة أنواع من الطرق سواء من خلال الصحافة، الأنترنت، المؤلفات، الإذاعة، أو التلفزة منظمة قانونيا بطرق تختلف من دولة إلى أخرى، إذ أن الأعراف و العادات ليست نفسها في دول العالم، و الحريات ليست معالجة بنفس الطريقة، كما أن حرية التعبير في أغلب الأحيان تكون مقيدة قانونيا لأسباب مختلفة قد تكون عقائدية (دينية)، أو سياسية.

و تجدر الإشارة إلى أن إختلاف موقف الدول بشأن حرية التعبير جعلت من الصعب بل من المستحيل وضع معايير مشتركة بين الشبكات المعلوماتية و الدول نظرا للإختلاف الكبير بين التشريعات الوطنية.

أما في ما يخص النظرة الأوروبية في ميدان الحريات، فلقد عبرت عنها من خلال الإتفاقية الأوروبية للحفاظ على حقوق الإنسان و الحريات الأساسية لـــ 4 نوفمبر 1950 تماشيا مع الإعلان العالمي لحقوق الإنسان، و التي تنص بأن : "كل شخص له الحق في حرية التعبير "[2]، هذا الحق يضم حرية التفكير ***"La liberté de pensée"***، حرية الضمير ***"La liberté de Conscience"***، حرية العقيدة ***"La liberté du culte ou la religion"***، حرية تلقي أو تبليغ معلومات أو أفكار ***"La liberté de recevoir ou de communiquer des informations ou des idées"***، بالإضافة إلى الحق في إحترام حرمة الحياة الشخصية و العائلية ***"Le droit de respect de la vie privée et familiale"***، و كذا حرمة المسكن أو محل الإقامة ***"Le droit de respect du domicile"*** و الإتصال ***"Et de la***

---

(1)_ أنظر النص باللغة الفرنسية :

« (la liberté d'expression) comprend la liberté de recherche, de recevoir et de répandre des informations et des idées de toutes espèce, sans considération de frontière, sous une forme orale, écrite, imprimée ou artistique et par tout autre moyen de son choix ».

(2)_ أنظر النص باللغة الفرنسية :

« Toute personne a droit à la liberté d'expression ».

correspondance" "، و من المعلوم أن كل هذه الحالات تطبق في ما يخص محيط الأنترنت و كل أنواع الشبكات المعلوماتية بإعتبارها تلعب نفس الدور الذي تلعبه الصحافة، الإذاعة، أو التلفزة[1].

هذه النصوص الدولية غالبا ما تكون متبوعة بنصوص دستورية وطنية كما سبق و أن ذكرناه بالنسبة للمثال الجزائري، و يمكن أن نؤكد بأن أحسن مثال في مجال الحريات و بما فيها حرية التعبير هي الولايات المتحدة الأمريكية، و التي سميت أيضا بدولة الحريات، و أين يشكل هذا المبدأ إحدى الركائز الأساسية التي يقوم عليها دستورها، حيث تنص المادة الأولى منه ***"1er amendement"*** بأن : ، "الكونغرس لن يكون بإمكانه وضع أي قانون ... يحد من حرية الكلام و الصحافة"[2] [3].

يفهم من هذا النص أن كل شخص يجب أن يتمتع بالحق في التعبير عن آرائه دون أي قيد[4].

بناءا على هذا المبدأ و حفاظا عنه، في 26 جوان 1997 قررت محكمة النقض للولايات المتحدة الأمريكية بأنه تعتبر غير دستورية البعض من النصوص التي جاء بها القانون حول أخلاقية الإتصالات ***"Loi sur la décence de la communication (Communication Decency Act)"*** لـــ 1 فيفري 1996[5].

هذا النص القانوني كان يمنع نشر عبر الشبكات بما فيها المعلوماتية رسائل إلكترونية غير أخلاقية ***« Indécents »*** أو عنيفة ***« Offensants »*** من الممكن أن يتطلع عليها القصر[6].

حيث صرحت محكمة النقض ما يلي :

"نحن نعتقد بأن التقنين الحكومي يعد ذات طبيعة تهدف أكثر إلى التدخل في حرية تبادل الأفكار بذلا من أن تشجعها"[7].

---

(1)_ أنظر : Féral-schuhl Christiane, ***Op.cit***, page 87.

(2)_ أنظر نص المادة باللغة الفرنسية :

« Le congrès ne pourra faire aucune loi ... restreignant la liberté de la parole et de la presse ».

(3)_ أنظر : Féral-schuhl Christiane, ***Op.cit***, page 87.

(4)_ أنظر : Féral-schuhl Christiane, ***Idem.***

(5)_ أنظر : Féral-schuhl Christiane, ***Idem.***

(6)_ أنظر : Féral-schuhl Christiane, ***Idem.***

(7)_ أنظر : Féral-schuhl Christiane, ***Idem.***

"المصلحة في تدعيم حرية التعبير في دولة ديموقراطية تفوق عملية الرقابة و الحضر النظري أين الآثار لم تثبت بعد"[1] [2].

و بالتالي إعتبرت المحكمة بأن هذا التقنين يعد مساسا بمبدأ أساسي دستوري.

و من الملاحظ أنه توجد في الولايات المتحدة الأمريكية العديد من الجماعات الضاغطة على الحكومة و بما فيها الجمعيات التي تتمتع في أغلب الأحيان بإمكانيات سواء مالية أو سياسية معتبرة، كما أن هذه الجمعيات تناضل في أغلب الأحيان في سبيل الدفاع على حرية التعبير التامة عبر شبكة الأنترنت، و من بين أهم هذه الجمعيات، جمعية ***"Electronic Frontier Foundation"*** التي أنشأت من طرف ***"Mitch Kapor"*** و***"John Perry Barlow"*** (موقع الأنترنت : ***http://www.eff.org/***)[3].

كما قلنا سابقا، حرية التعبير تعد مبدأ أساسي في كل دولة أو مجتمع يصرح أو يدعي بأنه ديموقراطي، غير أنه ليس الأمر كذلك في كل الأوقات إذ هنالك دول تصرح بأنها ديموقراطية في الظاهر إلا أنها في حقيقة الأمر تخفي دكتاتورية و هيمنة على شعبها بطريقة منظمة، حيث أنها تصل إلى هذه النتيجة من خلال الحد و الرقابة على المعلومات التي تنتشر داخل ترابها من خلال شتى وسائل الإعلام بما فيها شبكة الأنترنت و هذا بهدف القضاء على كل أنواع المعارضة، هذه الهيمنة نجدها خاصة في الدول ذات نظام إشتراكي و إستثناءا في بعض الدول ذات نظام ديموقراطي.

المطلب الثاني : حدود حرية التعبير عبر شبكة الأنترنت

إذا كانت حرية التعبير مبدأ أساسي، فإنها يجب أن لا تمس بالأشخاص في شرفهم مثلا أو بالنظام العام، كما قلنا سابقا، و تجدر الإشارة إلى أن هذه الحدود تشمل بالإضافة إلى الوسائل التقليدية للتعبير عن الرأي، شبكة الأنترنت و هذا ما سنراه في هذا الفصل[4].

و لقد نص على هذه الحدود صراحة الإعلان العالمي لحقوق الإنسان :

---

(1)_ أنظر النص باللغة الفرنسية :

« Nous présumons que la réglementation du gouvernement est plus de nature à interférer sur le libre-échange des idées plutôt qu'à l'encourager. L'intérêt de soutenir la liberté d'expression dans un pays démocratique l'emporte sur une censure théorique dont les effets ne sont pas prouvés ».

(2)_ أنظر : Féral-schuhl Christiane, ***Op.cit***, page 87.

(3)_ أنظر : Féral-schuhl Christiane, ***Ibid***, page 88.

(4)_ أنظر : Féral-schuhl Christiane, ***Idem.***

المادة 4 : "الحرية تتمثل في القدرة على القيام بكل ما لا يضر بالغير ..."[1].

كما نصت على هذه الحدود الإتفاقية الأوروبية لحقوق الإنسان و المواطن ***"La convention européenne des droit de l'homme et du citoyen".***

المادة 10 فقرة 2 : "ممارسة هذه الحريات المتضمنة واجبات و مسؤوليات يمكن أن تكون محل بعض الشكليات، الشروط، أو عقوبات مقررة قانونا و التي تشكل إجراءات ملزمة في مجتمع ديموقراطي للأمن الوطني، إلى إستقرار التراب الوطني أو إلى الأمن العام، إلى حماية النظام و إلى التنبأ بالجريمة، إلى حماية الصحة و الأخلاق، إلى حماية السمعة أو حقوق الغير، لمنع الإباحة بمعلومات سرية أو لضمان سلطة و إستقلالية السلطة القضائية"[2].

و من المعلوم أن حرية التعبير تمارس بطريقة مختلفة من دولة إلى أخرى و يعود إلى كل حكومة مسؤولية ضمان هذه الحرية و لكن أيضا معاقبة كل التجاوزات التي تمارس في هذا المجال[3].

المطلب الثالث : الإجراءات المتخذة من طرف الدول

ظاهريا و واقعيا يعد من الصعب للمشرع عموما التوفيق بين حرية التعبير و الحفاظ على الآداب العامة، و في هذا المجال صرحت المحكمة الأوربية لحقوق الإنسان بأن[4] :

"التدخلات للسلطات العامة في ممارسة حرية التعبير كانت إلزامية في مجتمع ديموقراطي لحماية الآداب العامة"[5].

و تجدر الإشارة إلى أنه إذا طرحت قضية من نفس النوع على محكمة النقض للولايات المتحدة الأمريكية فإنها لن تسير على نفس الرأي الذي أخذت به المحكمة الأوربية لحقوق الإنسان، بناءا على ما سلف ذكره بخصوص المثال الأمريكي.

---

(1)_ أنظر نص المادة باللغة الفرنسية :

Art. 4 : « La liberté consiste à pouvoir faire tout ce qui ne nuit pas à autrui … ».

(2)_ أنظر نص المادة باللغة الفرنسية :

Art. 10 alinéa 2 : « L'exercice de ces libertés comportant des devoirs et des responsabilités peut être soumis à certaines formalités, conditions, restrictions ou sanctions prévues par la loi, qui constituent des mesures nécessaires dans une société démocratique à la sécurité nationale, à l'intégrité territoriale ou à la sûreté publique, à la défense de l'ordre et à la prévention du crime, à la protection de la santé ou de la morale, à la protection de la réputation ou des droits d'autrui, pour empêcher la divulgation d'informations confidentielles ou pour garantir l'autorité et l'impartialité du pouvoir judiciaire ».

(3)_ أنظر : Féral-schuhl Christiane, ***Op.cit***, page 89.

(4)_ أنظر : Féral-schuhl Christiane, ***Idem.***

(5)_ أنظر النص باللغة الفرنسية :

« Les ingérences d'autorités publiques dans l'exercice de la liberté d'expression étaient nécessaires dans une société démocratique à la protection de la morale ».

و بالتالي يمكن أن نلاحظ من خلال المثال السالف الذكر بصفة خاصة الإختلافات بين الإتحاد الأوروبي و الولايات المتحدة الأمريكية في هذا الموضوع و عموما بين دول العالم، و التي ستجعل من الصعب وضع نصوص قانونية دولية مشتركة في مجال حرية التعبير و الآداب العامة[1].

من جهة أخرى يمكن أن نلاحظ و نؤكد بأن القانون سواء الفرنسي أو الجزائري يطبق على كافة النشاطات المرتبطة بشبكة الأنترنت في موضوع الحريات، فإذا كانت الدعامة المعلوماتية تعد وسيلة جديدة للتعبير عن الرأي و في تطور مستمر، إلا أن النصوص التشريعية و التنظيمية حتى و إن كانت في أغلب الأحيان تقليدية، إلا أنها تغطي تقريبا كل وسائل الإتصال عن بعد ***"Les moyens de télécommunication"***، و بالتالي لا مجال للقول بأن هنالك فراغ قانوني في هذا المجال، و ما دام هنالك نصوص قانونية قمعية بإمكانها تغطية موضوع الساعة و إذا كان بإمكان المحاكم المعاقبة على الجرائم المرتكبة في فضاء الأنترنت، إلا أنه يمكن طرح جملة من الإشكاليات ذات أهمية بالغة في هذا الموضوع، أي كيف يمكن إتيان دليل الجريمة المعلوماتية (أي الدليل الإلكتروني) ؟ و ما القيمة القانونية لهذا النوع الجديد من أدلة الإثبات ؟ و هل للحكومات الإمكانيات التقنية الكافية لإتيان أدلة الإثبات لقيام الجريمة ؟، أيضا ما العمل إذا كان المتهم قد إرتكب الجريمة عبر شبكة الأنترنت تستهدف أو تمتد أثارها إلى دولة (ب) و إنطلاقا من دولة (أ) مثلا ؟، وتجدر الإشارة إلى أن نفس هذه الإشكاليتين قد سبقنا و أن طرحناهما في الفصل الأول من المذكرة بخصوص جرائم المعلوماتية ضد الأموال، في هذه الحالة العديد من المحاكم طبقت العقوبة على الوسائط ***"Les intermédiaires"***، تحت تسمية : موزعي حق الدخول في شبكة الأنترنت و المثبتين لمواقع الأنترنت ***"Les fournisseurs d'accès à Internet et d'hébergement de sites Web"*** و الذين في هذه الحالة قد يجدون أنفسهم متهمين بالمشاركة في الجريمة المعلوماتية، و هذا عندما لا يقومون بالتصفية التقنية للمعلومات المعلوماتية و التي تشكل جريمة في نظر القوانين أو مخالفة للنظام العام في الدولة التي يمارسون فيها مهنتهم[2].

---

(1) _ أنظر : Féral-schuhl Christiane, ***Op.cit***, page 89.

(2) _ أنظر : Féral-schuhl Christiane, ***Ibid***, de la page 89 à 90.

المبحث الثاني :
الجرائم ذات صلة بالمعطيات المعلوماتية الشخصية

القانون الفرنسي لسنة 1978 المتعلق بالمعلوماتية، المعطيات و الحريات، يعد فريد من نوعه خاصة و أن الحكومة الفرنسية أنشأت في هذا الصدد ما يسمى باللجنة الوطنية للمعلوماتية و الحريات ***"(C.N.I.L) Commission Nationale de l'Informatique et des Libertés"*** في إطار هذا القانون و هي سلطة إدارية مستقلة [1] و ذات صلاحيات واسعة و هي مكلفة أساسا بالرقابة على التطبيق السليم لهذا القانون و كذا الرقابة على الإستعمال القانوني للمعطيات المعلوماتية ذات طابع شخصي و تنظيم كيفية إستعمالها و بطريقة قانونية على المستوى الوطني، و الغريب في الأمر هو أن المشرع الفرنسي على خلاف الدول الأخرى تنبأ بأهمية موضوع المعطيات المعلوماتية ذات الطابع الشخصي مبكرا أي في سنة 1978 أي في الوقت الذي كانت فيه المعلوماتية ليس لها دور مهم و فعال في المجتمع الفرنسي و في مختلف القطاعات، إذا المشرع الفرنسي من خلال هذا النص القانوني المستحدث وضع الأسس القانونية الكبرى التي ستنظم ميدان المعلوماتية و بالأدق المعطيات المعلوماتية ذات طابع شخصي مع علمه المسبق بأن مجال المعلوماتية سوف يتطور بسرعة كبيرة إلى درجة أنه سيحتل مكانة أساسية في مختلف القطاعات و على كل المستويات في فرنسا.

و بالتالي الأسئلة التي يمكن طرحها في هذا المبحث هي، ما هي أنواع المعطيات المعلوماتية التي تدخل في إطار المعالجة الآلية ؟ و إلى أي صنف تنتمي المعطيات المستهدفة من طرف هذا القانون ؟ (المطلب الأول)، و ما هي الجرائم المتعلقة بالشكلية الواجب إتباعها في معالجة هذا الصنف من المعطيات بحكم هذا القانون ؟ (المطلب الثاني)، أيضا ما هي الجرائم التي تدخل في إطار إستعمال هذه المعطيات وفقا للقانون ؟ (المطلب الثالث)، و أخيرا سنتكلم عن العقوبات المقررة في إطار هذا القانون في حالة الإعتراض لوظيفة اللجنة الوطنية للمعلوماتية و الحريات (المطلب الرابع).

المطلب الأول : أنواع المعلومات المعلوماتية

يعرف محيط المعلوماتية فئات مختلفة من المعطيات المنطقية، و في هذا الصدد قسم الأستاذ كتلا ***"Catala"*** المعلومات المعلوماتية إلى ثلاث أنواع[2] :

---

[1] _ أنظر صفحة الأنترنت التالية (مقال إعداد : جريدة يومية فرنسية ***"le Monde"***، تحت عنوان : ***"Il faut sauver la loi informatique et libertés"***، 14 أوت 2004، موقع النشر : لإتحادية المعلوماتية و الأنترنت ***"Fédération informatique & liberté"***) :
http://www.vie-privee.org/news302

[2] _ أنظر : محمد أمين الرومي، "**جرائم الكمبيوتر و الأنترنت**"، **مرجع سابـــق**، صفحة 43.

الفرع الأول : المعلومات المعلوماتية الإسمية

و هي بدورها تنقسم إلى معلومات معلوماتية شخصية و معلومات معلوماتية موضوعية

الفقرة الأولى : المعلومات المعلوماتية الشخصية

أو ما سمي في قانون 1978 الفرنسي، "المعلوماتية، المعطيات و الحريات" بـــ ***"les Fichiers Nominatifs"*** أي المعطيات المعلوماتية الإسمية أو الشخصية و هي المعلومات المرتبطة بالشخص كالحالة الإجتماعية أو المدنية بما في ذلك الإسم و اللقب و محل الإقامة و الجنسية و السوابق العدلية مثلا، و يرى الأستاذ كتلا ***"Catala"*** مثله مثل قانون 1978 الفرنسي إنعدام حق الغير في الإطلاع على هذه المعلومات مراعاة للخصوصية إلا في حالة وجود موافقة شخصية من صاحبها أو بأمر من السلطة المختصة[1].

الفقرة الثانية : المعلومات المعلوماتية الموضوعية

"و من أمثلتها المقالات الصحفية و الملفات الإدارية للموظفين وهي موجهة إلى الغير بحسب الأصل، و يرى الأستاذ كتلا ***"Catala"*** أنه يمكن الفصل بين مالك المعلومة و الشخصية المتصلة بها، فالصحافي الذي يكتب مقالا عن شخص معين له حق على المقال و لكن لا يجب أن يتعدى هذا الحق على حق الشخص محل المقال نفسه"[2].

الفرع الثاني : المعلومات المعلوماتية خاصة بالمصنفات الفكرية

كالمؤلفات أو الأغاني أو الأفلام أو البرامج المعلوماتية في شكل معطيات معلوماتية المحمية بقانون المصنفات الفنية و قانون حقوق المؤلف و قانون براءة الإختراع[3].

الفرع الثالث : المعلومات المعلوماتية المباحة أو مجانية التسجيل

و هي المعلومات المباحة للكافة و هي في شكل معطيات معلوماتية[4]، و تنقسم هذه المعلومات المعلوماتية إلى معلومات معلوماتية مباشرة ***"Les Informations informatiques directes"*** و معلومات معلوماتية تابعة للدومين العام ***"Les Informations informatiques relevant du domaine public"***.

---

[1] _ أنظر : محمد أمين الرومي، **المرجـــع نفســـه**، صفحة 44.

[2] _ أنظر : محمد أمين الرومي، **المرجـــع نفســـه**، صفحة 44.

[3] _ أنظر : محمد أمين الرومي، **المرجـــع نفســـه**، صفحة 44.

[4] _ أنظر : محمد أمين الرومي، **المرجـــع نفســـه**، صفحة 44.

الفقرة الأولى : المعلومات المعلوماتية المباشرة

يمكن تسجيلها أو نقلها بكل حرية سواء تعلق الأمر بمعطيات صنعها صاحبها بنفسه كمستند الوارد ***"Fichier (Word)"*** يتضمن معلومات خاصة بصاحبها و التي هي من إبتكاره[1].

الفقرة الثانية : المعلومات المعلوماتية التابعة للدومين العام

و هي الحالة الشائعة في ميدان المعلوماتية، مثلا : قاعدة معطيات ***"Base de données"*** تستعمل وثائق رسمية فهذه القاعدة يمكن نقلها بكل حرية إذ هي مفتوحة للجمهور، إلا أن المعلومات المعلوماتية يمكن أن تطرح إشكال، فالمعلومة قد تكون من الدومين العام دون أن تكون حرة للنسخ و النقل أو الإستعمال، مثل ما هو الحال بالنسبة للمعلومات الإسمية أو الشخصية ***"Fichiers nominatifs"*** سواء كانت إدارية أو غير ذلك التي يحكمها القانون الفرنسي لسنة 1978 حول المعلوماتية و الحريات و بالتالي هنا نرجع إلى المعلومات المعلوماتية الشخصية[2].

المطلب الثاني : الجرائم المتعلقة بمخالفة الشكلية الملزمة لمعالجة المعطيات المعلوماتية الشخصية

في ما يخص الشكلية الملزمة في معالجة المعطيات المعلوماتية ذات طابع شخصي، فلقد وردت في الفصل الرابع من القانون رقم 78-17 تحت عنوان : ***« Formalités préalables à la mise en œuvre des traitement »*** أي "الشكلية السابقة لإجراء المعالجة الآلية"، أيضا في الفصل الخامس من نفس القانون تحت عنوان : ***« Obligations incombant aux responsables de traitements et droits des personnes »*** أي "الإلتزامات الواجبة على المسؤولين عن العلاجات الآلية و حقوق الأشخاص".

من بين أمثلة الشكلية الواجبة الإتباع في معالجة المعطيات ذات طابع شخصي، ما ورد في المادة 41 من قانون 6 جانفي 78-17 من الفصل الخامس من نفس القانون ، التي تنص صراحة أنه عندما يكون العلاج الآلي لمعطيات يهم أمن الدولة، الدفاع أو الأمن العام، فإن حق الدخول ***"Le droit d'accès"*** يمارس وفق الشروط المنصوص عليها في نفس المادة و بالتالي مسألة المساس بالمعطيات المعلوماتية ذات طابع شخصي تعد أساسا مسألة من النظام العام و تخضع المخالفات في هذا المجال بطبيعة الحال إلى أحكام قانون العقوبات الفرنسي أو بموجب نصوص عقابية خاصة الواردة في قانون 78-17.

---

(1)_ أنظر : X. Linant de Bellefonds, A. Hollande, ***Op.cit***, Page 62.

(2)_ أنظر : X. Linant de Bellefonds, A. Hollande, ***Ibid***, de la Page 62 à 63.

في ما يخص حق إجراء معالجة آلية لمعطيات إسمية أو الدخول إليها فإنه يرخص بها من خلال طلب رسمي يوجه إلى اللجنة الوطنية للمعلوماتية و الحريات، التي تعين أحد أعضائها الذي ينتمي أو كان ينتمي سابقا لمجلس الدولة، المحكمة العليا أو مجلس المحاسبة للقيام بالتحريات و التحقيق، بالإضافة إلى إجراء التعديلات اللازمة لهذه المعالجة، و هذا الأخير بإمكانه أن يستعين بموظف من اللجنة الوطنية، و يتم إعلام المعني بالأمر صاحب العلاج الآلي الذي تقدم بطلب الترخيص بأنهم قاموا بإجراء المراقبة، و عندما تستنتج اللجنة بإتفاق مع المسؤول عن المعالجة الآلية، بأن المعلومات المحتواة فيها لا تشكل خطر يمس بسلامة الدولة، الدفاع أو الأمن و النظام العام، فإن هذه المعطيات يمكن نشرها على الغير.

لكن السؤال الذي يمكن طرحه في هذا الصدد هو، ما الغاية أو الهدف من هذه الشكلية التي فرضها القانون رقم 78-17 ؟ القانون رقم 78-17 وضع ضوابط محكمة في كيفية القيام بالمعالجة أو التصرف في معطيات معلوماتية ذات طابع شخصي، حتى لا يكون هنالك تجاوزات أو مساس بحقوق و حريات الغير أو مساس بأمن الدولة أو الأمن العام.

في حالة مخالفة الشكلية التي إشترطها القانون رقم 78-17 في ما يخص معالجة المعطيات المعلوماتية ذات طابع شخصي لاسيما ما جاء في الفصل الرابع في ما يخص الشكليات الواجب إتباعها في إجراء معالجة معلوماتية لمعطيات ذات طابع شخصي و الفصل الخامس من نفس القانون، فإن المادة 50 من الفصل الثامن من نفس القانون تحت عنوان « ***Dispositions pénales*** » "الأحكام العقابية" تنص صراحة بأن مخالفة التنظيمات المنصوص عليها في القانون رقم 78-17 يعاقب عليها بموجب المواد 226-16 إلى 226-24 من قانون العقوبات الفرنسي، و بالتالي سنركز دراستنا في الجانب العقابي الذي نظمته هذه المواد.

بالرجوع إلى المادة 226-16 من قانون العقوبات الفرنسي فإننا نجدها تنص صراحة بأنه يعاقب من يقوم بإجراء معالجة آلية لمعطيات معلوماتية ذات طابع شخصي لأي سبب كان حتى نتيجة الإهمال و خلافا لأحكام القانون رقم 78-17 في ما يخص الشكلية الملزمة لإجراء هذه العلاجات الآلية حسب ما ورد في الفصل الرابع و الخامس من نفس القانون، بـــ 5 سنوات حبس و 300000 € غرامة مالية.

في ما يخص الركن المادي للجريمة : فإن العمومية التي جاءت بها هذه المادة تحيل الفهم إلى أن الجريمة قائمة مهما كانت طبيعة الشكلية المسبقة الواجبة الإتباع التي تم مخالفتها، و حتى إن كان التصريح من طرف المسؤول عن العلاج مطابق لمعايير مبسطة إلا أنها غير مطابقة في الأصل للتنظيم التشريعي الخاص الذي جاء به القانون رقم 78-17[1].

---

[1] _ أنظر : André Lucas, Jean Devrèze, Jean Frayssinet, ***Op.cit***, de la Page 670 à 671.

و بالتالي التفسير الضيق للمادة 226-16 ق.ع.فرنسي قد يجعلنا نعالج الجريمة على أنها جريمة شكلية من صنف الجرائم الآنية و ذلك بمجرد إجراء المعالجة الآلية للمعطيات الشخصية[1].

من جهة أخرى التجريمة تطبق على من له سلطة القرار و إجراء هذا النوع من العلاجات الآلية و كذا من حقق النتيجة المتمثلة في العلاج الآلي لهذا النوع من المعطيات مخالفا في ذلك النصوص الواردة في القانون رقم 78-17، و كباقي الجرائم المعلوماتية الأخرى السؤال يطرح في ما يخص كيفية إثبات الجريمة بطريقة معلوماتية في حالة غياب قرائن أخرى كالشهود[2].

في ما يخص الركن المعنوي للجريمة : فلقد إعتبرت محكمة النقض الفرنسية بأن الجريمة المرتبطة بالمادة 41 من القانون رقم 78-17 و المجرمة بنص المادة 226-16 ق.ع.فرنسي هي عبارة عن جريمة شكلية ***"Délit formel"*** محضة غير أن المادة 226-16 ق.ع.فرنسي تحيل الفهم إلى أن الركن المعنوي قد يكون السهو أو الإهمال، إذا في نظرنا لا مكان للركن المعنوي في مثل هذه الجريمة و يكفي توافر الركن المادي لقيامها[3].

المطلب الثالث : الجرائم المتعلقة بإدارة و تنظيم المعطيات المعلوماتية الشخصية

تجدر الإشارة إلى أن القانون رقم 78-17 يفرض على المسؤول عن المعالجة الآلية توفير الحماية الكافية للمعطيات المعلوماتية ذات طابع شخصي (المعطيات المعلوماتية الإسمية) [4] ، حيث نصت المادة 34 فقرة 1 من القانون رقم 78-17 ما يلي : "المسؤول عن المعالجة ملزم بأن يأخذ كل إحتياطاته اللازمة بالنظر لطبيعة المعطيات و المخاطر التي يمكن أن تنجم عن هذه المعالجة، للمحافظة على أمن هذه المعطيات و بما في ذلك منع أن تكون محل تحريف، أو إتلاف، أو أن يطلع عليها الغير من دون ترخيص....".

في حالة مخالفة أحكام المادة 34 من القانون رقم 78-17، في هذه الحالة تطبق أحكام المواد 226-17، 226- 18 و 226-18-1 ق.ع.فرنسي.

- في ما يخص المادة 226-17 ق.ع.فرنسي فالركن المادي للجريمة : وفقا لنفس المادة غير واضح، غير أنه يمكن أن نفهم عموما بأن إجراء أي معالجة آلية لمعطيات إسمية دون أخذ كل الإحتياطات اللازمة نظرا لطبيعة المعطيات و المخاطر التي يمكن أن تنجم عن هذه المعالجة، بمعنى المحافظة على أمن هذه المعطيات

---

(1)_ أنظر : André Lucas, Jean Devrèze, Jean Frayssinet, ***Op.cit***, Page 671.

(2)_ أنظر : André Lucas, Jean Devrèze, Jean Frayssinet, ***Idem***.

(3)_ أنظر : André Lucas, Jean Devrèze, Jean Frayssinet, ***Idem.***

(4)_ تعريف المعطيات المعلوماتية الإسمية : "يعد إسمي كل معلومة معلوماتية تحتوي على إسم شخص معين أو أي عنصر يسمح بالتعرف عليه بصفة قاطعة و حتمية (مثلا : رقم الهاتف، عنوان البريد الإلكتروني، ... إلخ)".

و بما في ذلك منع أن تكون محل تحريف، أو إتلاف، أو أن يطلع عليها الغير من دون أي ترخيص يعاقب عليها بالحبس لمدة 5 سنوات و 300000 € غرامة مالية حسب ما ورد في نص **المادة 34 من القانون رقم 78-17**.[1]

الغرفة الجزائية لمحكمة النقض الفرنسية مددت في مجال العقوبة وفقا للمادة 226-17 و ذلك بإعتبار أن الجريمة تعد قائمة بحكم نفس المادة سواء تعلق الأمر بمعالجة مستهدفة لشخص معين أو أي إنتفاع من المعالجة الآلية التي يمكن أن تكون بصفة مباشرة أو غير مباشرة مرتبطة بأي شخص آخر[2].

في ما يخص الركن المعنوي للجريمة : وفقا للمادة 226-17 ق.ع.فرنسي هو الخطأ، الإهمال أو التقصير في أخذ الإحتياطات اللازمة في المعالجة الآلية[3].

- في ما يخص المادة 226-18 ق.ع.فرنسي فالركن المادي للجريمة هو : جمع المعطيات ذات طابع شخصي أي القيام بالمعالجة الآلية و ذلك بطرق إحتيالية.

إذا الركن المعنوي للجريمة هنا : يتمثل في اللجوء إلى طرق إحتيالية غير مشروعة و التي يفهم منها توافر سوء النية لدى مرتكب الجريمة، و بالتالي و خلاف ما جاء في المادة 226-17 ق.ع.فرنسي المتعلقة بالجريمة الغير عمدية فإن المادة 226-18 ق.ع.فرنسي تنص صراحة على أن الجريمة عمدية و تتم بطرق إحتيالية.

و تجدر الإشارة إلى أن المشرع الفرنسي في المادة 226-18 ق.ع.فرنسي لم يحدد المفهوم أو المقصود من الطرق أو الوسائل الإحتيالية كما إكتفى بالنص على تجريم جمع المعلومات بطريقة الغش دون توضيحات أخرى، غير أنه بموجب قرار صادر عن الغرفة الجزائية لمحكمة النقض الفرنسية الصادر في 3 نوفمبر 1987، فإنه حدد بأنه حتى تكون الجريمة قائمة يجب أن يكون الهدف من جمع المعلومات هو تكوين مستند أو قاعدة معطيات ***"Document ou base de données"*** أو إجراء معالجة آلية للمعطيات، أما إذا كان الهدف من جمع هذه المعلومات هو تكوين ملف عادي في هذه الحالة لا تطبق أحكام قانون العقوبات[4].

---

(1)_ أنظر : André Lucas, Jean Devrèze, Jean Frayssinet, ***Op.cit***, Page 672.

(2)_ أنظر : André Lucas, Jean Devrèze, Jean Frayssinet, ***Idem***.

(3)_ أنظر : André Lucas, Jean Devrèze, Jean Frayssinet, ***Idem***.

(4)_ أنظر : André Lucas, Jean Devrèze, Jean Frayssinet, ***Op.cit***, Page 673.

و تجدر الإشارة إلى أن المادة 226–18 ق.ع.فرنسي تعد الأكثر تطبيقا من جملة النصوص القانونية الأخرى أمام العدالة الفرنسية[1]، و العقوبة المقررة في المادة 226–18 ق.ع.فرنسي هي نفس العقوبات المقررة في المواد السابقة لها.

في ما يخص جريمة إجراء معالجة آلية تخص شخص طبيعي على الرغم من معارضته لذلك : و هو المفهوم الذي جاءت به المادة 226–18–1 ق.ع.فرنسي و إن كانت التجريمة المنصوص عليها في هذه المادة قريبة كثيرا من التجريمة المنصوص عليها في المادة السالفة الذكر.

في ما يخص مضمون المادة 226–18–1 ق.ع.فرنسي فإنها تنص صراحة بأن "إجراء معالجة معطيات ذات طابع شخصي تخص شخص طبيعي و على الرغم من إعتراضه لذلك، و عندما يكون الهدف من هذه المعالجة البحث عن زبائن آخرين، لاسيما في المجال التجاري، أو عندما يكون الإعتراض مبني على أسباب جدية، في هذه الحالة العقوبة تكون 5 سنوات حبس و بغرامة قدرها 300.000 €".

بالنسبة للجريمة المستهدفة من المادة 226–18–1 ق.ع.فرنسي فإنها تقوم على ركنين :

الركن المادي للجريمة : وفقا لنفس المادة فهو واضح، و يتمثل في إجراء معالجة آلية لمعطيات ذات طابع شخصي تخص أشخاص طبيعية.

أما الركن المعنوي للجريمة : فإنه يستوجب وجود سوء نية من طرف الشخص القائم بالمعالجة لإستعمال المعطيات الشخصية و ذلك على الرغم من إعتراض الشخص الطبيعي الذي تتعلق به هذه المعطيات، إذا هنالك مساس واضح بالحريات الشخصية أو الحياة الشخصية، و هنا سوء النية تكون مفترضة إذا كان هنالك إعتراض صريح من طرف الغير المعني من بهذه المعالجة الآلية.

– في ما يخص جريمة وضع و الإحتفاظ في الذاكرة المعلوماتية بمعطيات حساسة ذات طابع شخصي : ففي هذه الحالة قانون 1978 أولى عناية خاصة بحماية الأشخاص في حالة وجود معطيات حساسة قد تمس بحرياتهم و حياتهم الشخصية (المواد 8 و 9 من المطلب الثاني، الفصل الثاني تحت عنوان : " أحكام خاصة ببعض الفئات من المعطيات ")[2].

العقوبة المقررة لهذه الجريمة وردت في المادة 226–19 ق.ع.فرنسي التي نصت بأنه : "على خلاف الحالات المنصوص عليها قانونا، فإنه في حالة وضع أو الإحتفاظ في الذاكرة المعلوماتية بدون الرضا الصريح للمعني

---

(1)_ أنظر : André Lucas, Jean Devrèze, Jean Frayssinet, ***Op.cit***, page 673.

(2)_ أنظر : André Lucas, Jean Devrèze, Jean Frayssinet, ***Idem***.

بالمعطيات ذات طابع شخصي التي تبين بصفة مباشرة أو غير مباشرة، الآراء السياسية، الفلسفية أو العقائدية، أو الإنتماء النقابي للأشخاص أو تلك المتعلقة بالصحة أو الميول الجنسية لهذا الشخص، يعاقب بـــ 5 سنوات حبس و بغرامة قدرها 300.000 €.

و يعاقب بنفس العقوبات، و على خلاف الحالات المنصوص عليها قانونا، عند وضع أو الإحتفاظ في الذاكرة المعلوماتية بمعطيات ذات طابع شخصي لجرائم، عقوبات، أو تدابير الأمن".

من خلال المادة السالفة الذكر يمكن أن نستنتج من نص الفقرة الأولى منها أن هنالك حالة أين لا تطبق العقوبة المتعلقة بجريمة الإحتفاظ في الذاكرة المعلوماتية بمعطيات حساسة ذات طابع شخصي التي تبين بصفة مباشرة أو غير مباشرة، الآراء السياسية، الفلسفية أو العقائدية، أو الإنتماء النقابي للأشخاص أو تلك المتعلقة بالصحة أو الميول الجنسية و هي حالة الرضا الصريح للشخص المستهدف أو المعني بتلك المعطيات و هذا ما يحد من الحماية التي جاء بها نص المادة العقابية، بمعنى أن الجريمة تعد غير قائمة في حالة إتفاق أو موافقة صريحة من طرف المعني بالمعالجة المعلوماتية، و تجدر الإشارة إلى أن مجلس الدولة الفرنسي ألزم أن يتوافر في مثل هذه الحالة إتفاق صريح، واضح و كتابي حتى تكون المعالجة الآلية مباحة[1].

بالإضافة إلى الحالة السالفة الذكر التي تستثني تطبيق العقوبة هنالك حالة آخر مشتركة بين الفقرة الأولى و الثانية من المادة 226–19 ق.ع.فرنسي و هو الترخيص ***"L'autorisation"*** بموجب القانون أي قانون 78 المواد 25، 26 و 27 و هذا لصالح الدولة و السلطات العمومية و الأشخاص المعنوية المسيرة للخدمات العمومية و ذلك لسبب المصلحة العامة.

– الآن في ما يخص جريمة الإحتفاظ الغير مشروع بالمعطيات المعلوماتية ذات طابع شخصي إلى ما يزيد عن المدة المحددة قانونا لذلك : هذه الجريمة نصت عليها المادة 226–20 ق.ع.فرنسي التي جاء فيها ما يلي: "في حالة الإحتفاظ بمعطيات ذات طابع شخصي إلى ما يزيد عن المدة المحددة قانونا، بموجب طلب ترخيص أو رأي، أو بموجب تصريح مسبق إلى اللجنة الوطنية للمعلوماتية و الحريات، يعاقب بـــ 5 سنوات حبس و بغرامة قدرها 300.000 € غرامة، إلا إذا تم الإحتفاظ لأهداف تاريخية، إحصائية، أو علمية و في إطار الشروط المحددة بموجب القانون.

يعاقب بنفس العقوبات في خارج الحالات المحددة بموجب القانون، حالة المعالجة الآلية لأسباب أخرى غير التاريخية، الإحصائية أو العلمية لمعطيات ذات طابع شخصي و المحتفظ بها إلى ما يزيد عن المدة المنصوص عليها في الفقرة الأولى".

---

(1)_ أنظر : André Lucas, Jean Devrèze, Jean Frayssinet, ***Op.cit***, Page 674.

من خلال المادة 226–20 ق.ع.فرنسي يمكن أن نستنتج بأن العقوبة المقررة لهذه الجريمة تنتفي إذا كان الغرض من الإحتفاظ بالمعطيات ذات طابع شخصي يعود لأهداف تاريخية مثلا : قاعدة معطيات أرشيفية ***"Base de données d'archives"***، أو إحصائية أو علمية و لكن في إطار شروط حددها قانون 1978، و من هذا المنطلق يكون الإحتفاظ بالمعطيات إلى ما يزيد عن المدة المحددة قانونا لذلك مباح و قانوني[1].

الفقرة الثانية من نفس المادة تعاقب بنفس العقوبة الواردة في الفقرة الأولى إذا كان الهدف من المعالجة الآلية ليس للأسباب الإستثنائية السالفة الذكر و إنما لأسباب أخرى و إذا تم الإحتفاظ في هذه الحالة بالمعطيات إلى ما يزيد عن المدة المحددة قانونا لذلك، هنا تطبق العقوبة[2].

المقصود من الإحتفاظ بالمعطيات المعلوماتية الإسمية في هذه الجريمة هو : "تخزين المعطيات المعلوماتية بكل أنواعها ذات طابع شخصي في الذاكرة سواء كانت ذاكرة الكمبيوتر أو أي نوع آخر من الذاكرات المعلوماتية أو الشبكات المعلوماتية و بطريقة تسمح التداول و الإطلاع عليها من جديد و خارج المدة المسموح بها قانونا للإحتفاظ بها".

المطلب الرابع : الجرائم المتعلقة بالإستعمال الغير مشروع لمعطيات معلوماتية شخصية

من بين أهم الجرائم المتعلقة بإستعمال المعطيات المعلوماتية ذات طابع شخصي و بطريقة غير مشروعة، لدينا : جريمة تحريف إستعمال أو الهدف ***"Détournement d'usage et de finalité"*** الذي أنشأت من أجله المعطيات المعلوماتية ذات طابع شخصي التي في الأصل أنشأت لإستعمال محدد أو مضبوط بموجب القانون أو التنظيم أو الترخيص، و المنصوص عليها في المادة 226–21 ق.ع.فرنسي، أما الجريمة الثانية فتتعلق بالتبليغ أو الإفشاء الغير مشروع ***"Divulgation illégale"*** لمعلومات معلوماتية ذات طابع شخصي و المنصوص عليها في المادة 226–22 ق.ع.فرنسي.

– في ما يخص جريمة تحريف إستعمال أو الهدف ***"Détournement d'usage ou de finalité"*** الذي أنشأت من أجله المعطيات المعلوماتية ذات طابع شخصي : فلقد نصت عليه المادة 226–21 ق.ع.فرنسي التي جاء فيه ما يلي : "في حالة حيازة شخص لمعطيات ذات طابع شخصي بمناسبة تسجيلها، ترتيبها أو تصنيفها، نقلها أو أي شكل آخر من المعالجة، و يحرف هذه المعلومات عن هدفها مثلما هو محدد في الأحكام التشريعية، العقد التنظيمي أو قرار اللجنة الوطنية للمعلوماتية و الحريات الذي يسمح المعالجة الآلية، أو بالتصريحات السابقة لإجراء هذه المعالجة، يعاقب بـــ 5 سنوات حبس و بغرامة قدرها 300.000 € غرامة".

---

(1) _ أنظر : André Lucas, Jean Devrèze, Jean Frayssinet, ***Op.cit***, page 674.

(2) _ أنظر : André Lucas, Jean Devrèze, Jean Frayssinet, ***Idem***.

إحدى أهم المواضيع المتعلقة بحماية المعطيات المعلوماتية ذات طابع شخصي هو ضمان إحترام الهدف الذي أنشأت من أجله هذه المعطيات [1] ***"Le respect de la finalité pour la quelle on été établis ces données"*** مثلما تم تحديده بموجب قانون 1978، أو بموجب التنظيم أو بناءا على قرار من اللجنة الوطنية للمعلوماتية و الحريات، أو بموجب تصريح مسبق على القيام بالمعالجة الآلية لهذا الصنف من المعطيات.

بهذا المعنى نص المادة 226-21 ق.ع.فرنسي قابل للتطبيق على كل شخص أيا كان حائز لمعلومات معلوماتية إسمية أو شخصية و ذلك بمناسبة تسجيلها ***"Enregistrement"***، ترتيبها أو تصنيفها ***"Classement"***، أو نقلها ***"Transmission"*** أو أي نوع آخر من المعالجات، إذا الركن المادي للجريمة : يتمثل في تحريف هذه المعطيات من الهدف الذي وضعت من أجله[2].

و من الملاحظ أن هذه الجريمة كثيرا ما يشار إليها سواء من طرف اللجنة الوطنية للمعلوماتية و الحريات أو من طرف العدالة، و بما في ذلك حالة الإستعمال التجاري لمعطيات معلوماتية ذات طابع شخصي وضعت في الأصل لإستعمال آخر، و مثال ذلك : القضية التي طرحت على محكمة المرافعات الكبرى لباريس [3] أين تم محاكمة موظف تابع للشركة الفرنسية للكهرباء و الغاز ***(EDF)*** على أساس جريمة تحريف إستعمال معلومات ذات طابع شخصي، إذ قام هذا الأخير ببيع قائمات من المشتركين في شركة ***(EDF)*** (الإسم و اللقب و العنوان السكني ومعلومات أخرى إن وجدت ذات طابع شخصي) إلى شركات التأمين، أو مثل القضية التي طرحت على محكمة ران [4] أين تم محاكمة مدير صندوق التوفير و الإحتياط الذي قام بمراسلة زبائن في بنكه بإشهارات لصالح مواد و خدمات لا علاقة لها بنشاط المؤسسة[5].

على العموم تطبيق نص المادة 226-21 ق.ع.فرنسي مخيب للأمل المرجو منه و هو الحد من جريمة التحريف للنتيجة التي وضعت من أجلها المعطيات المعلوماتية ذات طابع شخصي، إذ نجد مقابل العقوبة المقررة، المشرع الفرنسي نفسه في بعض الأحيان يضع قواعد مخالفة للمبدأ الذي جاءت به هذه المادة و من أمثلة ذلك : المادة 105 و 106 من قانون المالية الفرنسي لسنة 1999 (القانون رقم 98-1166 المؤرخ في 30 ديسمبر 1998) و الذي كان يسمح بتبادل المعلومات ذات طابع شخصي بين مديرية الضرائب و الجمارك

---

(1)_ أنظر : André Lucas, Jean Devrèze, Jean Frayssinet, ***Op.cit***, Page 675.

(2)_ أنظر : André Lucas, Jean Devrèze, Jean Frayssinet, ***Idem***.

(3)_ ***Jugement du tribunal de grande instances de Paris section pénale du 16 septembre 1994***

(4)_ ***Jugement du tribunal de Rennes section pénale du 8 septembre 1988***

(5)_ أنظر : André Lucas, Jean Devrèze, Jean Frayssinet, ***Idem***.

و أجهزة الضمان الإجتماعي، و مع العلم بأن النص العقابي الوارد في المادة 226-21 ق.ع.فرنسي كانت منصوص عليها سابقا في المادة 44 من قانون 6 جانفي 1978[1].

- في ما يخص الجريمة الثانية، أي جريمة الإفشاء الغير مشروع ***"Divulgation illégale"*** لمعلومات معلوماتية ذات طابع شخصي : فلقد نصت عليها المادة 226-22 ق.ع.فرنسي و التي جاء نصها كما يلي : "في حالة إلتقاط أي شخص، بمناسبة تسجيلها، ترتيبها أو تصنيفها، نقلها أو أي نوع آخر من المعالجة، معطيات ذات طابع شخصي و يترتب عنه المساس بإعتبار المعني أو حرمة حياته الشخصية، بإيصال و بدون ترخيص من طرف المعني، هذه المعطيات إلى علم الغير الذي ليست له صفة للحصول عليها، معاقب عليه بـــ 5 سنوات حبس و بغرامة قدرها 300.000 € غرامة.

الإفشاء المنصوص عليه في الفقرة السابقة معاقب عليه بـــ 3 سنوات حبس و 100.000 € غرامة إذا تمت بسبب عدم الإحتياط أو الإهمال.

في الحالات المنصوص عليها في الفقرتين السابقتين، المتابعة لا يمكن أن تتم إلا بناءا على شكوى من طرف الضحية، من طرف ممثله القانوني أو من طرف ذوي حقوقه".

من خلال نص المادة 226-22 ق.ع.فرنسي يمكن أن نلاحظ بأن الأشخاص المعنيين بالتجريمة هم الذين قاموا بإلتقاط معلومات معلوماتية ذات طابع شخصي و التي يترتب عن الإفشاء بها نتائج و آثار سلبية بالنسبة للمعني بهذه المعلومات سواء في إعتباره أو حرمة حياته الشخصية أو أيضا شرفه [2]، و بالتالي خارج هذه الحالة و إذا كان الإفشاء بالمعلومات أو المعطيات لا يرتب بالفعل أي أثر سلبي لصاحب هذه المعلومات أو المعطيات، في هذه الحالة لا تقوم الجريمة.

إذا الركن المادي للجريمة : يتمثل في تبليغ أو إفشاء معلومات ذات طابع شخصي للغير الذي ليست له أي صفة قانونية للحصول عليه و بدون ترخيص من طرف المعني بهذه المعلومات.

في ما يخص الركن المعنوي للجريمة : فلقد فرقت المادة 226-22 ق.ع.فرنسي بين حالتين :

الأولى حسب الفقرة الأولى و هو أن يتم الإفشاء بالمعلومات ذات طابع شخصي بطريقة عمدية، و في هذه الحالة العقوبة المقررة هي 5 سنوات حبس و غرامة قدرها 300.000 €.

---

(1) _ أنظر : André Lucas, Jean Devrèze, Jean Frayssinet, ***Op.cit***, Page 676.

(2) _ أنظر : André Lucas, Jean Devrèze, Jean Frayssinet, ***Idem***.

أما الحالة الثانية حسب الفقرة الثانية من نفس المادة، هو أن يتم الإفشاء بسبب عدم إتخاذ الإحتياطات أو الإهمال، في هذه الحالة العقوبة المقررة تكون 3 سنوات حبس و 100.000 €.

المطلب الخامس : جريمة الإعتراض لعمل اللجنة الوطنية للمعلوماتية و الحريات

كما قلنا في بداية هذا المبحث يعد عمل اللجنة الوطنية للمعلوماتية و الحريات ضروري لضمان التطبيق السليم لقانون 6 جانفي 1978 و الحرص على عدم خرق بنوده في مجال المعطيات المعلوماتية ذات طابع شخصي، و بالتالي عرقلة أعمالها يعد خرقا لقانون 1978 و بالتالي معاقب عليه جزائيا بموجب نص خاص أي قانون 1978.

بالرجوع إلى قانون 6 جانفي 1978 نجد المادة 51 من الفصل الثامن من نفس القانون تحت عنوان : "الأحكام الجزائية" ، تنص عما يلي : "يعاقب بالحبس لمدة سنة و 15000 € غرامة في حالة الإعتراض لعمل اللجنة الوطنية للمعلوماتية و الحريات :

1 – سواء بالإعتراض لمهام أعضائه أو أعوانه المؤهلين لذلك تطبيقا للفقرة الأخيرة من المادة 19.

2 – سواء برفض تبليغ لأعضائه أو أعوانه المؤهلين تطبيقا للفقرة الأخيرة من المادة 19 المعلومات أو المستندات المفيدة لمهمتهم، أو بإخفاء هذه المستندات أو المعلومات، أو بحذفها.

3 – سواء بتبليغ معلومات غير مطابقة لمحتوى التسجيلات مثلما كانت عليه في الوقت الذي طولبت بها أو لا تبين هذا المحتوى في شكل يسمح التطلع عليه بصفة مباشرة".

المبحث الثالث : جرائم المعلوماتية الماسة بإعتبار الأشخاص و حرمة حياتهم الشخصية عبر شبكة الأنترنت

أي معلومة بإمكانها التنقل عبر شبكة الأنترنت و في آن واحد يمكن أن تكون حاملة لجريمة، و تجدر الإشارة إلى أنه ليست شبكة الأنترنت محل التجريم و إنما محل التجريم هو إستعمالها بطريقة من شأنها المساس بالمال المملوك للغير كما رأيناه في الفصل الأول، أو أيضا بالأشخاص في إعتبارهم كما هو الحال في ما يخص جريمة القذف و الإهانة و السب عبر الشبكة المفتوحة ***"L'infraction de diffamation et d'humiliation (outrage) et d'injure à travers le réseau ouvert"*** (المطلب الأول)، أو خرق حرمة الحياة الشخصية و بالأخص المساس بسرية المراسلات عبر شبكة الأنترنت ***"L'infraction d'atteinte à la vie privé et plus précisément des correspondances privées sur le réseau Internet"*** (المطلب الثاني) ، و تجدر الإشارة إلى أنه كان من الممكن إدماج المبحث الثاني من نفس الفصل في هذا العنوان بإعتبار المساس بالمعطيات الشخصية (المعطيات الإسمية ***"Les fichiers nominatifs"***) يعتبر هو الآخر طريقة من بين الطرق العديدة للمساس بحرمة الحياة الشخصية إلا أننا لم نفعل كذلك بإعتبار أن هذا الموضوع خصص له المشرع الفرنسي قانون خاص فريد من نوعه و نظرا لتضمنه أنواع كثيرة من الجرائم متعلقة بهذا الموضوع فضلنا دراسة هذه النقطة في مبحث ثاني مستقل.

المطلب الأول : جريمة القذف و الإهانة و السب عبر شبكة الأنترنت

من بين الجرائم الرئيسية التي تدخل في باب جرائم الإعتبار هي جريمة القذف، الإهانة و السب، و تجدر الإشارة إلى أن هذه الجرائم ورد النص عليها في قانون العقوبات و إن كانت في الحقيقة لها صلة وطيدة بقانون الإعلام المؤرخ في 3 أفريل 1990[1].

و تجدر الإشارة إلى أن المشرع الجزائري أدخل تعديلات في ما يخص هذه الجرائم الثلاثة، إثر تعديل قانون العقوبات بموجب القانون رقم 01-09 المؤرخ في 2001/6/26[2].

و بالتالي سنتطرق لهذه الجرائم الثلاثة من حيث التفسير في حالة إرتكابها في مجال معلوماتي مفتوح، أي شبكة الأنترنت سواء من خلال التشريع الجزائري أو المقارن.

---

[1]_ أنظر : أحسن بوسقيعة، "**الوجيز في القانون الجزائي الخاص** " **(الجزء الأول) الجرائم ضد الأشخاص و الجرائم ضد الأموال** ، دار هومه، (طبعة منقحة و متممة في ضوء قانون 2006/12/20) الطبعة الثامنة 2008، (الجزائر)، صفحة 194.

[2]_ أنظر : أحسن بوسقيعة، **المرجـــع نفســـه**، صفحة 194.

الفرع الأول : جريمة القذف عبر شبكة الأنترنت

وردت جريمة القذف كجريمة تقليدية في الأصل بالنسبة للتشريع الجزائري في نص المادة 296 ق.ع.جزائري، و بالإضافة إلى المادة 144 مكرر و المادة 146 ق.ع.جزائري، أما المشرع الفرنسي فلقد نص على هذه الجريمة بموجب تشريع خاص و بالأخص قانون الإعلام المؤرخ في 29 جويلية 1881 المتعلق بحرية الصحافة[1].

و تجدر الإشارة إلى أن التعريف الذي جاء به المشرع الجزائري بخصوص جريمة القذف و الوارد في نص المادة 296 فقرة 1 ق.ع.جزائري هو نفس التعريف الذي جاء به المشرع الفرنسي في نص المادة 29 فقرة 1 من قانون 29 جويلية 1881 التي عرفتها على أنها :

أي : "كل إدعاء أو إتهام بواقعة من شأنها المساس بشرف أو بإعتبار شخص أو هيئة المدعى عليها بها تعد قذف"، كما عرفتها المادة 296 فقرة 1 على أنها : "... كل إدعاء بواقعة من شأنها المساس بشرف أو إعتبار الأشخاص أو الهيئات المدعى عليها بها أو إسنادها إليهم أو إلى تلك الهيئة ..."[2].

السؤال الذي يمكن طرحه في هذه الحالة هو : هل نص المشرع سواء الجزائري أو الفرنسي على إمكانية إرتكاب جريمة القذف عبر الشبكات المعلوماتية، أم أن النصوص العقابية التقليدية يمكن أن يمتد أثرها إلى محيط المعلوماتية ؟

بالرجوع إلى الفقرة الثانية من المادة 296 ق.ع.جزائري يمكن أن نلاحظ بأن المشرع لم ينص صراحة على المعلوماتية أو شبكة الأنترنت كوسيلة لإرتكاب جريمة القذف، إذ نصت : "... من الممكن تحديدهما من عبارات الحديث أو الصياح أو التهديد أو الكتابة أو المنشورات أو اللافتات أو الإعلانات موضوع الجريمة "، غير أنه يمكن تمديد حالة الحديث أو الكتابة أو المنشورات أو اللافتات أو أيضا الإعلانات إلى محيط المعلوماتية بكل سهولة لكون شبكة الأنترنت هي الأخرى وسيلة بإمكانها تحقيق ذلك، و بإعتبار أن المشرع بالمقابل لم يحدد الوسائل المستعملة لتحقيق الجريمة على سبيل الحصر، و بالتالي يأتي في هذه الحالة دور القضاء في خلق إجتهادات في هذا السبيل.

---

(1)_ أنظر : **الملحق رقم 15**

(2)_ أنظر نص المادة باللغة الفرنسية :

Art 29 § 1 : « Toute allégation où imputation d'un fait qui porte atteinte à l'honneur ou à la considération de la personne ou du corps auquel la fait est imputé est une diffamation ».

في حين أنه بالرجوع إلى نص المادة 144 مكرر ق.ع.جزائري فإنها نصت صراحة و بخلاف المادة 296 فقرة 2 ق.ع.جزائري على أن القذف الموجه إلى رئيس الجمهورية أو الهيئات العمومية قد يكون بأية آلية لبث الصوت أو الصورة أو بأية وسيلة إلكترونية أو معلوماتية أو إعلامية أخرى.

أما بالرجوع إلى التشريع العقابي الفرنسي في هذا المجال فلقد جاء مخالف للتشريع الجزائري لكونه أدمج هذه الجريمة في قانون الإعلام الصادر بتاريخ 29 جويلية 1881 المتعلق : بحرية الصحافة ***"La liberté de la presse"***، المعدل و المتمم، و بالأخص في جزء تحت عنوان : "عن الجرائم و الجنح المرتكبة بواسطة الصحافة أو أي وسيلة أخرى للنشر ***"Des crimes et délits commis par voie de la presse ou tout autre moyen de publication"***"، بالإضافة إلى قانون 30 سبتمبر 1986 المتعلق : بالإتصال السمعي البصري ***"La communication audiovisuelle"***، هذين القانونين يعاقبان الجرائم المرتكبة بواسطة وسائل الإعلام و بما فيها الوسائل الإلكترونية و المعلوماتية، بإعتبار أن كل أنواع وسائل الإعلام مستهدفة بهذه القوانين (المواد 23 و 30، 31 و 32 من قانون 1881)، وهذه النصوص القانونية قابلة للتطبيق في محيط الأنترنت و الشبكات المعلوماتية المفتوحة، و بما فيها الرسائل الإلكترونية المتبادلة في مجال خاص ***"Les messages de correspondance privée"***، و بالتالي الرسائل الإلكترونية المستهدفة هي تلك التي تم نشرها بواسطة موقع أنترنت أو في مجال مناقشة بين مستعملي شبكة الأنترنت ***"Forum de discussion entre les internautes"***[1]، و يشترط في هذه الحالة حتى تقوم الجريمة أن يكون مجال المناقشة المعلوماتي مفتوح إلى كامل جمهور الأنترنت أي المتصلين بالشبكة، بمعنى أنه إذا كان مجال المناقشة المعلوماتي من نوع خاص ***"De type privé"*** و مفتوح إلا لعدد محدود من الجمهور في هذه الحالة لا تقوم الجريمة كما هو الحال بالنسبة للرسائل الإلكترونية المتبادلة في مجال خاص، لسبب بسيط و هو إنتفاء ركن العلنية عبر شبكة الأنترنت لقيام الجريمة[2].

في ما يخص الوسائل المستعملة في جريمة القذف، فبالنسبة للمشرع الجزائري كما قلنا سابقا فإنه لم يشير صراحة إلى أنها قد ترتكب بواسطة المعلوماتية (الأنترنت) في المادة 296 فقرة 1 ق.ع.جزائري على خلاف المادة 144 مكرر ق.ع.جزائري، في حين أن المشرع الفرنسي نص عليها صراحة في المادة 23 من قانون 29 جويلية 1881 و بالنسبة لكل أنواع الأشخاص أو الهيئات المستهدفة بهذه الجريمة، و التي جاء نصها كما يلي :

---

(1)_ مجال المناقشة المعلوماتي عبر شبكة الأنترنت هو : مكان يتم فيه التناقش في مواضيع معينة ذات مصلحة عامة، و كل عضو في هذا المجال المعلوماتي بإمكانه إرسال رسائل إلكترونية التي يمكن لبقية الأعضاء الإطلاع عليها، والذين بدورهم بإمكانهم الرد.

(2)_ أنظر : Féral-schuhl Christiane, ***Op.cit***, page 90.

المادة 23 : "... أو بأي وسيلة إتصال بالجمهور بطريقة إلكترونية ..."[1].

و تجدر الإشارة إلى أن المواد 30 و 31 و 32 من نفس القانون نصت بأنه إذا إرتكب القذف بإحدى الوسائل المنصوص عليها في المادة 23 بما فيها الوسيلة الإلكترونية أو المعلوماتية و ضد الأشخاص أو الهيئات الواردة في نصوص المواد 30 و 31 و 32 فإنه يعد جريمة و بالتالي معاقب عليه جزائيا بموجب هذه المواد.

و تجدر الإشارة من جهة أخرى إلى أن المشرع الفرنسي في هذا الصدد قيد شرعية المتابعة الجزائية في هذه الجريمة وفقا للمادة 65 من قانون 29 جويلية 1881 من حيث التقادم بـــ 3 أشهر من تاريخ أول فعل نشر أو تثبيت عبر شبكة الأنترنت و ليس من تاريخ إكتشاف الجريمة، في حين أن المشرع الجزائري لم ينص على مهلة خاصة لتقادم الدعوى العمومية في هذه الجريمة و بالتالي فهي تتقادم وفقا لقواعد القانون العام، أي بمرور 3 سنوات من تاريخ إرتكابها[2]، ما لم يتخذ أي إجراء يقطع ميعاده، و نفس الشيء بالنسبة لجريمتي الإهانة و السب عبر شبكة الأنترنت.

الفرع الثاني : جريمة الإهانة عبر شبكة الأنترنت

و هو الفعل المنصوص عليه في المادة 144 ق.ع.جزائري، لكن منذ تعديل قانون العقوبات بموجب القانون رقم 01-09 المؤرخ في 2001/06/26، أضاف المشرع صورة جديدة من الجرائم و المتمثلة في إهانة بعض الهيئات العمومية، و بالأخص المادة 144 مكرر و مكرر 2 و 146 ق.ع.جزائري[3].

و بالتالي الفئات المعنية بالجريمة هي : رئيس الجمهورية (مادة 144 مكرر ق.ع.جزائري)، و الرسول (ص) أو باقي الأنبياء أو ما هو معلوم من الدين و بأي شعيرة من شعائر الإسلام (مادة 144 مكرر 2 ق.ع.جزائري)، و أخيرا البرلمان أو إحدى غرفتيه أو المجالس القضائية أو المحاكم أو الجيش الوطني الشعبي أو أية هيئة نظامية أو عمومية أخرى (مادة 146 ق.ع.جزائري).

السؤال الذي يطرح في هذا المجال : ما هو العامل المشترك بين هذه المواد، و كذا علاقتها بمحيط المعلوماتية و الجريمة المعلوماتية ؟

---

[1]_ أنظر نص المادة باللغة الفرنسية :

Art. 23 : « … soit par tout moyen de communication au public par voie électronique … ».

[2]_ أنظر : أحسن بوسقيعة، "**الوجيز في القانون الجزائي الخاص**" **(الجزء الأول) الجرائم ضد الأشخاص و الجرائم ضد الأموال، مرجـــع ســـابـــق**، صفحة 212.

[3]_ أنظر : أحسن بوسقيعة، **المرجـــع نفســـه**، صفحة 223.

بالرجوع إلى نص المادة 144 مكرر ق.ع.جزائري فإننا نجدها تنص : "يعاقب بالحبس من ثلاثة (3) أشهر إلى إثني عشر (12) شهرا و بغرامة من 50.000 د.ج إلى 250.000 د.ج أو بإحدى هاتين العقوبتين فقط كل من أساء إلى رئيس الجمهورية بعبارات تتضمن إهانة أو سبا أو قذفا سواء كان ذلك عن طريق ... أو أية وسيلة إلكترونية أو معلوماتية أو إعلامية أخرى ...".

في حين أن المادة 144 مكرر 2 ق.ع.جزائري جاء نصها كما يلي : "يعاقب بالحبس من ثلاث سنوات (3) سنوات إلى خمس (5) سنوات و بغرامة من 50.000 دج إلى 100.000 دج أو إحدى هاتين العقوبتين فقط من أساء إلى الرسول (ص) أو باقي الأنبياء أو إستهزأ بالمعلوم من الدين بالضرورة أو بأية شعيرة من شعائر الإسلام سواء ... أو أية وسيلة أخرى ...".

أما المادة 146 ق.ع.جزائري فجاء نصها كما يلي : "تطبق على الإهانة أو السب أو القذف الموجه بواسطة الوسائل التي حددتها المدتين 144 مكرر و 144 مكرر 1 ضد البرلمان أو إحدى غرفتيه أو ضد المجالس القضائية أو المحاكم أو الجيش الشعبي الوطني أو أية هيئة نظامية أو عمومية أخرى، ...".

في حين أن المشرع الفرنسي نص على هذه الجريمة صراحة في المادة 26 من قانون 29 جويلية 1881 في ما يخص إهانة رئيس الجمهورية، و التي جاء نصها كما يلي :

المادة 26 : "الإساءة[1] الموجهة إلى رئيس الجمهورية بإحدى الوسائل المنصوص عليها في المادة 23[2] معاقب عليها بغرامة قدرها 45000 €.

العقوبات المقررة في الفقرة السابقة تطبق على إهانة الشخص الذي يمارس الكل أو جزء من إمتيازات أو مهام رئيس الجمهورية"[3].

و بالتالي بعد التمعن جيدا في النصوص القانونية السالفة الذكر سواء الجزائرية أو الفرنسية يمكن أن نلاحظ بأن العامل المشترك الرابط بينها هو الوسيلة التي بموجبها يمكن إرتكاب جريمة الإهانة ضد الفئات المحددة

---

(1)_ في ما يخص مصطلح « ***Offense*** » يعني بالغة العربية "الإساءة"، بمعنى أن جريمة الإساءة قد تشمل جريمة القذف أو السب أو الإهانة في آن واحد أو إحداهم، و تجدر الإشارة إلى أن هذا المصطلح إستعمل سواء من طرف المشرع الجزائري أو الفرنسي إلا إزاء فئات خاصة من الأشخاص، بما فيها رئيس الجمهورية أو الرسول (ص) و باقي الأنبياء بالنسبة للتشريع الجزائري (المواد 144 مكرر و مكرر 2 ق.ع.جزائري و المادة 26 من قانون 29 جويلية 1881 الفرنسي).

(2)_ من بين الوسائل التي نصت عليها المادة 23 في ما يخص إرتكاب جريمة الإهانة هي : الوسائل الإلكترونية و المعلوماتية و بما فيها شبكة الأنترنت.

(3)_ أنظر نص المادة باللغة الفرنسية :

Art 26 : « L'offense au Président de la République par l'un des moyens énoncés dans l'article 23 est punie d'une amende de 45000 euros.

Les peines prévues à l'alinéa précédent sont applicable à l'offense à la personne qui exerce tout ou partie des prérogatives du Président de la République ».

بموجب نفس هذه المواد أي الوسيلة الإلكترونية أو المعلوماتية و بالأخص شبكة الأنترنت كما هو الحال بالنسبة لجريمة القذف.

و عليه كل فعل إجرامي متعلق بإهانة الفئات المنصوص عليها بموجب المواد 144 مكرر و مكرر 2 و 146 ق.ع.جزائري و ذلك عبر شبكة الأنترنت يمكن أن يكون محل متابعة و لو بصفة تلقائية من طرف النيابة العامة وفقا للمادة 144 مكرر فقرة 2 ق.ع.جزائري، شريطة إتيان دليل وقوع الجريمة المسندة إلى شخص طبيعي معين أو معنوي و هو موضوع آخر متعلق بالدليل الإلكتروني و قيمته القانونية حتى تتم المتابعة الجزائية.

الفرع الثالث : جريمة السب عبر شبكة الأنترنت

بالرجوع إلى المادة 29 فقرة 2 من قانون 29 جويلية 1881 نجدها تعرف السب كما يلي :

المادة 29 : "... كل عبارة شتم، مصطلح كراهية أو شتم الذي لا يحتوي أي إسناد إلى واقعة معينة عبارة عن سب"، في حين أن المشرع الجزائري عرف هذه الجريمة في نص المادة 297 ق.ع.جزائري التي جاءت عموما بنفس المعنى : "يعد سبا كل تعبير مشين أو عبارة تتضمن تحقيرا أو قدحا لا ينطوي على إسناد أية واقعة"[1].

في ما يخص الفئات المستهدفة بهذه الجريمة حسب التشريع العقابي الجزائري فهي : الأفراد (المادة 299 ق.ع.جزائري)، الفرد أو الأفراد بسبب إنتمائهم العرقي، الديني أو المذهبي (المادة 298 ق.ع.جزائري)، الهيئات العمومية و الجيش الوطني الشعبي و المجالس القضائية (المادة 146 ق.ع.جزائري)، و أخيرا رئيس الجمهورية، و الرسول محمد (ص) و باقي الأنبياء (المادة 144 مكرر و مكرر 2 ق.ع.جزائري).

أما بالنسبة للتشريع العقابي الفرنسي في ما يخص جريمة السب بالإضافة إلى التعريف الذي جاء به في المادة 29 فقرة 2 من قانون 29 جويلية 1881 نجد المواد : 30 و 31، و كذا المادة 33 من نفس القانون التي أشارت في نصها إلى المادتين السالفتي الذكر و إن كانت في الأصل متعلقة بجريمة القذف ، حيث جاء نص المادة 33 كما يلي :

المادة 33 : "السب المرتكب بنفس الوسائل في مواجهة الهيئات أو الأشخاص المحددين بموجب المادة 30 و 31 من نفس القانون الحالي معاقب عليه بغرامة قدرها 12000 €.

---

(1)_ أنظر نص المادة باللغة الفرنسية :

Art 29 § 2 : « ... Toute expression outrageante, termes de mépris ou invective qui ne renferme l'imputation d'aucun fait est une injure ».

السب المرتكب بنفس الطريقة في مواجهة الخواص، عندما لا تكون مسبوقة بإستفزازات، معاقب عليه بغرامة قدرها 12000 €.

يعاقب بستة أشهر حبس و 22500 € غرامة السب المرتكب، طبقا للشروط الواردة في الفقرة السابقة، في مواجهة شخص أو مجموعة أشخاص بسبب أصلهم أو إنتمائهم أو عدم إنتمائهم إلى عرق، أمة، فئة أو ديانة معينة.

في حالة الإدانة بأحد الوقائع الواردة في الفقرة السابقة، يمكن للمحكمة أن تأمر زيادة على ذلك :

1° بإعلان أو نشر الحكم الصادر وفقا للشروط المحددة في المادة 131 فقرة 35 من قانون العقوبات"[1].

و بالتالي المادة 33 عممت تجريم الوسائل المستعملة في إرتكاب جريمة السب في المواد 30 و 31 و من بينها تقنية المعلوماتية في حالة إستعمالها لإرتكاب الجريمة ضد كل من المحاكم و المجالس و الجيوش البرية البحرية و الجوية، الهيئات و الإدارات العمومية (مادة 30) و كذا ضد أعضاء الوزارات و أعضاء إحدى غرفتي البرلمان و الموظفين العموميين و الأعوان التابعين للسلطة العمومية و الوزراء و المواطنين المكلفين بخدمات أو عهدة عمومية مؤقتة أو دائمة، المحلفين و الشهود بسبب شهادتهم (مادة 31).

و تجدر الإشارة إلى أن جريمة السب مثلها مثل الإهانة أو القذف حتى تتم عبر الشبكة الأنترنت أي الشبكة المفتوحة يجب توافر نظام قد يكون إلكتروني كالنقال أو أي نوع آخر من الآلات الإلكترونية إذا كانت مزودة بحق الدخول في شبكة الأنترنت مثلا، أو نظام معلوماتي كما هو متعارف عليه من خلال إستعمال الكمبيوتر بشرط أن يكون هو الآخر مزود بحق الدخول في شبكة الأنترنت، و بالتالي فعل السب أو الإهانة أو القذف يمكن أن يشكل جريمة إذا توافرت أركانه الأساسية بالإضافة إلى الوسيلة و الكيفية التقنية لنشرها، التي قد تكون بالكتابة (في صفحات أو مواقع الأنترنت أو مجالات المناقشة المفتوحة لكافة مستعملي شبكة الأنترنت و الذين بإمكانهم التطلع على العبارات المجرمة) أو بواسطة الإعلامات أو الإشهارات في مواقع الأنترنت أو صفحات الأنترنت بحيث يمكن لأكبر عدد من الجمهور التطلع عليها، كما يمكن أن ترتكب هذه الجرائم

---

[1] _ أنظر نص المادة باللغة الفرنسية :

Art 33 : « L'injure commise par les même moyens envers les corps ou les personnes désignés par l'article 30 et 31 de la présente loi sera punie d'une amende de 12000 euros.
L'injure commise de la même manière envers les particuliers, lorsqu'elle n'aura pas été précédée des provocations, sera punie d'une amende de 12000 euros.
Sera punie de six mois d'emprisonnement et de 22500 euros d'amende l'injure commise, dans les conditions prévues à l'alinéa précédent, envers une personne ou un groupe de personnes à raison de leur origine ou de leur appartenance ou de leur non-appartenance à une ethnie, une nation, une race ou une religion déterminée.
En cas de condamnation pour l'un des faits prévus par l'alinéa précèdent, le tribunal pourra en outre ordonner :
1° L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35 du code pénal ».

بواسطة إستعمال برامج الكلام أو تسجيل و تثبيت الكلام عبر شبكة الأنترنت[1] و بطريقة تسمح لعدد كبير من الجمهور سماع العبارات المجرمة و المسندة إلى المجني عليه (شخص طبيعي أو معنوي).

من جهة أخرى هنالك بعض التساؤلات التي يمكن طرحها من بينها، لماذا لم يعمم المشرع الجزائري كما هو الحل بالنسبة للمشرع الفرنسي إستعمال الوسائل الإلكترونية أو المعلوماتية صراحة في ما يخص إرتكاب جرائم السب و القذف و الإهانة ضد كل الفئات المحمية بموجب قانون العقوبات كما فعل بالنسبة لجريمة الإساءة في المواد 144 مكرر و مكرر 2 و 146 ق.ع.جزائري حتى تكون الحماية الجزائية متكاملة تمتد إلى جل التكنولوجيات الجديدة التي تسمح إرتكاب هذه الجرائم ؟

أيضا السؤال الآخر الذي يمكن طرحه هو، ما هو القانون الواجب التطبيق و كذا المحكمة المختصة في المحاكمة الجزائية إذا كان المجني عليه في الجزائر و الجاني مرتكب الجريمة في دولة أخرى أو أن موقع الأنترنت الذي نشرت فيه العبارات المجرمة تابعة لدولة ثالثة ؟

المطلب الثاني : خرق حرمة الحياة الشخصية عبر شبكة الأنترنت

إذا كان الإستعمال الغير مشروع لشبكة الأنترنت قد يؤدي إلى إرتكاب كل من جرائم القذف، السب أو الإهانة إزاء الغير، فإنه من جهة أخرى قد يؤدي إستعماله بطريقة غير مشروعة إلى المساس بحرمة الحياة الشخصية للأفراد، كما هو الحال بالنسبة لجريمة المساس بسرية المراسلات للأفراد عبر شبكة الأنترنت ، الفعل المجرم بموجب المواد 226–15 و 432–9 ق.ع.فرنسي.

بالرجوع إلى المادة 226–15 ق.ع.فرنسي نجدها تنص عما يلي :

المادة 226–15 : "في حالة إرتكاب بسوء نية، فتح، حذف، تأخير أو تحريف مراسلات وصلت أم لا إلى مكان المراسلة و موجهة إلى الغير، أو الإطلاع عليها إحتياليا، معاقب عليه بسنة (1) حبس و 45000 € غرامة.

---

[1]_ و تجدر الإشارة إلى أنه حتى يكون الكلام بهدف القذف السب و أو الإهانة عبر شبكة الأنترنت مجرم يشترط أن يكون في إطار مفتوح إلى كافة الجمهور أي مجال حدث جماعي و أنه إذا تم ذلك في إطار خاص كأن يكون الحديث إلا مع شخص واحد على سبيل الخصوص و في هذه الحالة تنتفي الجريمة.

تطبق نفس العقوبات في حالة إرتكاب بسوء نية، حجز، تحريف، إستعمال أو إفشاء مراسلات صادرة، مرسلة أو متحصل عليها بوسائل الإتصال الحديثة أو القيام بتثبيت آلات هدفها تحقيق هذه الأفعال"[1].

من خلال الفقرة الثانية من نص المادة السالفة الذكر يمكن أن نلاحظ بأن المشرع الفرنسي مدد مجال الحماية الجزائية للمراسلات إلى تلك التي تتم بوسائل الإعلام المستحدثة (المعلوماتية و شبكة الأنترنت)، و بالتالي كل ما يدخل في حكم المراسلة الإلكترونية و بما في ذلك البريد الإلكتروني فهو محل حماية جزائية، بمعنى المساس بسرية هذه المراسلات و في إطار الأفعال المنصوص في المادة أعلاه لاسيما : حجز، تحريف، إستعمال أو إفشاء هذه المراسلات ذات طبيعة إلكترونية معلوماتية[2].

و تجدر الإشارة إلى أن محكمة باريس [3]، رفضت تبريرات محامي المتهمين الذي إعتبر أن الرسائل الإلكترونية لا تتمتع بقواعد السرية التي تتمتع بها الرسائل التقليدية بحجة أنها غير محمية تقنيا بموجب خوارزمية ***"Non cryptés"*** كما أنها تمر على وسطاء موزعين للخدمات ***"Serveurs intermédiaires"*** الذين يتولون نقل هذه الرسائل الإلكترونية عبر الشبكة و هي مكشوفة إلى المرسلين إليهم[4].

و كان تبرير المحكمة في رفضها لهذا الطرح هو أن طبيعة الرسالة الإلكترونية التي هي الأخرى ترسل بمبادرة من المرسل ***"L'expéditeur"*** إلى المرسل إليه ***"Le destinataire"*** الذي من المفروض يتلقاها وحده دون سواه، عبارة عن مراسلة شخصية ***"Correspondance personnelle"***، و بالتالي تطبق عليها نفس الأحكام المطبقة بالنسبة للبريد التقليدي لاسيما الفقرة الأولى من المادة 226-15 ق.ع.فرنسي[5].

و بالتالي و من جهة أخرى يمكن إعتبار جريمة المساس بسرية المراسلات الشخصية قائمة حتى في مجال إلكتروني إذا كان أساس المراسلة هو تفريد كلا من المرسل و المرسل إليه[6].

---

(1)_ أنظر نص المادة باللغة الفرنسية :

Art 226-15 c.p.f : « Le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non a destination est adressée à des tiers, ou d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 45000 euros d'amende.
Est 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 voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions ».

(2)_ أنظر : Frédérique-Jérome Pansier & Emmanuel Jez, ***La Criminalité sur Internet***, édition Que sais-je ? (P.U.F) 2ème édition mise à jour, Septembre 2001, page 71.

(3)_ ***Jugement du tribunal de grandes instances de Paris Section pénale du 2 novembre 2000***

(4)_ أنظر : Frédérique-Jérome Pansier & Emmanuel Jez, ***Op.cit***, page 71.

(5)_ أنظر : Frédérique-Jérome Pansier & Emmanuel Jez, ***Idem***.

(6)_ أنظر : Frédérique-Jérome Pansier & Emmanuel Jez, ***Ibid***, page 72.

من جهة أخرى يمكن أن نلاحظ بأن المادة 226-15 نصت في فقرتها الثانية نصت على فعل إجرامي آخر سيسمح بتحقيق حجز، تحريف، إستعمال أو إفشاء المراسلات ذات طبعة إلكترونية معلوماتية، أي تثبيت آلات من طبيعة إلكترونية أو معلوماتية ***"procéder à l'installation d'appareils"*** لتحقيق إحدى الجرائم المذكورة سالفا، و التي يمكن ربطها بالنظام المعلوماتي أو بجهاز الكمبيوتر المتصل بشبكة الأنترنت، غير أنه من جهة أخرى كان لا بد على المشرع الفرنسي أن ينص على وسيلة أخرى لتحقيق نفس هذه الجرائم و هو تثبيت في النظام المعلوماتي أو جهاز الكمبيوتر برامج مقرصنة ***"Procéder à l'installation de programmes pirates"*** أو من طبيعتها تحقيق الأفعال المجرمة المنصوص عليها في الفقرة الثانية و عبر شبكة الأنترنت.

بالإضافة إلى المادة 226-15 ق.ع.فرنسي السالفة الذكر، نجد المادة 432-9 ق.ع.فرنسي، جاء نصها كما يلي :

المادة 432-9 ق.ع.فرنسي : "في حالة ما إذا كان شخص مراقب لدى السلطة العمومية أو مكلف بمهمة متعلقة بخدمة عمومية، يتصرف عند ممارسة أو بمناسبة ممارسة وظائفه أو مهمته، بتوجيه أمر، بإرتكاب أو تسهيل، خارج الحالات المنصوص عليها قانونا، تحريف، حذف، أو فتح المراسلات أو إفشاء محتوى هذه المراسلات، معاقب عليه بثلاثة سنوات (3) حبس و 45000 € غرامة.

تطبق نفس العقوبات في حالة ما إذا كان شخص منصوص عليه في الفقرة السابقة أو عون عند مستغل لشبكات إتصال الإلكتروني مفتوحة للجمهور أو لموزع خدمات الإعلام و الإتصال عن بعد، يتصرف عند ممارسة مهامه، بتوجيه أمر، بإرتكاب أو تسهيل، خارج الحالات المنصوص عليها قانونا، توقيف أو تحريف مراسلات صادرة، مرسلة أو متحصل عليها بواسطة وسائل الإعلام الحديثة، و كذا إستعمال أو إفشاء محتواها"[1].

هذه المادة جاءت بنفس التجريمة المنصوص عليها في المادة 226-15 ق.ع.فرنسي، لاسيما الفعل الإجرامي الماس بسرية المراسلات التقليدية وفقا للفقرة الأولى من المادة 432-9 ق.ع.فرنسي و كذا الفعل الإجرامي الماس بالمراسلات الإلكترونية و التي يتم نقلها عبر الشبكات المعلوماتية المفتوحة [2] ***"Réseaux ouverts au***

---

[1]_ أنظر نص المادة باللغة الفرنسية :

Art 432-9 c.p.f : « Le fait, par une personne dépositaire de l'autorité publique ou chargée d'une mission de service public, agissant dans l'exercice ou à l'occasion de l'exercice de ses fonction sa mission, d'ordonner, de commettre ou de faciliter, hors les cas prévus par la loi, le détournement, la suppression ou l'ouverture de correspondances ou la révélation du contenu de ces correspondances, est puni de trois ans d'emprisonnement et de 45000 euros d'amende.
Est puni des mêmes peines le fait, par une personne visée à l'alinéa précédent ou un agent d'un exploitant de réseau ouverts au public de communication électroniques ou d'un fournisseur de services de télécommunications, agissant dans l'exercice de ses fonctions, d'ordonner, de commettre ou de faciliter, hors les cas prévus par la loi, l'interception ou le détournement des correspondances émises, transmises ou reçues par la voie des télécommunications, l'utilisation ou la divulgation de leur contenu ».

[2]_ الشبكات المعلوماتية كما ذكرناه في المقدمة العامة عدة أنواع، وحتى تقوم الجريمة لم يشترط المشرع الفرنسي أن ترتكب هذه الأخيرة عبر نوع معين من الشبكات المعلوماتية أو الإلكترونية، بل يكفي أن تسمح هذه الشبكة مهما كان نوعها بإرتكاب إحدى الجرائم ضد سرية المراسلات الإلكترونية المنصوص عليها في المواد 226-15 فقرة 2 و 432-9 فقرة 2 ق.ع.فرنسي.

"public de communication électronique" (شبكة الأنترنت) المنصوص عليها في الفقرة الثانية من نفس المادة، لكن تكمن التفرقة بين المادتين في صفة مرتكب الجريمة إذ أن المادة 226-15 ق.ع.فرنسي جاءت بعقوبة أخف إذا إرتكبت الجريمة المعلوماتية من طرف شخص طبيعي عادي أي سنة حبس و غرامة أما بالرجوع إلى المادة 432-9 ق.ع.فرنسي فنجدها جاءت بعقوبة حبس أشد أي ثلاثة سنوات حبس و هذا إذا إرتكبت الجريمة من طرف عون أو شخص تابع للسلطة العمومية أو مكلف بمهام في إطار خدمة عمومية، و بالأخص الأعوان الذين يعملون لحساب مستغلي الشبكات المفتوحة أو شبكة الأنترنت أو لحساب موزعي الخدمات المعلوماتية أو الإعلامية أو أيضا موزعي حق الدخول إلى شبكة الأنترنت *"Les fournisseur d'accès au réseau Internet"*، و في هذه الحالة الفعل المجرم هو توجيه المسؤول أمر إلى أعوان أو أشخاص آخرين أو أن يسهل للغير أو أن يرتكب بنفسه و أثناء ممارسته لمهامه لفعل توقيف أو تحريف مراسلات ذات طابع إلكتروني معلوماتي من أمثلتها : *"L'e-Mail"* متحصل عليها في أغلب الأحيان بواسطة وسائل الإعلام الحديثة كأجهزة الكمبيوتر متصلة بشبكة الأنترنت، إلا أن هذا لا يمنع إمكانية إرتكاب الجريمة المعلوماتية بأي وسيلة أخرى في أغلب الأحيان ذات طابع إلكتروني كالهاتف النقال *"Le téléphone mobile"* مزود بحق الدخول في شبكة الأنترنت مثلا، بالإضافة إلى الإستعمال الغير مشروع لهذه المراسلات الإلكترونية أو إفشاء محتواها إلى الغير سواء من الطرف العون المسؤول نفسه، أو بموجب أمر موجه إلى عون أو أي شخص آخر.

أما في ما يخص التشريع العقابي الجزائري في هذا المجال فلقد ورد في نص المادة 333 ق.ع.جزائري التي جاءت على خلاف التشريع العقابي الفرنسي عامة و لم تتطرق إلا للجانب التقليدي للجرائم الرامية لإفضاء أو إفشاء، إتلاف رسائل أو مراسلات موجهة إلى الغير و ذلك بسوء نية بالإضافة إلى المادة 137 ق.ع.جزائري المتعلقة بالجرائم المرتكبة من طرف موظف الدولة أو مندوب عن مصلحة للبريد و الرامية إلى إفضاء، إختلاس أو إتلاف رسائل مسلمة إلى البريد أو يسهل ذلك، و بالتالي سواء بالنظر إلى المادة 333 أو 137 فإننا يمكن أن نلاحظ بأن المشرع الجزائري لم يجرم صراحة التصرفات المذكورة سابقا و هذا بالنسبة للبريد الإلكتروني و كذا الجرائم المرتكبة من طرف موظفين يعملون لحساب مستغلي الشبكات المفتوحة أو شبكة الأنترنت[1] أو لحساب موزعي الخدمات المعلوماتية أو الإعلامية أو أيضا موزعي حق الدخول إلى شبكة الأنترنت *"Les fournisseur d'accès au réseau Internet"* خلافا عن مصالح البريد التقليدية، غير أنه من جهة أخرى و أمام عمومية المشرع في هذا المجال، يمكن أن نؤكد إمكانية تمديد تطبيق هذه المواد العقابية بخصوص التصرفات الرامية إلى المساس بالمراسلات الإلكترونية و عبر الشبكات المعلوماتية بموجب الممارسة و الإجتهادات قضائية، إذ أن المراسلة سواء تمت بطريقة تقليدية أو بواسطة المعلوماتية إلا أنها تبقى

---

[1] _ من أمثلة المؤسسات التي تستغل شبكة الأنترنت لتقديم خدمات معلوماتية لمستعمليها ومن بينها إستعمال البريد الإلكتروني أو البحث عبر الشبكة المفتوحة : ***www.yahoo.fr, www.google.fr ou aussi www.msn.fr***.

مراسلة ذات طابع خاص و بالتالي المساس بسريتها يعد خرق لحرمة الحياة الشخصية للأفراد و بصفة عامة مساس بالحريات الفردية.

المبحث الرابع :
جرائم المعلوماتية الماسة بالقاصر عبر شبكة الأنترنت

حرية التعبير عبر شبكة الأنترنت يجب أن لا تمس بالنظام العام كما رأيناه في بداية هذا الفصل، و بهذا المعنى حماية القصر تقع في مقدمة إنشغالات مختلف الدول[1]، بإعتبار أن شبكة الأنترنت لها جوانب ضارة كون أنها قد تتيح الفرصة للقصر الدخول إلى محتويات جنسية لا أخلاقية التي بإمكانها التأثير سلبيا على تصرفاتهم و أخلاقياتهم، أو أن تعطي الفرصة لمجرمين الجنسيين ***"Les délinquants sexuels"*** الإتصال بهم.

إذا حماية الطفل القاصر عبر شبكة الأنترنت، هو أولا و قبل كل شيء مقاومة المحتويات الغير أخلاقية و الماسة بالآداب العامة بمعنى مواقع الأنترنت المتضمنة لصفحات، و كذا مجالات المناقشة ***"Forums de discussion"*** مفتوحة لجمهور الأنترنت ***"Les internautes"*** أو أيضا بواسطة برامج خاصة للمناقشة [2] عبر الشبكة بواسطة الصورة ***"Par l'image"*** و الكتابة ***"Par écris (Chat)"*** و الكلام ***"Par la parole"*** و بطريقة مجانية في أغلب الأحيان[3].

من جهة أخرى تكمن الصعوبة بالنسبة لشبكة الأنترنت في كونها ذات طابع عالمي و هذا بفضل التسهيلات التقنية للدخول في الشبكة و كذا سهولة الإتصال بواسطتها، إذا من الصعب التصدي لجل المحتويات اللا أخلاقية في الشبكة بمختلف أنواعها و بما فيها تلك المتعلقة بالقصر ***"Sites et page Web en relation avec les actes pédophiles"*** نظرا لعددها الهائل و المتزايد، المستهدف لنوع معين من جمهور الأنترنت و بما فيهم القصر، بالإضافة إلى الصعوبة المتعلقة بالقانون الواجب التطبيق و الجهة القضائية المختصة بمحاكمة مجرمي الأنترنت ضد القصر بإعتبار أن الموقع الجغرافي لكل من مرتكب الجريمة بالإضافة إلى الضحية و كذا المحتويات المجرمة و بالأخص الموزع المعلوماتي ***"Le serveur informatique"*** الذي يسمح بنشر و بث مثل هذه المحتويات المجرمة عبر شبكة الأنترنت قد يختلف في أغلب الأحيان، كما أنه يمكن إثارة المسؤولية الجزائية لموزعي حق الدخول إلى شبكة الأنترنت ***"Les fournisseurs d'accès au réseau Internet"*** المثبتين لصفحات و مواقع الأنترنت ***"Hébergeurs de sites et page Web"***، لمثل هذه المحتويات بصفتهم شركاء في الجريمة الأصلية.

---

(1)_ أنظر : Eric TAVENARD, mémoire de (DESS) droit du multimédia et de l'informatique, ***La pornographie sur Internet***, sous la direction du : professeur Jérôme HUET, université Paris II – Panthéon Assas (France), année 2002-2003, page 33.

(2)_ من بين أمثلة برامج المناقشة عبر شبكة الأنترنت ***"Les logiciels de discussion ou la messagerie instantanée"*** : ***"Skype, Windows Live Messenger"***.

(3)_ أنظر : Etienne WERY, ***« Sexe en ligne : aspects juridiques et protection des mineurs »***, édition LARCIER (Droit des technologies) 2004, page 49.

و تجدر الإشارة من جهة أخرى على أنه رغم توافر العديد من الوسائل التقنية المعلوماتية أي البرامج المعلوماتية التي يمكن لأولياء القصر التحكم فيها بهدف التصفية و التصدي لمثل هذه المحتويات الغير مشروعة إلا أن هذه الوسائل التقنية غير كافية لضمان الحماية الكاملة للقاصر عندما يتجول في فضاء الأنترنت، و بالتالي كان لا بد على المشرع وضع تدعيم لهذه الحماية التقنية بوضع نصوص عقابية محكمة.

لدى سندرس هذا الموضوع من خلال 4 نقاط رئيسية التالية :

سندرس جريمة تحريض القاصر على الفسق و الدعارة عبر شبكة الأنترنت ***"Excitation du mineur à la débauche et la prostitution à travers le réseau Internet"*** (المطلب الأول)، سندرس بعد ذلك جريمة نشر رسائل إلكترونية ذات طبيعة جنسية لا أخلاقية و التي من المحتمل أن يطلع عليها القاصر عبر شبكة الأنترنت ***"L'infraction de diffusion de messages a caractères pornographiques susceptibles d'être vues ou aperçus par un mineur via le réseau Internet"*** (المطلب الثاني)، و أخير سنختتم هذا المبحث بدراسة الجرائم المعلوماتية التي لها علاقة بالمعطيات المعلوماتية المخلة بالحياء و المتعلقة بقاصر ***"L'infraction informatique liée aux fichiers ou données de natures pédophiles en relation avec un mineur"*** و هذا من خلال التصرفات الجرمية التي يمكن أن تتم بواسطة هذا النوع من المعطيات في التشريع العقابي الجزائري و المقارن (المطلب الثالث).

المطلب الأول : جريمة تحريض قاصر على الفسق و الدعارة عبر شبكة الأنترنت

في ما يخص هذا النوع من الجرائم فالمشرع الجزائري خصص لها في قانون العقوبات القسم السابع تحت عنوان : "تحريض القصر على الفسق و الدعارة" أي المواد من 342 ق.ع.جزائري إلى 349 ق.ع.جزائري المعدلة بموجب المادة 60 من القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006، أما المشرع الفرنسي فلقد نص عليها في قانون العقوبات في القسم الثاني مكرر تحت عنوان : "عن اللجوء إلى الدعارة إزاء القصر أو الأشخاص الضعيفة خصوصا " ***Section 2 bis : « Du recours à la prostitution de mineurs ou de personnes particulièrement vulnérables »*** أي المواد من 225-12-1 ق.ع.فرنسي إلى 225-12-4 ق.ع.فرنسي و تجدر الإشارة إلى أن آخر تعديل لهذا القسم كان بموجب القانون رقم 2003-239 المؤرخ في 18 مارس 2003، الجريدة الرسمية الصادرة بتاريخ 19 مارس 2003، غير أنه بعد التطلع على هذه المواد يمكن أن نلاحظ بأن المشرع الجزائري على خلاف زميله الفرنسي، لم يولي إهتماما إلى حالة إرتكاب الجريمة بإستعمال شبكة إتصال، في حين أن المشرع الفرنسي في نصوصه العقابية و على خلاف القاعدة العامة بالنسبة لهذه الجرائم الواردة في نص المادة 225-12-1 ق.ع.فرنسي ، فإنه خصص بموجب مادة مستقلة حالة تحريض القاصر أو الشخص في حالة ضعف على الفسق و الدعارة بإستعمال أي نوع من أنواع شبكات الإتصال عن بعد و خصوصا المستحدثة و بما فيها الشبكات المعلوماتية أو الإلكترونية (السلكية أو اللاسلكية) التي تشدد فيها

العقوبة الأصلية الواردة في المادة 225–12–1 ق.ع.فرنسي[1]، و بالتالي بالرجوع إلى المادة 225–12–2 ق.ع.فرنسي في ما يخص الحالة الثانية من حالات تشديد العقوبة أي حالة الشخص أي بمفهوم القانون الفرنسي القاصر دون الخامسة عشر من عمره أو الشخص الضعيف [2] الذي إتصال به المجرم بعد أن قام مسبقا بنشر رسائل أو بريد إلى جمهور غير محدد و ذلك بإستعمال شبكة إتصال، ففي هذه الحالة العقوبة المقررة هي 5 سنوات حبس و 75000 €.

حيث جاء نص المادة 225–12–2 ق.ع.فرنسي كما يلي :

المادة 225–12–2 ق.ع.فرنسي : "العقوبات ترفع إلى 5 سنوات حبس و 75000 € غرامة :

...

2– عندما يكون الشخص قد وضع في إتصال مع المسؤول عن الوقائع بفضل إستعماله لشبكة إتصال، لنشر رسائل إلى جمهور غير محدد ..."[3].

و بالتالي الخصوصية التي جاءت بها هذه الحالة هو إستعمال شبكة إتصال و التي من شأنها تسهيل عملية الإتصال عن بعد بين القاصر أو الشخص في حالة ضعف و المجرم، و بالتالي مجرد إستعمال أي نوع من أنواع شبكات الإتصال عن بعد بما فيها المستحدثة (الشبكات المعلوماتية أو السلكية و اللاسلكية مثلا) لتسهيل عملية الدخول مع المجني عليه بهدف تحريضه على الفسق أو الدعارة، في هذه الحالة و بعد إتيان دليل قيام الجريمة (أي الدليل الإلكتروني) بواسطة شبكة الأنترنت مثلا، في هذه الحالة تشدد العقوبة.

في ما يخص كيفية تحقيق هذا النوع من الجرائم بواسطة شبكة الأنترنت، فالمجرم بواسطة تقنية المعلوماتية يجب أن يقوم أولا بإجراء بمراسلة عشوائية إزاء جمهور غير محدد و بالأخص القصر بهدف تسهيل عملية الإتصال عن بعد معهم، و يجب فهم بأن المراسلة قد تأخذ عدة صور (بريد إلكتروني ***"e-Mail"***، أو بواسطة الإعلانات في صفحات الأنترنت ***"Les annonces sur les sites Web"*** أو عن طريق مجالات المناقشة ***"Forums de discussion"*** أو برامج الإتصال التلقائي الكتابية السمعية البصرية ***"Messagerie instantanée"*** مثلا و هذا في ما

---

(1)_ أنظر : Etienne WERY, ***Op.cit***, de la page 63 à 64.

(2)_ الشخص الضعيف بمفهوم المادة 225–12–1 فقرة 2 ق.ع.فرنسي : هو كل شخص يبين ضعف أو عجز ظاهر كان يعلم به مرتكب الجريمة و يستغلها، و هذا الضعف أو العجز قد يكون راجع لمرض و عجز، خلل أو نقص جسدي أو نفسي أو في حالة حمل.

« ... lorsque cette personne présente une particulière vulnérable, apparente ou connue de son auteur, due à une maladie, à une déficience physique ou psychique ou à un état de grossesse ».

(3)_ أنظر نص المادة باللغة الفرنسية :

Art 225-12-2 c.p.f : « Les peines sont portées à cinq ans d'emprisonnement et 75000 euro d'amende :

...

2° Lorsque la personne a été mise en contact avec l'auteur des faits grâce à l'utilisation, pour la diffusion de messages à destination d'un public non déterminé, d'un réseau de communication ... » .

يخص شبكة الأنترنت، كما قد تتم المراسلة عبر الشبكات اللاسلكية و بما فيها الهواتف النقالة لنشر الرسائل القصيرة ***"Les SMS"*** أو ***"MMS"*** مثلا).

من جهة أخرى بعد الإطلاع على النصوص العقابية الجزائرية و الفرنسية في ما يخص جريمتي تحريض القاصر على الفسق و الدعارة، يمكن أن نلاحظ بأن المشرعين الفرنسي و الجزائري قد إختلفى بشأن المصطلحات المستعملة في هذا المجال حيث عبر المشرع الجزائري عن مصطلح الفسق في النص العقابي باللغة الفرنسية بمصطلح ***"Débauche"*** في حين أن المشرع الفرنسي لم يعبر عنها بهذا المصطلح و إنما بمصطلح ***« ... y compris de façon occasionnelle ... »*** بمعنى ***"La prostitution occasionnelle"*** و هذا بالرجوع إلى نص المادة 225-12-1 فقرة 2 ق.ع.فرنسي.

و تجدر الإشارة إلى أن هنالك إختلاف بين كل من الدعارة ***"Prostitution"*** و الفسق ***"Débauche ou prostitution occasionnelle"*** من حيث المعنى، و بالتالي الفسق و على خلاف الدعارة لا يستوجب الإحتراف و لا البحث عن مقابل مالي[1].

السؤال الذي يمكن طرحه هو لماذا إعتبر المشرع الفرنسي حالة إستعمال إحدى أنواع شبكات الإتصال عن بعد من بين حالات تشديد العقوبة وفقا للمادة 225-12-2 ق.ع.فرنسي ؟

تعد حالة إستعمال شبكات الإتصال عن بعد ظرف مشدد للعقوبة الأصلية الواردة في المادة 225-12-1 ق.ع.فرنسي في نظرنا لثلاثة أسباب، أي أن هذه الوسيلة ستسمح أولا : للمجرم الإتصال عن بعد و بسهولة بأكبر عدد ممكن من القصر أو الأشخاص في حالة ضعف، و ثانيا : و في أغلب الحالات بطريقة سرية و بإستعمال تسمية تخلتف عن الإسم الحقيق للمجرم ***"De façon anonyme et dans la plupart des cas en utilisant un pseudonyme de substitution au vrais nom du délinquant"*** تجعل من الصعب التعرف على هوية المرسل للبريد أو الإعلام الإلكتروني عبر شبكات الإتصال عن بعد، و ثالثا : لسبب التزايد المستمر لعدد جمهور الأنترنت المشتركين في شبكة المفتوحة ***"Les internautes abonnés au réseau Internet"*** مما يسهل مهمة المجرم المعلوماتي في إرتكاب الجريمة.

من جهة أخرى و بالرجوع إلى المادة 225-12-3 ق.ع.فرنسي نجدها تنص على ما يلي :

المادة 225-12-3 ق,ع.فرنسي : "في حالة إرتكاب الجرائم المنصوص عليها في المواد 225-12-1 و 225-12-2 في الخارج من طرف مواطن فرنسي أو من طرف شخص مقيم عادة داخل الإقليم الفرنسي،

---

(1)_ أنظر : أحسن بوسقيعة، "**الوجيز في القانون الجزائي الخاص**" **(الجزء الأول) الجرائم ضد الأشخاص و الجرائم ضد الأموال، مرجـــع ســابـــق**، صفحة 114.

القانون الفرنسي خلافا لما جاء في نص الفقرة الثانية من المادة 113-6 و مقتضيات الجملة الثانية من المادة 113-8 التي لا تطبق في هذه الحالة"[1].

و بالتالي الفرق واضح بين كل من المواد 225-12-1، 225-12-2 و المادة 225-12-3 ق.ع.فرنسي، بإعتبار أن المواد 225-12-1، 225-12-2 تتعلق بجريمة تحرض القاصر على الفسق و الدعارة و لكن في حدود الإقليم الوطني الفرنسي، في حين أن المادة 225-12-3 ق.ع.فرنسي تشمل نفس الجرائم السالفة الذكر و لكن خارج الإقليم الوطني الفرنسي سواء إرتكبت الجريمة بالوسائل التقليدية أو بواسطة إستعمال شبكة إتصال أيا كان نوعها و بما فيها شبكة الأنترنت، حيث تتم الجريمة باللجوء كما ذكرناه سابقا إلى تقنيات الإتصال عن بعد بالقصر و بما فيها البرامج المعلوماتية السمعية البصرية و الكتابية الخاصة بذلك، أو عن طريق العرض على صفحات مواقع الأنترنت السياحة الجنسية ***"Le tourisme sexuel"*** في دول أجنبية جلابة ***"Pays exotiques"*** [2].

و بالتالي و وفقا لما ورد في المادة 225-12-3 ق.ع.فرنسي إذا إرتكبت الجريمة خارج التراب الوطني الفرنسي في هذه الحالة المشرع الفرنسي نص بأن القانون الفرنسي هو الواجب التطبيق، و هذا وفقا للشروط الواردة في المواد 113-6 و 113-8 ق.ع.فرنسي.

إذا ما هي الشروط الواجب توافرها، حتى يسري على الجرائم المرتكبة خارج الإقليم الوطني الفرنسي القانون الفرنسي وفقا للمواد 113-6 و 113-8 ق.ع.فرنسي ؟

المادة 113-6 ق.ع.فرنسي : "القانون الفرنسي يطبق على كل جريمة يرتكبها فرنسي خارج إقليم الجمهورية. يطبق على الجرائم المرتكبة من طرف فرنسيين خارج الجمهورية إذا كانت الوقائع معاقب عليها من طرف تشريع الدولة التي إرتكبت فيها.
تطبق مقتضيات المادة الحال في حينئذ حتى إذا إكتسب المتهم الجنسية الفرنسية ما بعد الوقائع المنسوبة إليه"[3].

---

(1)_ أنظر نص المادة باللغة الفرنسية :
Art 225-12-3 c.p.f : « Dans le cas ou les délits prévus par les articles 225-12-1 et 225-12-2 sont commis à l'étranger par un français ou par une personne résidant habituellement sur le territoire français, la loi française est applicable par dérogation au deuxième alinéa de l'article 113-6 et les dispositions de la seconde phrase de l'article 113-8 ne sont pas applicables ».

(2)_ أنظر : Etienne WERY, ***Op.cit***, de la page 63 à 64.

(3)_ أنظر نص المادة باللغة الفرنسية :
Art 113-6 c.p.f : « La loi pénale française est applicable à tout crime commis par un français hors du territoire de la république.
Elle est applicable aux délits commis par des français hors du territoire de la république si les faits sont punis par la législation du pays ou ils ont été commis.
Il est fait application du présent article lors même que le prévenu aurait acquis la nationalité française postérieurement au fait qui lui est imputé ».

المادة 113–8 ق.ع.فرنسي : "في الحالات المنصوص عليها في المواد 113–6 و 113–7، متابعة الجرائم لا يمكن أن تتم إلا بناءا على طلب من طرف النيابة العامة. يجب أن تسبق بشكوى من طرف الضحية أو ذوي حقوقه أو بناءا على إبلاغ رسمي من طرف سلطات الدولة أين إرتكبت الواقعة"[1].

و بالتالي تتمثل شروط تطبيق قانون العقوبات الفرنسي على الجرائم الواردة في المواد 225–12–1 و 225–12–2 ق.ع.فرنسي في :

– وجوب أن يكون مرتكب الجرائم ذو جنسية فرنسية أو مقيم عادة داخل الإقليم الفرنسي أي متحصل على بطاقة إقامة سارية المفعول ***"Carte de séjour en cour de validité"***.

– أن تكون الوقائع معاقب عليها من طرف تشريع الدولة التي إرتكبت فيه.

– المتابعة القضائية في الحالة الواردة في المادة 225–12–3 ق.ع.فرنسي لا يمكن أن تباشر إلى بناءا على طلب من طرف النيابة العامة التي يجب أن تسبق بشكوى من طرف الضحية أو ذوي حقوقها أو بناءا على إبلاغ رسمي من طرف سلطات الدولة التي إرتكبت فيها الجريمة.

و من الملاحظ أن المشرع الفرنسي زيادة على مقتضيات المادة 225–12–3 ق.ع.فرنسي، فإنه مدد مجال تطبيق قانون العقوبات الوطني إلى كل الجرائم كقاعدة عامة سواء كانت ذو تكييف جنحة أو جناية و معاقب عليها بالحبس سواء إرتكبت هذه الجرائم من طرف مواطن فرنسي أو أجنبي خارج الإقليم الفرنسي عندما تكون ضحية هذه الجريمة ذو جنسية فرنسية وقت وقوعها و هذا وفقا للمادة 113–7 ق.ع.فرنسي.

و من الملاحظ من خلال دراستنا للجريمة الواردة في المواد 225–12–1 و 225–12–2 و بناءا على المواد 113–6، 113–7 و 113–8 ق.ع.فرنسي فالقانون الفرنسي حتى يكون ساري المفعول على الجرائم المرتكبة خارج الإقليم الوطني يكفي أن يكون مرتكبها شخص ذو جنسية فرنسية، أو مقيم في فرنسا كما أنه ساري المفعول حتى لو لم يكن مرتكبها من إحدى الفئتين السالفتين الذكر، بشرط أن تكون الضحية ذو جنسية فرنسية.

المطلب الثاني : جريمة نشر رسائل إلكترونية مخلة بالأخلاق الحميدة عبر شبكة الأنترنت

بالرجوع إلى المادة 227–24 ق.ع.فرنسي نجدها تنص عما يلي :

المادة 227–24 ق.ع.فرنسي : "في حالة إنشاء، نقل، أو نشر بأي وسيلة كانت و مهما كانت الدعامة المحمولة عليها، رسالة ذات طابع عنيف، مخلة بالحياء أو من طبيعتها أو من طبيعتها المساس بصفة خطيرة بشرف

---

[1] _ أنظر نص المادة باللغة الفرنسية :

Art 113-8 c.p.f: « Dans les cas prévus aux articles 113-6 et 113-7, la poursuite des délits ne peut être exercée qu'a la requête du ministère public. Elle doit être précédée d'une plainte de la victime ou de ses ayant droit ou d'une dénonciation officielle par l'autorité du pays ou le fait a été commis.

الإنسان، أو بالمتاجرة بمثل هذه الرسالة، معاقب عليه بثلاث سنوات حبس و 75000 € غرامة إذا ثبت أن هذه الرسالة من المحتمل أن يراها أو يطلع عليها قاصر ..."[1].

بعد التمعن جيدا في مقتضيات المادة 227-24 ق.ع.فرنسي يمكن أن نلاحظ بكل وضوح أنها لا تطرح أي إشكال في ما يخص إمكانية تجريمها لفعل نشر الرسائل اللا أخلاقية المخلة بالأخلاق الحميدة و بما فيها المخلة بالحياء و التي من المحتمل أن يطلع عليها القاصر عبر شبكة الأنترنت [2]، و بالتالي سندرس أولا الخصائص التي تتميز بها هذه الجريمة في محيط معلوماتي عبر شبكة الأنترنت (الفرع الأول)، ثم سنرى بأن مقتضيات المادة 227-24 تطرح إشكالات من حيث التطبيق في محيط الأنترنت (الفرع الثاني).

الفرع الأول : خصائص الجريمة

بالرجوع إلى نص المادة 227-24 ق.ع.فرنسي يمكن أن نستنتج بأن المشرع الفرنسي لم يهتم في تقرير العقوبة لهذا النوع من الجرائم بوجوب توافر شكل أو طبيعة معينة لمحتوى الرسائل الإلكترونية (الفقرة الأولى)، في حين أنه أخذ بعين الإعتبار في تقرير العقوبة مسألة الإطلاع المحتمل على محتواها من طرف قاصر ***"L'accès potentiel par un mineur"*** (الفقرة الثانية).

الفقرة الأولى : عدم إشتراط شكل أو طبيعة معينة للرسائل الإلكترونية المجرمة

المادة 227-24 ق.ع.فرنسي خلفت المادة 283 ق.ع.فرنسي قديم و المتعلقة بـــ : "الإخلال بالأخلاق الحميدة ***"Outrage aux bonnes mœurs"***"، و تجدر الإشارة إلى أن المادة القديمة لم تعالج إلا ما يتعلق بالجنس ***"La sexualité"***، في حين أن المادة الجديدة محل الدراسة تشمل الصور بمختلف أنواعها كما تشمل مجرد التصريحات البسيطة في محيط الأنترنت مثلا، غير أنه المهم هو أن الرسالة يجب أن تكون ذات طابع مخل بالحياء أو ذات طبيعة من شأنها المساس بصفة خطيرة بشرف الإنسان[3].

الإشكال الأول الذي يمكن طرحه في ما يخص هذه الجريمة هو : ما هي الرسائل التي تدخل في حكم الطابع المخل بالحياء و الأخلاق الحميدة ؟ إذ أن تحديد مفهوم "الحياء ***"La décence ou la pudeur"*** أو الأخلاق الحميدة ***"Les bonnes mœurs"*** لها أهمية قصوا وذلك نظرا للغموض الذي يدور حولها و التي تعد في أغلب الأحيان

---

(1)_ أنظر نص المادة باللغة الفرنسية :

Art 227-24 c.p.f : « Le fait de fabriquer, de transporter, de diffuser par quelque moyen que ce soit et quel qu'en soit le support un message à caractère violent ou pornographique ou de nature à porter gravement atteinte à la dignité humaine, soit de faire commerce d'un tel message, est punis de trois ans d'emprisonnement et de 75000 euros d'amende lorsque ce message est susceptible d'être vu ou perçu par un mineur … ».

(2)_ أنظر : Eric TAVENARD, ***Op.cit***, page 35.

(3)_ أنظر : Eric TAVENARD, ***Idem***.

متغيرة بتغير المكان و الزمان، و عموما يمكن الإعتماد على ما قضت به محكمة النقض الفرنسية حيث عرفت ما يتنافى مع الحياء العام بأنه مبدئيا إثارة الشهوة الجنسية و التحريض على السلوك المنحط القبيح و الإنحرافات الجنسية، و تبعا لذلك يعتبر منافيا للحياء أي نوع من المعطيات التي تظهر الرجل و المرأة في وضع لا أخلاقي و كذا صور للرجل أو النساء و هم عراة تماما أو تلك التي تبرز عورتهم و هي عراية، أو تلك المعطيات أو المعلومات التي تقدم أوصافا دقيقة لمختلف أوضاع و كيفية الإتصالات الجنسية، و مع ذلك يجب التمييز بين المعطيات أو المعلومات التي تهدف فقط لإثارة الشهوة و التحريض على السلوكات المنحطة و تلك المعطيات أو المعلومات ذات طابع علمي بحث أو طبي بهدف التعليم و التكوين في ميدان الطب [1]، و تجدر الإشارة إلى أن الصور أو الأفلام التي تبرز الرجل أو المرأة مع قاصر وفقا للحالات السالفة الذكر فهي تدخل أيضا في حكم ما يتنافى مع الحياء و الأخلاق الحميدة وفقا للمادة 227-24 ق.ع.فرنسي.

في ما يخص التشريع الجزائري في هذا المجال فلقد ورد في نص المادة 333 مكرر ق.ع.جزائري، و بالتالي يتمثل محل الجريمة في كل مطبوع أو محرر أو رسم أو إعلان أو صور أو لوحات زيتية أو أي شيء مناف للحياء، و تجدر الإشارة إلى أن نفس المادة أوردة عبارة "... أي شيء ..."، و بالتالي فإنها تسمح التوسيع في التجريم ليمتد إلى أشياء لم يرد ذكرها في النص مثل الأفلام الخليعة ***"Films pornographiques"*** سواء محمولة على دعامة مادية كأشرطة الفيديو ***"Cassettes vidéos"*** أو الأسطوانات ***"Les CD-Rom ou DVD"*** أو محمولة في دعامة رقمية منطقية كالأفلام أو الصور ***Films, vidéos ou photos*** أو رسائل إلكترونية (بريد إلكتروني) ***Messages électroniques (e-Mails)*** أو المعطيات صوتية ***Fichiers vocaux ou audio*** في شكل معطيات معلوماتية ***Fichiers ou données informatiques***، مثلا : ****.avi, *.mp4, *.mp3, *.doc*** [2].

و تجدر الإشارة إلى أن المشرع سواء الفرنسي أو الجزائري لم يعتد بما إذا كانت المعطيات المنشورة أو المرسلة عبر الأنترنت صحيحة أم خاطئة [3]، بل الأهمية في قيام الجريمة محل الدراسة تكمن في توافر ركن الإخلال بالحياء و الأخلاق الحميدة وفقا لما هو متعارف عليه في التشريع الجزائري و الشريعة الإسلامية و إن تعريف الحياء و الأخلاق الحميدة كما سلف ذكره يختلف بحسب المكان و الزمان و لا ربما حتى في ما بين التشريع الجزائري و الفرنسي، و هو إذا المبدأ الذي أخذ به مجلس قضاء كان (فرنسا) [4]، حيث تتمثل وقائع

---

[1] _ أنظر : أحسن بوسقيعة، "**الوجيز في القانون الجزائي الخاص**" **(الجزء الأول) الجرائم ضد الأشخاص و الجرائم ضد الأموال ، مرجع سابـــق**، من الصفحة 111 إلى 112.

[2] _ أنظر : أحسن بوسقيعة، **المرجع نفســـه**، الصفحة 111.

[3] _ بمعنى أن المراسلة، قد تكون أفلام أو صور مثلا سواء كان محتواها حقيقي يبين بكل وضوح أفعال مخلة بالحياء بحضور قاصر كما قد يكون خياليا من أي حقيقية أي مجرد تمثيل لوقائع مخلة بالحياء دون أن تكون حقيقية فعلا.

[4] _ ***Arrêt de la cour de Caen section pénale du 8 septembre 1999***

القضية في كون أن شخص قام ببعث رسالة إلكترونية عبر شبكة الأنترنت و في مجال مناقشة ***"Forum de discussion"*** بين مستعملي شبكة الأنترنت ***"Les internautes"***، أين يقول فيها : "بأنه أب 5 بنات، و أنه يبيع صور شخصية لها، كما أنه بحوزته أفلام و يطلب من المشاركين الآخرين في مجال المناقشة أن يبعثوا له صور مماثلة و سيلتزم هو الآخر بتزويدهم بصور أخرى "، غير أنه بعد التحريات الأولية تبين بأن المتهم ليست بحيازته أي صورة أو معطيات من هذا النوع، لكن هذا لم يمنع مجلس قضاء كان **(الغرفة الجزائية)** بإدانته طبقا للمادة 227-4 ق.ع.فرنسي[1].

و تجدر الإشارة إلى أن المشرع سواء الجزائري أو الفرنسي في ما يخص هذا النوع من الجرائم إشترط توافر ركن العلنية حتى تتم المتابعة الجزائية[2].

الفقرة الثانية : إحتمال إطلاع القاصر على الرسائل الإلكترونية المجرمة كاف لقيام الجريمة

المادة 227-24 ق.ع.فرنسي تنص بأن الرسالة يجب أن تكون "من المحتمل الإطلاع عليها من طرف قاصر" ***« Susceptible d'être vu ou perçu par un mineur »*** و بالتالي الجريمة الواردة في هذه المادة عبارة عن جريمة شكلية ***"Délit matériel"*** حيث لا يشترط لقيامها أن يكون القاصر قد شاهد أو إطلع فعلا على الرسالة الإلكترونية أو المعطيات محل التجريم الحالي، و بالتالي يكفي تبيان بأنه كان من الممكن على أي قاصر الإطلاع عليها بسهولة حتى تكون الجريمة قائمة و هو ما يعطي لهذه المادة قوة أكبر في ما يخص قمع مثل هذه التصرفات[3].

على العموم المادة 227-24 ق.ع.فرنسي تم صياغتها من طرف المشرع الفرنسي بطريقة غامضة إذ أن التساؤل الذي يمكن أن يطرح بعد قراءة النص هو : متى يمكن إعتبار الرسائل الإلكترونية من المحتمل أن يطلع عليها القاصر ؟[4].

و لقد إعتبر العديد من رجال القانون و المحامين بأن هذه المادة غير دستورية، إذ أنهم يؤسسون رأيهم على سببين أساسيين : فمن جهة، مبدأ شرعية العقوبة لا يتلاءم مع الصياغة الغامضة و الغير دقيقة للتجريم، من جهة أخرى النص الجزائي من الناحية العملية يشكل خرق و إعتراض مبالغ فيه لحرية التعبير (المادة 7و 10 من الإتفاقية الأوربية لحقوق الإنسان).

---

(1)_ أنظر : Eric TAVENARD, ***Op.cit***, page 36

(2)_ أنظر : أحسن بوسقيعة، "**الوجيز في القانون الجزائي الخاص**" **(الجزء الأول) الجرائم ضد الأشخاص و الجرائم ضد الأموال ، مرجع سابـــق**، صفحة 112.

(3)_ أنظر : Eric TAVENARD, ***Op.cit***, page 36.

(4)_ أنظر : *Etienne WERY,* ***Op.cit***, page 97.

و بالتالي و رغم هذه المبررات فإن مجلس قضاء باريس لم يمشي في هذا الطرح و إن كان نوعا ما مؤسس و عليه و في قرار صادر في 2 أفريل 2002 قضى مجلس قضاء باريس [1] الغرفة الجزائية بإدانة منشأ موقع الأنترنت اللا أخلاقي المخل بالحياء، و الذي أسس توقيعه للعقوبة على نقطتين قانونيتين أساسيتين[2] :

النقطة الأولـــى : تتمثل في كون أنه لا يمكن إعتبار الجملة "... من المحتمل أن تشاهد أو يطلع عليها من طرف قاصر ..." المنصوص عليها في المادة 227-24 ق.ع.فرنسي مصدر لأي شك بإعتبار أن هذه الحالة يمكن أن تجسد ماديا ***"peut être matériellement établie"***، و بالتالي فإن هذا النص يحدد بدقة العناصر المكونة للجريمة و هذا في ما يتعلق بالتصرفات المادية المتمثلة في صنع، نقل أو نشر رسالة إلكترونية مجرمة، و هو ما يتوافق مع مبدأ مشروعية العقوبات المنصوص عليها في المادة 8 من الإتفاقية الأوروبية لحقوق الإنسان و كذا المادة 111-3 ق.ع.فرنسي[3].

النقطة الثانيـــة : في ما يخص مسألة حرية التعبير فالمجلس إعتبر بأن مسألة الحد من الحرية التي فرضتها المادة 227-24 ق.ع.فرنسي يهدف أساسا إلى حماية القاصر من الناحية الأخلاقية و لضمان إستقراره المعنوي ***"Moral"***، الفكري ***"Mental"*** و الجسدي ***"Physique"*** و بالتالي فإن التجريم و العقوبة في هذا المجال كان ضروري و مبرر في حالة التعسف في ممارسة الحق في التعبير عن الآراء أو الأفكار و ذلك إضرارا بالقاصر[4].

و تجدر الإشارة في هذا المجال بأن محكمة النقض الفرنسية [5]، الغرفة الجزائية صادقت بتاريخ 23 فيفري 2000 من جديد على قرار الإدانة الصادر عن المجلس القضائي إزاء مؤلف لأقراص مضغوطة (أسطوانات) تحتوي على صور مخلة بالحياء، و إعتبرت في هذه القضية بأنه حتى و إن كانت هذه الأقراص محمية بشفرات إلا أنه :

---

(1) _ ***Arrêt de la cour de justice de Paris chambre pénale du 2 avril 2002***

(2) _ أنظر : *Etienne WERY,* ***Op.cit***, de la page 97 à 98.

(3) _ أنظر : *Etienne WERY,* ***Ibid***, page 98.

(4) _ أنظر : *Etienne WERY,* ***Idem***.

(5) _ ***Arrêt de la cour suprême Française chambre pénale du 23 février 2000***

"كان بإمكان أطفال قصر الحصول على الأرقام السرية المناسبة وكذا المفاتيح التي ستسمح الإطلاع عليها، بمجرد تسجيل أنفسهم على الموزع الوارد في الأسطوانات دون أي رقابة من طرف وسيط"[1] [2].

من جهة أخرى تجدر الإشارة إلى أن التجريم المنصوص عليه في المادة 227-24 ق.ع.فرنسي يطبق سواء في ما يخص مسألة البريد الإلكتروني ***"Le courrier électronique « e-Mail »"*** [3] أو مواقع الأنترنت ***"Les sites Web"*** التي تحتوي على معلومات معلوماتية مجرمة بموجب هذه المادة[4].

الفرع الثاني : تطبيق المادة 227-24 ق.ع.فرنسي في مجال الأنترنت

و هنا سنتكلم عن حالات عملية سبق و أن طرحت أمام العدالة الفرنسية في ما يخص إرتكاب الجريمة بواسطة البريد الإلكتروني (الفقرة الأولى)، ثم سنرى حالة إرتكاب نفس الجريمة بواسطة النشر عبر مواقع الأنترنت، بإعتبارها التصرفات الأكثر إنتشار عبر شبكة الأنترنت (الفقرة الثانية).

الفقرة الأولى : تطبيق المادة 227-24 ق.ع.فرنسي على البريد الإلكتروني

في ما يخص إستعمال البريد الإلكتروني كوسيلة لإرتكاب الجرائم المنصوص عليها في المادة 227-24 ق.ع.فرنسي، فلقد سبق لمجلس قضاء أنجار (الغرفة الجزائية) أن فصلت في قضية تخص هذه الحالة و لكن هذه المرة لصالح المتهم، إذ تمثلت وقائع القضية في أن المتهم المتابع قام بإرسال بريد إلكتروني ذو طبيعة لا أخلاقية منافية للحياء إلى حوالي 30 شخص مرسل إليه، و لكن السؤال الذي طرح بشأن هذه الوقائع هو هل وقع هنالك خطأ في عملية توجيه البريد الإلكتروني من الناحية التقنية أم أن أحد المرسلين إليهم تغير عنوان بريده الإلكتروني و بالتالي الرسالة وجهت إلى غيره ؟ لسبب أن أحد المواطنين وجد نفسه في قائمة المرسلين إليهم و بدون أي إذن منه، و الذي تأثر كثيرا من محتوى هذه الرسالة، قام بمراسلة باعث هذه الرسالة دائما عن طريق البريد الإلكتروني بعد تلقيه للرسالة الأولى منه أين بين عدم قبوله لمثل هذه الرسائل و أنه لا يرغب في أن يراسل مرة أخرى منه، و نظرا لعدم إستجابة المرسل لطلبه و تنبيهه و بعد تلقي الضحية لبريد آخر منه، تقدم فيما بعد بشكوى رسمية ضده[5].

---

[1] _ أنظر النص باللغة الفرنسية :

« Des enfants pouvaient obtenir (les mots de passe), ainsi que la clé permettant leur visionnage, simplement en ce présentant comme majeurs (à un serveur télématique), sans aucun contrôle, par l'intermédiaire ».

[2] _ أنظر : Eric TAVENARD, ***Op.cit***, page 36.

[3] _ أنظر : *Etienne WERY,* ***Op. cit***, de la page 101 à 103.

[4] _ أنظر : Eric TAVENARD, ***Op.cit***, page 36.

[5] _ أنظر : *Etienne WERY,* ***Op. cit***, page 101.

كملخص لسير الدعوى العمومية، فإن محكمة الجنح لأونجار ***"Tribunal correctionnel d'Angers"*** برأت المتهم محل المتابعة الجزائية، و عند إستئناف وكيل الجمهورية لحكم أول درجة فإن مجلس قضاء أونجار ***"Cour d'appel d'Angers"*** بدوره أيد الحكم محل الإستئناف و جاء تسببيه لقراره كما يلي[1] :

"البريد الإلكتروني شبيه بالمراسلة السرية الخاصة. و هو محمي بموجب كلمة سر شخصية و سرية التي تدخل من طرف المستعمل عند دخوله إلى شبكة الأنترنت أو إلى بريده الإلكتروني. و بالتالي صاحبها هو الوحيد الذي بإمكانه الدخول إليها و هو المسؤول عن إستعمالها. و بالتالي لا يمكن للقاصر أن يدخل إليها إلا بإرادته أو نتيجة إهماله"[2] [3].

و بالتالي المجلس أكد بأن القاصر من الناحية القانونية غير أهل (منعدم الأهلية) ***"Juridiquement incapable"***، و من هذا المنطلق إذا دخل قاصر في البريد الإلكتروني لشخص آخر فلا يكون ذلك إلا بموجب عقد مبرم بين القاصر و هذا الشخص الآخر تتوافر لديه الأهلية القانونية و الذي سيتحمل في ما بعد المسؤولية المنجرة عما سيفعل القاصر ببرده الإلكتروني، و إما أن يستعمل القاصر البريد الإلكتروني لشخص مؤهل قانونا (بالغ سن الرشد) و بالتالي لا يمكن أن نحمل الغير المسؤولية الجزائية عن تصرفه، أي إرسال بريد إلكتروني لا أخلاقي أو من طبيعته المساس بشرف الإنسان إلى هذا العنوان لسبب بسيط هو أنه لم يتوقع بأن قاصر بإمكانه الدخول إليه و من جهة أخرى البريد الإلكتروني كان موجه في الأصل إلى شخص له أهلية قانونية، و بالتالي و في نظر المجلس فمن الناحية القانونية من جهة القاصر لا يمكنه أن يتعاقد مع الغير و من جهة أخرى الجريمة غير قائمة ما دام أن النية الجرمية ضد القاصر غير متوافرة و بالتالي المجلس القضائي أيد الحكم المستأنف فيه[4].

حيث أن النائب العام سجل طعن بالنقض في قرار مجلس قضاء لأنجار أمام محكمة النقض، و كان ردها في هذه القضية مغاير لما جاء به مجلس قضاء لانجار إذ إعتبرت بأن الرسالة الإلكترونية في حد ذاتها لم تكن تحتوي على الصور المجرمة و إنما كانت هذه الصور في موقع أنترنت آخر يمكن الدخول إليه من خلال الرسالة الإلكترونية محل التجريم و من خلال عنوان موقع الأنترنت المرفق في الرسالة، و بالتالي في هذه الحالة إعتبرت محكمة النقض الفرنسية بأن الجريمة غير قائمة، إذا المسؤولية الجزائية لا تعود أساسا في

---

(1)_ أنظر : *Etienne WERY, **Op.cit**, page 102.*

(2)_ أنظر النص باللغة الفرنسية :

« Le courrier électronique est assimilable à une correspondance privé. Il est protégé par un mot de passe personnel et confidentiel qui est composé par l'usager au moment de sa connexion à Internet ou à sa boite aux lettre électronique. Son titulaire est le seul à y avoir accès et il est responsable de son utilisation. Ce n'est que par sa volonté ou sa négligence qu'un mineur peut la consulter ».

(3)_ أنظر : *Etienne WERY, **Op.cit**, page 102.*

(4)_ أنظر : *Etienne WERY, **Idem**.*

قضية الحال إلى مرسل الرسالة الإلكترونية محل التجريم مما يطرح تسائل حول إمكانية تمديد المسؤولية الجزائية إلى موزعي حق الدخول إلى شبكة الأنترنت[1].

الفقرة الثانية : تطبيق المادة 227-24 ق.ع.فرنسي على مواقع الأنترنت

المبدأ في ما يخص تطبيق المادة 227-24 ق.ع.فرنسي في مجال مواقع الأنترنت لا يطرح إشكال ما دام أن فعل : النشر ***"Diffusion"***، إنشاء ***"Fabrication"*** أو نقل ***"Transport"*** الرسائل الإلكترونية ***"Messages électroniques"*** محل التجريم متوافر، و مهما كان نوع الدعامة التي تحملها ***« Quel qu'en soit le support »***، و تجدر الإشارة في هذه النقطة إلى أن مجال الأنترنت يعد من أحسن الدعامات الحاملة لمثل هذه الرسائل كدعامة رقمية خيالية ***"Support numérique virtuel"***، و جانب من الفقه متعجب إلى حد الآن لسبب عدم أخذ التشريع العقابي بعين الإعتبار حالة إستعمال هذه الدعامة كظرف مشدد للعقوبة نظرا للتزايد المستمر لمواقع الأنترنت اللا أخلاقية و المخلة بالحياء أو الماسة بشرف الإنسان[2].

غير أن الأمر ليس سهلا إذ أن تطبيق المادة السالفة الذكر على مجال الأنترنت يطرح إشكال في ما يخص مدى إمكانية أو عدم إمكانية من الناحية التقنية لقاصر أن يدخل في مواقع الأنترنت اللا أخلاقية، غير أن قانون العقوبات الفرنسي و بطريقة غير مباشرة ألزم المسؤولين عن مواقع الأنترنت أن يضعوا مكنزمات مهما كانت طبيعتها و إن كانت في أغلب الأحيان تقنية، الهدف منها منع أي قاصر دون سن الرشد الدخول إلى محتوى مواقعهم تحت طائلة العقوبة[3].

و لقد سبق للعدالة أن طبقت المادة 227-24 ق.ع.فرنسي إزاء مسؤولي مواقع أنترنت تتضمن المعطيات المجرمة بمفهوم المادة، و تجدر الإشارة إلى أن آخر قرار صادر في هذا المجال كان بتاريخ 2 أفريل 2002 عن مجلس قضاء باريس[4] التي أصدرت عقوبة غرامة قدرها 30.000 € ضد مسؤول عن مواقع أنترنت لا أخلاقية بحجة أنه لم يستعمل منظومة معلوماتية محكمة ***"Système informatique efficace"*** لمنع أي قاصر من الدخول إلى هذه المواقع[5].

و بالتالي و نظرا لكون أن المجلس لم يحدد بدقة الإحتياطات التي كان على (المتهم) صاحب مواقع الأنترنت، إتخاذها لمنع الدخول إليها من طرف أي قاصر، فإنه إكتفى بتوجيه إنتقاضات في ما يخص الإجراءات التقنية

---

(1)_ أنظر : *Etienne WERY,* ***Op.cit***, page 103.

(2)_ أنظر : Eric TAVENARD, ***Op.cit***, page 37.

(3)_ أنظر : Eric TAVENARD, ***Idem***.

(4)_ ***Arrêt de la cour de Paris chambre pénale du 2 avril 2002***

(5)_ أنظر : Eric TAVENARD, ***Op.cit***, page 37.

لحماية أي قاصر التي وضعت من طرف المتهم، حيث إعتبر المجلس بأن التنبيهات و مكنزمات الحد من الدخول إلى بعض محتويات الموقع التي وضعت من طرف المتهم في صفحات إستقبال مواقع الأنترنت ***"Les pages d'accueil des sites Web"*** لا تشكل وقاية كافية لكون أن هذه الإجراءات التقنية المتخذة لا تتدخل إلا بعد أن تمكن المستعمل الدخول إلى موقع الأنترنت و مشاهدة النصوص الكتابية و صور العرض لموقع الأنترنت ذات طابع لا أخلاقي مخل بالحياء ، و من هذا المنطلق وضح المجلس بأن في مثل هذه الحالة هنالك إلتزام بالإحتياط الذي يقع على عتق مؤلف موقع الأنترنت كقاعدة عامة، هذا الإلتزام بالإحتياط يلزم مؤلف موقع الأنترنت بالإلتزام بتحقيق نتيجة و المتمثلة في ضمان عدم إمكانية دخول القاصر إلى هذه المواقع (تقنيا)، و ليس مجرد بدل عناية[1].

و بالتالي و من خلال ما جاء به مجلس قضاء باريس في ما يخص حالة إرتكاب الجريمة المنصوص عليها في المادة 227-24 ق.ع.فرنسي و بواسطة موقع أنترنت، السؤال الذي يمكن طرحه هنا هو : ما المقصود بالإحتياطات اللازمة التي يجب أن يتخذها المسؤول عن موقع الأنترنت و المشار إليها في القضية السالفة الذكر من طرف مجلس قضاء باريس ؟ و تجدر الإشارة في ما يخص هذه النقطة أنه لا يوجد أي نص معياري ***"Texte normatif"*** سواء وطني فرنسي أو أوروبي يحدد معايير الإحتياط في هذا المجال، و لقد وضحت محكمة النقض الفرنسية في قرارها الصادر في 23 فيفري 2000 [2] بأن الجهات القضائية في الموضوع ***Les juridictions de fond*** هي الوحيدة المختصة في تقييم ما إذا كانت الإجراءات المتخذة تعد كافية لمنع مشاهدة أو الإطلاع على الرسالة أو المحتوى من طرف قاصر[3].

بموجب هذا القرار الفريد من نوعه، فإن مجلس قضاء باريس فرق بين كل من المرسل ***"L'émetteur"*** و المرسل إليه ***"Le receveur"*** و بالتالي حسب رأيها المسؤولية الجزائية في هذه الحالة لا تقع على عتق المرسل إليه في إتخاذ إحتياطاته عندما يتجول في صفحات و مواقع الأنترنت و إنما المسؤولية في هذه الحالة تقع على عتق المرسل الذي لا بد له أن يتخذ كل الإحتياطات اللازمة التي تفرض بقوة القانون حتى لا تكون هذه المواقع مفتوحة إلا لفئة معينة من جمهور الأنترنت (البالغين سن الرشد فما فوق)[4].

و تجدر الإشارة إلى أن قرار 2 أفريل 2002 الصادر عن مجلس قضاء باريس يعد إجتهاد قضائي فريد من نوعه معتمد عليه على المستوى الأوروبي، و ما يثبت ذلك هو الحكم الصادر عن محكمة نويس (ألمانيا)

---

(1)_ أنظر : Eric TAVENARD, ***Op.cit***, page 37.

(2)_ ***Cass. Crim., 23 février 2000, Bull. crim. n° 85***

(3)_ أنظر : Eric TAVENARD, ***Op.cit***, page 37.

(4)_ أنظر : Eric TAVENARD, ***Idem***.

الصادر في 19 أوت 2002[1] و الذي أدان مؤلف لصفحات أنترنت ***"Editeur de pages Web"*** ذات طابع لا أخلاقي مخل بالحياء لسبب عدم فعالية الآليات التقنية الخاصة بالدخول إلى محتويات هذه الصفحات، و تجدر الإشارة إلى أنه في هذه القضية مؤلف صفحات الأنترنت أراد أن يقوم بعملية الإختيار فيما بين مستعملي شبكة الأنترنت الذين يودون الدخول إلى محتوى صفحاته، و من هذا المنطلق و بالإضافة إلى التحذيرات المكتوبة المتعلقة بمحتوى صفحاته و كذا القوانين و التنظيمات الوطنية المعمول بها في هذا المجال، فإن مستعمل شبكة الأنترنت الذي يود الدخول إلى هذه الصفحات كان لابد عليه أن يدخل كتابيا في المجال الخاص بذلك في صفحة أنترنت المتهم رقم بطاقته البنكية أو رقم بطاقة التعريف بإعتبار أن إحدى هذه المعطيات ستمكن المسؤول عن هذه الصفحات التأكد بأن من سن الشخص الذي يود الدخول إلى صفحة الأنترنت[2].

غير أنه و على الرغم من الضمانات التي وفرها المسؤول عن المحتويات إلا أن القاضي الجزائي أول درجة إعتبر بأن الإجراءات الوقائية المتخذة من طرف المتهم لم تكن تسمح حقيقة بأن الشخص مستعمل شبكة الأنترنت فعلا هو بالغ سن الرشد، إذ أنه في نظر القاضي "حتى إذا كان رقم بطاقة التعريف أو البطاقة البنكية يسمح بمعرفة إذا كان الشخص قاصر أو بالغ سن الرشد، إلا أن ليس بإمكان أي منظومة معلوماتية تسمح بالتأكد بأن المعلومات الموفرة في صفحة الأنترنت هي فعلا للشخص الذي يود الدخول إليها، إذ أنه من المحتمل جدا أن يستعمل القاصر رقم بطاقة تعريف أو البطاقة البنكية لأحد أوليائه أو أي شخص آخر بالغ سن الرشد، و بالتالي و نظرا لإنعدام وجود أي ضمان حقيقي للإجراءات الوقائية المعمول بها من طرف المتهم و ما دام هنالك شك فيها فإن القاضي الجزائي أدان منشئ هذه الصفحات محل التجريم[3].

الفرع الثالث : عدم كفاية التشريع العقابي الفرنسي

على الرغم من صرامة مقتضيات المادة 227-24 ق.ع.فرنسي و أمام تضاعف مواقع الأنترنت الغير أخلاقية، إلا أن الجهات القضائية لم تأتي بالكثير من الإجتهادات القضائية في هذا المجال، و هذا كما أن عدد مواقع الأنترنت الفرنسية التي لا تحترم المبدأ الذي جاء به قرار 2 أفريل 2002 لمجلس قضاء باريس، هائل[4].

من جهة أخرى يمكن ملاحظة بأن مقتضيات المادة 227-24 ق.ع.فرنسي لا تسري إلا في حدود التراب الوطني الفرنسي و بالتالي و بالنسبة لمواقع الأنترنت الأجنبية فهذه المادة غير سارية المفعول مما يجعلنا

---

(1) _ ***Jugement du tribunal de Neuss (Allemagne) section pénale du 19 août 2002***

(2) _ أنظر : Eric TAVENARD, ***Op.cit***, page 38.

(3) _ أنظر : Eric TAVENARD, ***Idem***.

(4) _ أنظر : Eric TAVENARD, ***Idem***.

نستنتج بأن الطابع العالمي لشبكة الأنترنت يعد عائق و صعوبة إضافية للتشريع الفرنسي أو غيره إلى جانب الصعوبات التقنية لإتيان دليل إرتكاب الجريمة[1].

و بالتالي كان لا بد على المشرع الفرنسي إجراء تعديل لنص المادة 227-24 ق.ع.فرنسي و بطريقة تجعله يطبق حتى في ما يخص مواقع الأنترنت الأجنبية و بالإضافة إلى موزعي حق الدخول إلى شبكة الأنترنت إن كان ذلك ممكن[2].

المطلب الثالث : الجريمة المعلوماتية المرتبطة بالمعطيات المخلة بالحياء المتعلقة بالقصر

هذه الجريمة جاء بها قانون فرنسي تحت تسمية قانون ڤيڤـــو « ***Loi Guigou*** » و الذي أدمج في ما بعد في المادة 14 من القانون رقم : 2002-305 المؤرخ في 4 مارس 2002[3]، ليصبح منصوص عليه في المادة 227-23 ق.ع.فرنسي، مما يجعلنا نستنتج بأن هذا النوع من الجرائم التي ترتكب بواسطة المعلوماتية و عبر شبكة الأنترنت و نظرا لحداثتها فلم يتم تنظيمها بنص عقابي إلا في سنة 2002 بالنسبة للتشريع الفرنسي في حين أن قانون العقوبات الجزائري لا يزال لحد الآن يفتقر لهذا النوع من التشريعات و الذي يعد ضروري نظرا لتعميم إستعمال شبكة الأنترنت من طرف نسبة في تزايد مستمر من الجمهور و من بينهم القصر مما يزيد نسبة خطورة شبكة الأنترنت بخصوص الجريمة محل الدراسة، حيث جاء نص **المادة 227-23 ق.ع.فرنسي** كما يلي :

المادة 227-23 ق.ع.فرنسي : "في حالة نشر، تثبيت، تسجيل أو إرسال صورة أو ما يمثل قاصر عندما تكون هذه الصورة أو هذا التمثيل يبين طابع مخل بالحياء، يعاقب بـــ 3 سنوات حبس و 45000 € غرامة. الشروع في الجريمة معاقب عليه بنفس العقوبات.

في حالة إهداء أو نشر مثل هذه الصورة أو التمثيل، بأي وسيلة كانت، تصديرها أو توريدها، القيام بتصديرها أو القيام بتوريدها، معاقب عليه بنفس العقوبات.

حصة العقوبات ترفع إلى 5 سنوات حبس و 75000 € غرامة إذا إستعمل لنشر الصورة أو التمثيل للقاصر إتجاه جمهور غير محدد، شبكة إتصال.

في حالة حيازة مثل هذه الصورة أو التمثيل يعاقب عليها بـــ 2 حبس و 30000 € غرامة.

---

(1)_ أنظر : Eric TAVENARD, ***Op.cit***, page 38.

(2)_ أنظر : Eric TAVENARD, ***Ibid***, page 39.

(3)_ أنظر : *Etienne WERY,* ***Op.cit***, de la page 64 à 65.

الجرائم المنصوص عليها في الفقرة الثانية، الثالثة و الرابعة يعاقب عليها بـــ 10 سنوات حبس و 30000 € غرامة عندما ترتكب من طرف جماعة منظمة.

مقتضيات هذه المادة تطبق أيضا على الصور المخلة بالحياء لشخص إذا تبين بأن المظهر الجسدي أو المرفولوجي هو لقاصر، إلا إذا تم تبيان بأن هذا الشخص كان بالغ 18 سنة في يوم التثبيت أو التسجيل لصورته"[1].

سنركز دراستنا في هذا المطلب على مختلف الجرائم المرتبطة بالمعطيات المعلوماتية المخلة بالحياء و المتعلقة بالقصر، و بالأخص بواسطة وسائل الإتصال الحديثة أي المعلوماتية و الوسائل الإلكترونية الأخرى و بما فيها شبكة الأنترنت، و هذا وفقا للمادة 227-23 ق.ع.فرنسي بإعتبار أن المشرع الجزائري لم يجرم هذه التصرفات في قانون العقوبات إلى حد الآن (الفرع الأول)، ثم سندرس بعد ذلك موضوع مدى إمكانية إثارة المسؤولية الجزائية للوسطاء التقنيين ***"Les intermédiaires techniques"*** في حالة إرتكاب هذه الجرائم (الفرع الثاني)، و أخيرا سنبين بأن الحل الجزائي أو العقابي ليس الوسيلة الوحيدة لحماية القصر في هذا المجال و بالأخص عبر شبكة الأنترنت و بالتالي هنالك وسائل وقائية مسبقة على الحل الجزائي و هي : الرقابة الإدارية للمحتويات عبر الشبكة المفتوحة، بالإضافة إلى رقابة أولياء القصر في ما يخص تصرفاتهم عبر الشبكة (الفرع الثالث).

الفرع الأول : الأفعال المجرمة وفقا للمادة 227-23 ق.ع.فرنسي

من خلال قراءة المادة 227-23 ق.ع.فرنسي التي لا مثيل لها في قانون العقوبات الجزائري الحالي يمكن أن نلاحظ ما يلي :

---

(1)_ أنظر نص المادة باللغة الفرنسية :

Art 227-23 c.p.f : « Le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image ou la représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique et puni de trois ans d'emprisonnement et 45000 euros d'amende. La tentative est punie des mêmes peines.
Le fait d'offrir ou de diffuser une telle image ou représentation, par quelque moyen que ce soit, de l'importer ou de l'exposer, de la faire importer ou de la faire exposer, est puni des mêmes peines.
Les peines sont portées à cinq ans d'emprisonnement et à 75000 euros d'amende lorsqu'il a été utiliser, pour la diffusion de l'image ou de la représentation du mineur à destination d'un public non déterminé, un réseau de télécommunications.
Le fait de détenir une telle image ou représentation est puni de deux ans d'emprisonnement et 30000 euros d'amende.
Les infractions prévues aux deuxième, troisième et quatrième alinéas sont punies de dix ans d'emprisonnement et 500 000 euros d'amende lorsqu'elles sont commises en bande organisée.
Les dispositions du présent article sont également applicables aux images pornographiques d'une personne dont l'aspect physique est celui d'un mineur, sauf s'il est établi que cette personne était âgée de dix-huit ans au jour de la fixation ou de l'enregistrement de son image ».

أولا هو أن الجريمة المعلوماتية المرتبطة بالمعطيات المخلة بالحياء المتعلقة بالقصر [1] تنقسم إلى عدة أنواع من التصرفات الجرمية أي و وفقا للفقرة الأولى من نفس المادة : فعل النشر الذي يضم (فعل تثبيت و تسجيل أو تسليم، إستيراد أو تصدير) و فعل إهداء صورة أو تمثيل فيه قاصر ذات طابع مخل بالحياء.

و تجدر الإشارة إلى أنه إذا إرتكبت هذه التصرفات بطريقة تقليدية هنا تطبق المادة 227-23 فقرة 1 ق.ع.فرنسي، في حين أنه إذا إرتكبت بإستعمال وسائل الإتصال الحديثة (مثلا : شبكة الأنترنت أو أي نوع آخر من الشبكات المعلوماتية أو شبكات الإتصال اللاسلكية)، في هذه الحالة تطبق أحكام الفقرة 3 من نفس المادة و بالتالي العقوبة الجزائية في هذه الحالة تشدد.

و يكمن الركن المعنوي للجريمة من خلال هذه التصرفات الجرمية المنصوص عليها في المادة 227-23 فقرة 1 ق.ع.فرنسي، في القصد الجنائي العام المتمثل في توافر النية الجرمية للإضرار بالقاصر.

و بالتالي هذه التصرفات تتم بطريقة عمدية و مع علم مرتبكها بأنها غير مشروعة، إذا حتى تقوم الجريمة لم يشترط المشرع توافر عند الجاني القصد الجنائي الخاص.

في حين أن الركن المادي للجريمة [2] و كما سبق ذكره في النص العقابي هو قيام المجرم بعملية النشر ***"La diffusion"*** لمعطيات متعلقة بقصر و ذات طابع مخل بالحياء، و تجدر الإشارة إلى أنه لا يهم طبيعة هذه المعطيات (مثلا : صور، أفلام) إذ أنه في كل الأحوال تعد الجريمة قائمة، و يكمن عموما فعل النشر في عرض مثل هذه المعطيات على الجمهور عبر شبكة الأنترنت أو بأي وسيلة إلكترونية أو معلوماتية أخرى بإعتبار أن المشرع الفرنسي لم يحدد كيفية النشر و بالتالي سواء كان النشر بطريقة معلوماتية عبر وسائل الإتصال الحديثة بما فيها شبكة الأنترنت أو غير ذلك (أي الطرق التقليدية الأخرى) فالجريمة تعد قائمة، و يضم فعل النشر حسب مفهوم الفقرة الأولى من المادة 227-23 كلا من التصرفات التالية :

في ما يخص فعل التثبيت ***"La fixation"***، فيكمن في إدخال المعطيات المتعلقة بالقصر و ذات طابع مخل بالحياء (مهما كانت طبيعتها) في شبكة الأنترنت في مواقع الأنترنت و بالأخص في صفحات الأنترنت المحتواة في هذه المواقع و بطريقة تجعلها في متناول أكبر عدد ممكن من الجمهور أو بكل بساطة عرض هذه المعطيات للإستنساخ عبر شبكة الأنترنت من طرف جمهور الأنترنت ***"Les internautes"*** مما يضفي عليه طابع العلنية،

---

[1] _ المشرع الفرنسي في نص المادة 227-23 ق.ع.فرنسي، حدد محل الجرائم التي تدخل ضمنها بأنها كل صورة أو تمثيل لقاصر ذات طابع مخل بالحياء ***Image ou une représentation d'un mineur a caractère pornographique***.

[2] _ في ما يخص الركن المادي للجريمة فسنركز عموما دراستنا في المادة 227-23 ق.ع.فرنسي على الجرائم المنصوص عليها فيها ولكن في مجال معلوماتي أي و حسب مفهوم المادة بإستعمال وسائل إتصال حديثة و على العموم لم يشترط المشرع توافر ركن العلنية حتى تقوم الجريمة و لكنه إعتبر فعل النشر على جمهور غير محدد و بإستعمال وسائل إتصال مستحدثة ظرف مشدد للعقوبة حسب مفهوم الفقرة 3 من نفس المادة.

أي بواسطة برامج الإستنساخ *"Les logiciels de téléchargement"* المعدة لهذا الغرض، و تجدر الإشارة إلى أن فعل التثبيت قد يتم إما على مواقع و صفحات الأنترنت *"Les sites et pages Web"* أو بمجرد وضع هذه المعطيات الغير مشروعة في ذاكرة جهاز الكمبيوتر للمجرم و بالأخص في ملف منقسم *"Dossier partagé"* و الذي سيسمح لجمهور الأنترنت مهما كان نوعه إستنساخها بمجرد دخوله إلى شبكة الأنترنت و ذلك بإستعمال برامج خاصة بالإستنساخ من خواص إلى خواص [1] *"Logiciels de téléchargement peer to peer"* أو أيضا من خلال موزعات معلوماتية عامة أو خاصة *"Serveurs informatiques public ou privé"*، هذا لا يعني بالضرورة بأن الجريمة لا يمكن أن تتشكل إلا إذا إرتكبت عبر شبكة الأنترنت إذ أن المادة السالفة الذكر تطبق على كل أنواع شبكات الإتصال الحديثة، مثلا : شبكة الويفي *"Wifi"*، بلوتوث *"Bluetooth"* إيثرنت *"Ethernet"* أو أيضا أنترانت *"Intranet"*.

و تجدر الإشارة إلى أن النص العقابي الفرنسي لم يحصر فعل التثبيت في شبكة الأنترنت أو أي شبكة معلوماتية من نوع آخر فقط، و بالتالي قد يتم هذا التصرف بأي وسيلة أخرى و مثال ذلك أيضا : تثبيت أفلام أو صور عبر القناة التلفزية *"Les chaînes télévisés"* التي تبث بطرق سلكية أو لا سلكية (هرتزية *"Hertzienne"* أو رقمية *"Numérique"* من خلال الأقمار اللإصطناعية *"Par satellite"*) مثلا.

في ما يخص فعل التسجيل *"L'enregistrement"*، فيتمثل هذا التصرف في تسجيل صور أو أفلام أو غير ذلك من المعطيات المرئية السمعية أو الكتابية بواسطة وسائل تسجيل تقنية حديثة (مثلا : آلة تصوير أي كاميرا رقمية *"Camera numérique"* أي بذاكرة رقمية *"Avec mémoire numérique"*) أو بواسطة وسائل تسجيل تقليدية (مثلا : آلة تصوير أي كاميرا قياسية *"Caméra analogique"*)، إذ أن المشرع الفرنسي من خلال نصه العقابي لم يشترط أن يتم فعل التسجيل للمعطيات الغير مشروعة بواسطة نوع معين من الآلات، و بالتالي قد تسجل هذه المعطيات من قبل المجرم سواء بوسائل تقليدية أو حديثة *"Des moyens traditionnels ou modernes"*، كما أن فعل التسجيل يتعلق بكل بساطة بحفظ هذه المعطيات مهما كان نوعها و المجرمة طبقا للقانون سواء على دعامة مادية أو معنوية كما سلف شرحه.

في ما يخص فعل التسليم *"La transmission"* فيتمثل في تقديم لشخص أو عدة أشخاص المعطيات المجرمة و بالتالي فعل التسليم يكون من يد إلى يد بمفهومه التقليدي حيث تكون المعطيات المجرمة محمولة على دعامة مادية أيا كان نوعها، كما قد يكون التسليم للمعطيات غير محمولة على دعامة مادية أي في مجال معلوماتي أو

---

[1] _ بمعنى أن الإستنساخ في هذه الحالة يتم إلا بين الخواص الذين يتبادلون المعطيات مجانيا فيما بينهم، و تجدر الإشارة إلى أن ركن العلنية متوافر لكون أن كل مستعمل لشبكة الأنترنت لديه برنامج معلوماتي خاص بالإستنساخ من خواص إلى خواص أي بهدف تبادل المعطيات عبر شبكة الأنترنت، فإنه بإمكانه التحصل على مثل هذه المعطيات المجرمة و في أي شكل كانت.

إلكتروني، إذا في هذه الحالة الأخيرة التسليم سيتم بواسطة وسائل إتصال حديثة بما فيها شبكة الأنترنت (مثلا : عبر البريد الإلكتروني ***"e-Mail"***).

و تجدر الإشارة إلى أنه و إن كان ظاهريا فعل النشر ***"La diffusion"*** يتشابه من حيث المفهوم مع فعل التسليم ***"La transmission"***، إلا أن الأمر ليس كذلك إذ أن النشر بطبيعة الحال يهدف إلى تصويب أكبر عدد ممكن من الجمهور سواء عبر شبكة الأنترنت أو بأي وسيلة أخرى في حين أن فعل التسليم يستهدف إما شخص واحد أو عدد محدود من الأشخاص، إلا أن السؤال الذي يمكن طرحه هو : لماذا لم يفرق المشرع الفرنسي بين فعل النشر و التسليم من حيث العقوبة ؟ إذ أنه بالرجوع إلى الفقرة 1 من المادة 227–23 ق.ع.فرنسي يمكن أن نلاحظ بأن العقوبة هي نفسها بالنسبة لكل من التصرفين بإستعمال وسائل الإتصال الحديثة، أي حسب الفقرة 3 من نفس المادة هي : 5 سنوات حبس و 75000 €.

من جهة أخرى بالرجوع إلى الفقرة الثانية من المادة 227–23 ق.ع.فرنسي يمكن أن نلاحظ بأن المشرع الفرنسي جرم أيضا فعل إهداء ***"Offrir"*** المعطيات المستهدفة بالتجريم العقابي و إن كان في الأصل لا يختلف على فعل التسليم ***"La transmission"*** إلا إذا تم ذلك بدون مقابل بالنسبة للحالة الأولى أو بمقابل بالنسبة للحالة الثانية، إلا أن المشرع الفرنسي جرم هذا التصرف بنفس العقوبة المقررة في الفقرة الأولى من نفس المادة، هذا و بالإضافة إلى باقي التصرفات التي سلف ذكرها و شرحها، مع العلم بأن كل هذه التصرفات المرتكبة في محيط معلوماتي أي : فعل التثبيت، النشر، التسجيل، الحفظ، التسليم، أو الإهداء فهي في الأصل تعد تصرفات جرمية تقليدية.

أيضا من بين التصرفات الجرمية المجرمة وفقا للفقرة 2 من نفس المادة : فعل إستيراد و تصدير المعطيات المجرمة وفقا لنفس المادة فقرة 2 و هذا في محيط معلوماتي، ما دام أن المشرع لم يحدد على سبيل الحصر الوسيلة التي من الممكن إستعمالها في الجريمة ***"... par quelque moyen que ce soit ..."***، و بالتالي يتمثل فعل الإستيراد ***"Importer"*** في إستنساخ المعطيات المجرمة بموجب نفس المادة من شبكة الأنترنت أو أي نوع آخر من الشبكات الإلكترونية في حين أن فعل التصدير ***Exporter*** يتمثل في إرسال المعطيات المجرمة بموجب نفس المادة عبر شبكات الإتصال، فإذا كان الأمر واضح في ما يخص التصرفين السابقين و بطريقة تقليدية أي على سبيل المثال : إنتاج جملة من الأسطوانات المتضمنة المعطيات المجرمة إلى الخارج، أو العكس إستيرادها من الخارج سواء لأغراض شخصية أو بهدف ترويجها و عرضها أساسا على الجمهور، في حين أن فعل الإستيراد و التصدير في مجال إلكتروني أو معلوماتي فيتمثل في القيام بتلك التصرفات و لكن عبر الشبكات المعلوماتية و دون أن تكون المعطيات المجرمة محمولة على دعامة مادية.

بالرجوع إلى الفقرة الثالثة من المادة 227-23 ق.ع.فرنسي يمكن أن نلاحظ بكل وضوح بأن المشرع الفرنسي أولى إهتمام كبير في ما يخص الجريمة موضوع هذه المادة و في محيط معلوماتي أو إلكتروني، حيث أنه إعتبر فعل النشر الذي يضم (فعل تثبيت و تسجيل أو تسليم، إستيراد أو تصدير) و ذلك عبر شبكات الإتصال (سلكية أو لا سلكية و بما فيها المعلوماتية) و مع توافر ركن العلنية [1] ظرف مشدد للعقوبة، إذ أن درجة خطورة الجريمة في هذه الحالة أكبر إذ بإمكانها أن تمس أكبر عدد ممكن من الجمهور و بسهولة و سرعة، و هذا على عكس ما إذا تم الفعل بطريقة تقليدية.

يمكن أن نلاحظ أيضا بكل وضوح من خلال الفقرة الرابعة من نفس المادة بأن فعل حفظ ***"Détenir"*** المعطيات المجرمة معاقب عليه وفقا لنفس المادة الفقرة الرابعة بـــ : عامين حبس نافذ و 30000 € غرامة، و قد تتم عملية الحفظ في دعامات مادية ***"Supports matériels"*** (مثلا : أشرطة ممغنطة أو أقراص مضغوطة، أو أقراص مرنة) كما يمكن أن يتم على دعامات منطقية أو معلوماتية ***"Supports virtuels ou numériques"*** (مثلا : عبر شبكة الأنترنت أي في ذاكرة البريد الإلكتروني ***"La mémoire de la boite e-mail"***، صفحة أو موقع أنترنت ***"Page ou site Internet"***)، أي في مجال معلوماتي مستقل عن أي دعامة مادية ***"Environnement informatique indépendant de tous support matériel"***، و بالتالي إذا تم فعل الحفظ سواء في دعامة مادية أو منطقية فالجريمة بمفهوم المادة 227-23 فقرة 4 ق.ع.فرنسي تعد قائمة.

من جهة أخر المشرع الفرنسي شدد العقوبة في حالة إرتكاب الجرائم المنصوص عليها في الفقرة 2 و 3 من المادة 277-23 ق.ع.فرنسي إذا إرتكبت من طرف مجموعة منظمة بناء على إتفاق و التي تتكون على الأقل على شخصين فما فوق و حتى إن تم ذلك بواسطة شبكات الإتصال و بما فيها المعلوماتية لتصبح 10 سنوات حبس و 500000 €.

أخيرا نص المشرع الفرنسي على أن مقتضيات المادة 227-23 فقرة 1، 2، 3، 4 قابلة للتطبيق في حالة الصور، الأفلام أو أي نوع آخر من المعطيات المتعلقة بشخص ذو ملامح قاصر الذي لم يكتمل سن الثامن عشر في تاريخ تثبيت التسجيل لهذه الصور أو المعطيات.

---

[1] _ المشرع الفرنسي لم يشترط صراحة في الفقرتين الأولى و الثانية من المادة 227-23 ق.ع.فرنسي السالفتي الذكر توافر ركن العلنية حتى تقوم الجريمة.

الفرع الثاني : المسؤولية الجزائية للوسطاء التقنيين

نظرا لصعوبة فهم بالتدقيق الدور التقني المنسوب إلى الوسطاء التقنيين في سلسلة المسؤولية التقنية عبر شبكة الأنترنت، فإن المحاكم الفرنسية لم تستقر على رأي واحد بخصوص هذه المسألة حيث جاءت في بعض الأحيان متناقضة في أحكامها و أمام غياب إجتهاد قضائي جامع صادر عن محكمة النقض الفرنسية[1].

حيث أنه و أمام هذا الوضع و الفراغ القانوني السائد قررت اللجنة الأوروبية إدراج في توجيهاته ا المتعلقة بالتجارة الإلكترونية الصادرة بتاريخ 8 جوان 2000[2] في المطلب الرابع ***"Section 4"*** مسؤولية الوسطاء التقنيين ***"La responsabilité des intermédiaire techniques"*** [3]، مثل ما هو الحال بالنسبة لموزعي وسائل البحث عبر شبكة الأنترنت ***"Les fournisseurs d'outils de recherche sur Internet"*** (الفقرة الأولى)، و كذا مسؤولية موزعي حق الدخول إلى شبكة الأنترنت، و موزعي حق تثبيت المحتويات عبر شبكة الأنترنت ***"Les fournisseurs d'accès et d'hébergement"*** (الفقرة الثانية).

الفقرة الأولى : المسؤولية الجزائية لموزعي وسائل و آليات البحث عبر شبكة الأنترنت

في هذا المجال يمكن أن نفرق في ما يخص وسائل البحث عبر شبكة الأنترنت بين : آليات البحث ***"Les moteurs de recherche"*** (أ)، و أدلة مواقع الأنترنت حسب تصنيفها ***"Les annuaires des sites Web selon leurs catégorie"*** (ب).

أ- آليات البحث عبر شبكة الأنترنت

المفهوم من آلية البحث عبر شبكة الأنترنت هو "نظام إستغلال لقاعدة معطيات متصلة بموزع معلوماتي متخصص في تسهيل الدخول عبر شبكة الأنترنت إلى مصادر (صفحات، مواقع أنترنت مثلا) إنطلاق من كلمات مفتاح"[4]، و هذه الآلية تسمى أيضا في ميدان المعلوماتية بـــ : "روبوت" ***« robot »*** الذي تكمن مهمته التقنية في إجراء مسح و فهرسة ***Sonder et indexer*** تلقائيا لصفحات و مواقع الأنترنت التي يمكن العثور عليها

---

(1)_ أنظر : Etienne WERY, ***Op.cit***, de la page 42.

(2)_ ***Directive 2000/31/CE du parlement européen et du conseil du 8 juin 2000***

(3)_ أنظر : Etienne WERY, ***Op.cit***, page 42.

(4)_ أنظر ترجمة النص باللغة الفرنسية :

« Système d'exploitation de banques ou de bases de données, et par extension, un serveur spécialisé permettant d'accéder sur la toile à des ressources (exemple pages, sites) à partir de mots clés »

بواسطة آلية البحث من خلال آثار تتركها على الشبكة و التي ستسمح تلقي معلومات حول محتوى هذه الصفحات أو مواقع الأنترنت في نتائج البحث[1].

و بالتالي المعلومة المتحصل عليها من طرف آلية البحث يمكن أن تكون محل رقابة مزدوجة : الأولى تتدخل على سبيل وقائي بواسطة إستعمال تقنيات معلوماتية آلية لتصفية هذه المعلومات ***"Techniques automatiques de filtrage"*** التي ستقصي مواقع و صفحات الأنترنت التي تحتوي على كلمات مفتاح "لا أخلاقية بشتى أنواعها ***Offensants***"، أما الرقابة الثانية فهي رقابة لاحقة تأتي من خلال تلقي شكاوي من طرف مستعملي شبكة الأنترنت إذ أن هذه الآليات للبحث تسمح في أغلب الأحيان لمستعمليها بتقديم شكواهم إلى مصالحها التقنية و هذا عبر شبكة الأنترنت دائما من خلال نوافذ خاصة بمراسلة مصالحها التقنية المختصة في هذا المجال[2].

غير أنه تجدر الإشارة إلى أن هذه التقنيات سواء الوقائية أو اللاحقة بناءا على شكاوي مستعملي آلية البحث، فإنها ليست بضمان كافي ضد المحتويات الغير مشروعة، لكون أنه في بعض الأحيان قد تكون هنالك مواقع أنترنت تضم محتويات غير مشروعة دون أن تحتوي على أي كلمة مفتاح من بين الكلمات المحتواة في القائمة السوداء لروبوت آلية البحث ***"Le Robot du moteur de recherche"*** الذي يقوم تلقائيا بإقصائها من نتائج البحث، أو في الحالة العكسية قد تكون هنالك مواقع أنترنت مشروعة و مباحة و مع ذلك فإنها تكون محل إقصاء من نتائج البحث لكونها تحتوي إحدى الكلمات الغير مباحة في القائمة السوداء لروبوت آلية البحث[3].

و بالتالي عندما تكون عدم مشروعية الموقع أو صفحة الأنترنت لا شك فيها، مثل ما هو الحال في ما يخص المحتويات المتعلقة بالممارسة الجنسية مع قاصر، في هذه الحالة فإن محتوى موقع أو صفحة الأنترنت يتم حذفه من نتائج البحث بصفة تلقائية و بطريقة تقنية كما سلف تبيانه، غير أن الأمر قد يتعقد في حالة عدم التأكد بدقة ما إذا كان موقع الأنترنت فعلا غير مشروع أم لا إلا بعد إجراء تحقيق معمق في ما يخص مدى مشروعية المحتويات (حقوق المؤلف، المساس بحرمة الحياة الشخصية، أيضا في ما يخص جرائم الإعتبار الأخرى كالقذف و السب مثلا)، إذا في ما يخص الحالات الغامضة فإن المسؤول عن آلية البحث لا يمكنه أن يلعب دور القاضي و بالتالي ليس بإمكانه حذف الموقع أو تعليقه إلا بناءا على طلب السلطات القضائية المختصة[4].

---

(1)_ أنظر : Eric TAVENARD, ***Op.cit***, page 43

(2)_ أنظر : Eric TAVENARD, ***Idem***.

(3)_ أنظر : Eric TAVENARD, ***Idem***.

(4)_ أنظر : Eric TAVENARD, ***Idem***.

في هذه الحالة، يتعين على الأقل حسب رأينا وضع إجراءات خاصة بتبليغ المسؤول على المحتويات التي من المحتمل أن تكون غير مشروعة مع تمكين هذا الأخير من التظلم أمام الجهات التقنية لآلية البحث.

في ما يخص مسؤولية المسؤولين عن آلية البحث في التشريع الفرنسي بخصوص موضوع فهرسة مواقع و صفحات الأنترنت الغير مشروعة فإنها لم تكن محل إجتهادات قضائية إلا بمناسبات نادرة، و في هذا الصدد يمكن ذكر على الأقل سابقة قضائية تعلقت بأمر قضائي إستعجالي صادر عن محكمة المرافعات الكبرى لباريس بتاريخ 31 جويلية 2000 [1]و تتلخص وقائع القضية في أن مؤسستين قامتا بإنشاء موقع أنترنت مخل بالحياء و تحت تسمية و لقب شخص لا علاقة له بهذا الموقع، و عند إكتشاف الضحية لموقع الأنترنت محل النزاع، تقدم بدعوى إستعجالية بهدف توقيف موقع الأنترنت محل النزاع مؤقتا إلى غاية الفصل في الدعوى الجزائية لغلقه و مطالبة الضحية بالتعويض عن الأضرار، و تجدر الإشارة إلى أن دعوى المدعي كانت ضد مثبت الموقع ***"l'hébergeur sur Internet"*** ثم ضد مالك آلية البحث بإعتباره مسؤول عن فهرسة هذا الموقع الغير مشروع في نتائج البحث و بالتالي تكمن مسؤولية المسؤولين عن آلية البحث في كونهم قاموا بالسماح إلى أكبر عدد ممكن من مستعملي الشبكة من خلال الإشهار عبر الأنترنت للإطلاع على محتويات هذا الموقع و الذي تسبب في الإضرار بالضحية التي تحمل نفس إسم هذا الموقع[2].

ب- أدلة مواقع و صفحات الأنترنت

هذه الأدلة عبارة عن قائمة مواقع تعرض عبر شبكة الأنترنت حسب أصنافها، و بالتالي كل موقع حتى تكون له فرصة الورود في هذه الفهارس، لا بد عليه أن يسجل نفسه من خلال إستمارة يبين فيها عنوان الموقع، و عرض موجز لمحتواه و كذا الكلمات المفتاح المتعلقة بهذا الموقع، و بالتالي عملية الفهرسة لا تتم بصفة تلقائية بواسطة روبوت آلية البحث و إنما بتدخل بناء على طلب موجه من طرف مالكي المحتويات إلى المسؤولين التقنيين لآلية البحث و في أغلب الأحيان بطريقة معلوماتية عن طريق نوافذ في صفحة آلية البحث مخصصة لهذا الغرض[3].

و تجدر الإشارة إلى أن نظام المسؤولية هو نفسه بالنسبة لآلية البحث بشرط أن يتحمل صاحب الفهرس عند أول فهرسة مسؤولية نشر المحتويات بمعنى صفحات و مواقع الأنترنت مع علمه بمحتواها و يقوم بترتيبها بحسب صنفها و موضوعها و ذلك بناء على طلب كما سلف تبيانه و في نفس الوقت يجب على الحائز للفهرس أن يكون على علم بمضمون كل المواقع و صفحات الأنترنت و مراقبتها قبل قيامه بفهرستها و في

---

(1) _ ***Ordonnance du tribunal de grandes instances de Paris du 31 juillet 2000***

(2) _ أنظر : Eric TAVENARD, ***Op.cit***, page 44.

(3) _ أنظر : Eric TAVENARD, ***Idem***.

حالة إغفال أو غياب هذه الرقابة فإن ذلك قد يؤدي إلى إثارة المسؤولية الجزائية إذا ثبت و أن هذا التخلف و الإمتناع عن الرقابة قد تم بطريقة عمدية[1].

أما في حالة ما إذا كانت محتويات موقع الأنترنت التي في الأصل عند فهرستها في دليل مواقع و صفحات الأنترنت كانت مشروعة، و في ما بعد قام المسؤول عن الموقع بإجراء تعديلات و إضافات لمحتويات غير مشروعة ففي هذه الحالة يطبق منطقيا نفس الإجراء الذي سبق الكلام عنه بالنسبة لآليات البحث عبر شبكة الأنترنت و بخصوص القضية التي طرحت على محكمة المرافعات الكبرى لباريس بتاريخ 31 جويلية 2000 السالفة الذكر[2].

الفقرة الثانية : موزعي حق الدخول و التثبيت في شبكة الأنترنت

موزعي حق الدخول و التثبيت في شبكة الأنترنت على خلاف آليات البحث و أدلة مواقع و صفحات الأنترنت، لهم نظام خاص يكاد يعفيهم تماما من المسؤولية و لاسيما منها الجزائية غير أن الوضع و إن كان إلى حد الآن جامد في ما يخص إثارة مسؤوليتهم الجزائية إلا أنه لن يدوم ما دام أنه في العديد من الحالات تم طرح هذا الإشكال سواء من طرف رجال الفقه أو المحامين لاسيما الفرنسيين و بموجب تدخل السلطة التشريعية لفرض مسؤولية أكبر مما كانت عليه لهذه الفئة من الوسطاء التقنيين [3]، و من جهة أخرى يتعين التفرقة بين موزعي حق الدخول إلى شبكة الأنترنت ***Les fournisseurs d'accès a Internet*** (أ) و موزعي حق التثبيت في شبكة الأنترنت ***Les fournisseurs d'hébergement*** (ب).

و هنا يتعين تبيان مدى إمكانية إثارة المسؤولية الجزائية بالنسبة للفئتين السالفتي الذكر من الوسطاء التقنيين و كذا تبيان الدور الأساسي الذي يلعبانه عبر شبكة الأنترنت و علاقتهم مع الجرائم المرتكبة ضد القصر في هذا المجال ؟

أ- موزعي حق الدخول إلى شبكة الأنترنت

يعد موزع حق الدخول إلى شبكة الأنترنت جهاز يعرض على زبائنه حق الدخول في الشبكة المفتوحة "أنترنت" أو بصفة عامة إلى أي شبكة إتصال سلكية أو لا سلكية[4].

---

(1)_ أنظر : Eric TAVENARD, ***Op.cit***, de la page 44 a 45.

(2)_ أنظر : Eric TAVENARD, ***Ibid***, page 45.

(3)_ أنظر : Eric TAVENARD, ***Idem***.

(4)_ أنظر : Eric TAVENARD, ***Idem***.

يرى معظم فقهاء القانون بأن المسؤولية الجزائية لموزع حق الدخول إلى شبكة الأنترنت تعد قائمة بصفته شريك في الجريمة الأصلية في ما يخص محتوى مواقع الأنترنت المجرم بإعتبار أن دوره كان تقني بحث أي تسهيل عملية إتصال مستعملي شبكة الأنترنت بالمحتويات المجرمة في شبكة المفتوحة و بالتالي و حسب هذا الرأي يتعين على موزع حق الدخول في شبكة الأنترنت أن يكون على علم بكل المحتويات التي مرت على يد مصالحه و الموجودة في شبكة الأنترنت و العمل على تصفيتها و التصدي لها مسبقا، غير أن الواقع عكس ذلك إذ في حالة عدم علم موزع حق الدخول في شبكة الأنترنت بمحتويات مجرمة تم تسهيل عملية الإطلاع عليها عبر الشبكة المفتوحة مسبقا و أنه لم يتم العمل على التصدي لها تقنيا قبل تحريك الدعوى العمومية ففي هذه الحالة تعد المسؤولية الجزائية لموزع حق الدخول إلى شبكة الأنترنت غير قائمة بإعتبار أنه من غير الممكن الرقابة على الكمية الكبيرة و الهائلة من المعلومات التي تمر من دون إنقطاع على مصالحه التقنية و هو الرأي الراجح من حيث الممارسة القضائية حاليا[1].

ب- موزعي حق التثبيت في شبكة الأنترنت

هنالك حاليا في العالم العديد من المؤسسات و الشركات التجارية خاصة أو عمومية تعرض على الزبائن المستعملين لشبكة الأنترنت إمكانية تثبيت محتوياتهم و ذلك على العموم مقابل أتعاب (مثلا : مواقع و صفحات أنترنت في موزعاتها المعلوماتية ***Ses serveurs*** [2].

و بالتالي موزع حق التثبيت يتعامل مع الزابون المعلوماتي كمؤجر إذ يؤجر مكان و حجم معين لهذا المكان في شبكة الأنترنت أين تكون للمستأجر فرصت نشر ما يشاء، و في هذه الحالة تكون المسؤولية الجزائية مقدرة كما هو الحال بالنسبة لحالة موزعي حق الدخول إلى شبكة الأنترنت، أي أن مسؤوليته لا تعد قائمة في حالة عدم علمه بالمحتويات المجرمة و نظر لإستحالة إمكانية مراقبته لكل المحتويات نظرا لكميتها الهائلة[3].

هذا الطرح يمكن الأخذ به و لكن بتحفظ إذ أنه في حالة منح موزعي حق التثبيت عنوان أنترنت لموقع أنترنت جديد بإمكان للمصالح التقنية الرقابة على محتوى صفحات هذا الموقع التي إستلمتها في الأصل مسبقا من طرف الزابون مؤلف هذا الموقع، إذا في هذه الحالة و نظرا لكون المصالح التقنية تنبأت بان نشاط الزابون من خلال محتويات موقعه تعد غير مشرعة، في هذه الحالة فقط تعد المسؤولية الجزائية قائمة لموزع حق التثبيت إذا قام بتثبت تثبيت المحتويات[4].

---

(1)_ أنظر : Eric TAVENARD, ***Op.cit***, de la page 45.

(2)_ أنظر : Eric TAVENARD, ***Ibid***, page 46.

(3)_ أنظر : Eric TAVENARD, ***Idem***.

(4)_ أنظر : Eric TAVENARD, ***Idem***.

بالرجوع إلى المادة 6-2 من القانون الفرنسي رقم 575-2004 لـــ 21 جوان 2004 المتعلق : "بالثقة في الإقتصاد المعلوماتي" المتمم في 11 جويلية 2010[1]، فإن مسؤولية موزع حق التثبيت كوسيط تقني لا تكون قائم إلا في حالة عدم تدخل هذا الأخير في سبيل التصدي للمحتويات الغير مشروعة عبر الشبكة من خلال منع تقنيا الإطلاع عليها بناء على أمر قضائي[2]، بمعنى آخر، موزع حق التثبيت ليس مسؤول عن المحتويات التي يثبتها عبر الشبكة المفتوحة إلا في حالة عدم إمتثاله لأمر قضائي في سبيل التصدي أو حذف أو منع الدخول تقنيا إلى المحتويات المجرمة، و بالتالي الوسيط التقني لن يكون مسؤول جزائيا إلا في حالة تلقيه لأمر قضائي بالتدخل تقنيا في ما يخص المحتويات الغير مباحة و لم يمتثل و يستجب له، غير أنه من الناحية العملية فمسؤولية الوسطاء التقنيين لم تثار أمام العدالة إلا في مناسبات نادرة[3].

حسب ما سلف تبيانه فأن القانون حول الثقة في الإقتصاد المعلوماتي عدل في إلتزامات الوسطاء التقنيين و بما فيهم موزعي حق التثبيت حيث أنه إذا كان في الأصل كقاعدة عامة ليس للوسيط التقني إلتزام في ما يخص الرقابة على مضمون المحتويات التي تمر على مصالحه التقنية، إلا أنه بموجب هذا القانون الجديد أصبح من الممكن إثارة المسؤولية الجزائية و المدنية للوسطاء التقنيين مهما كانت وظيفتهم، أي في حالة علمه بالمحتويات الغير مشروعة و مع ذلك فإنه قام بتثبيتها أو لم يتدخل لحذفها، أو في حالة عدم إمتثاله لأمر قضائي يحثه على التدخل تقنيا من أجل وضع حد لهذه المحتويات، إلا أن السؤال الذي يمكن طرحه في هذه الحالة هو كيف يمكن تحديد بدقة مدى توافر المعرفة و العلم الفعلي للوسيط التقني بالمحتويات الغير مشروعة التي قام بتثبيتها ؟[4].

الفرع الثالث : تطوير حماية وقائية للقاصر من المحتويات اللا أخلاقية

في هذا الفرع سنبين بأن حماية القاصر من المحتويات الغير مشروعة و مخاطر الأنترنت من المفروض يتعين أن يتم تطويرها على شقين، الشق الأول من هذه الحماية يتعلق بالجانب العقابي أو القمعي الذي سلف لنا و أن

---

(1)_ أنظر : Eric TAVENARD, ***Op.cit***, de la page 46.

(2)_ جاء نص المدة 6-2 كما يلي : "الأشخاص الطبيعية أو المعنوية التي تضمن، حتى مجانيا لوضع تحت تصرف الجمهور عبر الشبكة من خلال مصالح الإتصال، إمكانية تخزين إشارات، كتابات، صور، أصوات أو رسائل مهما كانت طبيعتها المبعوثة من طرف المرسلين، لا يمكن أن تثار مسؤوليتها المدنية بسبب النشاطات أو المعلومات المخزنة بناء على طلب لمرسل معين إلى هذه المصالح إذا لم تكن على علم بطبيعتها الغير مشروعة أو عن وقائع أو حالات التي تظهر هذا الطابع، أو منذ لحظة علمها تصرفت بسرعة لسحب هذه المعطيات أو جعل الدخول إليها غير ممكن".

« Les personne physiques ou morales qui assurent, même a titre gratuit, pour la mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services ne peuvent pas voir leur responsabilité civile engagée du fait des activités ou des informations stockées à la demande d'un destinataire de ces service si elle n'avaient pas effectivement connaissance de leur caractère illicite ou de faits et circonstances faisant apparaître ce caractère ou si, dés le moment ou elles ont eu cette connaissance, elles ont agi promptement pour retirer ces données ou en rendre l'accès impossible ».

(3)_ أنظر : Eric TAVENARD, ***Op.cit***, de la page 46.

(4)_ أنظر : Eric TAVENARD, ***Ibid***, de la page 46 à 47.

تحدثنا عنه، أم الشق الثاني فيتعلق خصوصا بالجانب الوقائي كمرحلة سابقة عن اللجوء إلى المتابعة القضائية (الجزائية و المدنية)، و يتعلق هذا الجانب بتوعية القصر من مخاطر الأنترنت و هذا من خلال وسيلتين أساسيتين أولها : تدخل السلطة الإدارية المختصة بالرقابة على مختلف المحتويات التي تمر على مستوى الموزع ***"Le Serveur"*** للوسطاء التقنيين داخل التراب الوطني عندما يتعلق الأمر بشبكة الأنترنت، أو على مستوى أي نوع آخر من وسائل النشر أو الإتصال الحديثة كما هو بالنسبة لشبكات الإتصال اللاسلكية كالإتصالات بواسطة الهواتف النقالة مثلا أو بواسطة الأقمار الصناعية كالبث التلفزي مثلا[1] (الفقرة الأولى).

أما الوسيلة الثانية : للحماية الوقائية للقصر فتتمثل في التدخل الفعال للأولياء الذين يلعبون دور أساسي في توعية و تربية القاصر بإعتبارهم الحاجز الأساسي بين القاصر و العالم الخارجي (أي شبكة الأنترنت) و ما تحمله من معطيات أو تصرفات غير مشروعة[2] (الفقرة الثانية).

الفقرة الأولى : الرقابة على المحتويات من طرف سلطة إدارية

في هذا المجال و بالخصوص بالنسبة للتشريع الفرنسي تجدر إلى أن حماية القصر ضد المحتويات الغير مشروعة منذ زمن طويل كانت محل رقابة إدارية و هذا مهما كان نوع الدعامة الحاملة للمعلومات، و من هذا المنطلق يمكن القول بأن الرقابة الإدارية كانت موجودة منذ بداية فترة الطبع، التأليف و النشر على الورق و التي تطورت في ما بعد لتشمل تكنولوجيات الإعلام و الإتصال الحديثة لتصبح في شكلها العددي ***"Numérique"*** [3](أولا).

في ما بعد أصبح يمتد دور السلطة الإدارية إلى المحتويات العددية و بما في ذلك محتويات شبكة الأنترنت [4] (ثانيا).

أولا : الرقابة الإدارية في مجال الصحافة المكتوبة

في هذا المجال تعد مقتضيات القانون رقم 49-956 سارية المفعول على النشرات الموجهة للشباب (1)، كما يمتد مفعولها إلى كل أنواع المؤلفات و المنشورات الأخرى عندما يتبين بأن أثرها يشكل خطر على الشباب من الناحية الأخلاقية[5] (2).

---

(1)_ أنظر : Eric TAVENARD, ***Op.cit***, page 48.

(2)_ أنظر : Eric TAVENARD, ***Idem***.

(3)_ أنظر : Eric TAVENARD, ***Idem***.

(4)_أنظر : Eric TAVENARD, ***Ibid***, page 49.

(5)_ أنظر : Eric TAVENARD, ***Idem***.

1 – المنشورات الخاصة بالشباب

المادة الأولى من القانون رقم 49–356 عرفت الكتابات الخاصة بالشباب على أنها : "منشورات دورية كانت أم لا، التي من خلال طبيعتها أو عرضها أو موضوعها موجهة أو خاصة بالأطفال و المراهقين"[1] [2].
و تجدر الإشارة إلى أنه في حالة وجود إشكال في ما إذا كانت المنشورة محل النزاع الجزائي موجهة أم لا للشباب، فإن المحكمة هي المختصة في تقدير ذلك[3].

من جهة أخرى بين قانون 1949 مختلف أنواع الجرائم الخاصة بالنشر و الموجهة للقصر إذ أن المادة 2 نصت بأن المنشورات المعنية بموجب المادة الأولى من نفس القانون يجب أن لا تتضمن "أي رسم أو بيان، أي كتابة، أي وقائع، مواضيع أو عناوين، تعرض" أفعال الفسق أو أي تصرف ذات تكييف جناية أو جنحة أو من طبيعتها التأثير سلبيا على نفسية و أخلاقية الطفولة أو الشبيبة[4].

أيضا من خلال المادة 13 من قانون 1949 يمكن أن نلاحظ بأن المشرع الفرنسي أدخل حيز النفاذ عملية الرقابة الإدارية المسبقة على النشرات الخاصة بالطفولة و الشباب، حيث جاء نصها كما يلي[5] :

"الإستراد من أجل البيع أو النشر المجاني في فرنسا لنشريات أجنبية خاصة بالشباب تعد مقيدة بموافقة الوزير المكلف بالإتصال بناء على إقتراح إيجابي الذي تبديه لجنة مكلفة بالحراسة و الرقابة على النشريات الخاصة بالأطفال و المراهقين"[6] [7].

و بالتالي هذه اللجنة المستقلة التي أنشأت بموجب المادة 3 من قانون 1949 و التي يترأسها عضو من مجلس الدولة، مكلفة أساسا بعد إجراء عملية رقابة على كل أنوع المعلومات بأن تقترح كل الإجراءات الواجب

---

(1)_ أنظر النص باللغة الفرنسية :
« Publications périodiques ou non qui, par leur caractère, leurs présentation ou leur objet, apparaissent comme principalement destinées aux enfants et adolescents ».

(2)_ أنظر : Eric TAVENARD, ***Op.cit***, page 49.

(3)_ أنظر : Eric TAVENARD, ***Idem***.

(4)_ أنظر : Eric TAVENARD, ***Idem***.

(5)_ أنظر : Eric TAVENARD, ***Idem***.

(6)_ أنظر النص باللغة الفرنسية :
« L'importation pour la vente ou la distribution gratuite en France de publications étrangères destinées à la jeunesse est subordonnée à l'autorisation du ministre chargé de l'information prise sur avis favorable de la commission chargée de la surveillance et du contrôle des publications destinées à l'enfance et à l'adolescence ».

(7)_ أنظر : Eric TAVENARD, ***Op.cit***, de la page 49.

إتخاذها و التي من شأنها تطوير أو تحسين المنشورات الخاصة بالأطفال و الشباب كما أنها مكلفة بإخطار السلطات المختصة بالجرائم و كل التصرفات بواسطة الصحافة و التأليف التي من شأنها الإضرار بالطفولة[1].

2- إمتداد الرقابة الإدارية إلى كل المنشورات الورقية

يعد الإطار التشريعي و التنظيمي الفرنسي الخاص بالمنشورات الخاصة بالأطفال و في سبيل حمايتهم أساسا من الجرائم المرتكبة في هذا المجال غير فعال إذا لم يتدخل المشرع الفرنسي ليمدد من هذه الحماية إلى كل أنواع المنشورات أي كانت طبيعتها و التي قد تكون حاملة لجريمة و في آن واحد تشكل خطر على أخلاقيات القاصر[2].

و بالتالي و في سبيل حماية هذه الفئة من أفراد المجتمع من مخاطر الأنترنت، وضع من طرف الحكومة الفرنسية نظام تدخل إداري مسبق ساري النفاذ على كل أنواع المنشورات و بما فيها الواردة على شبكة الأنترنت و هذا طبقا لنص المادة 14 من قانون 16 جويلية 1949، و بالتالي المنشورات المعنية بنظام الحماية و التي قد تخضع لإجراء المنع المسبق على الإطلاع عليها هي[3] :

"المنشورات من أي طبيعة كانت و التي تشكل خطر على الشبيبة بسبب طبيعتها اللا أخلاقية أو المخلة بالحياء أو بسبب المكانة المفتوحة فيها للإجرام و العنف"[4].

في هذه الحالة، الترخيص الإداري يمنح من طرف وزير الداخلية، بناءا على رأي من اللجنة المكلفة بالرقابة و الحراسة في ما يخص المنشورات الخاصة بالطفولة و الشباب[5].

من هذا المنطلق بإمكان وزير الداخلية أن يمنع :

"إقترح، تسليم أو بيع للقصر ذو ثمانية عشر سنة من السن المنشورات من أي طبيعة كانت و التي تشكل خطر على الشبيبة بسبب طبيعتها اللا أخلاقية أو المخلة بالحياء أو بسبب المكانة المفتوحة فيها للإجرام و العنف.

---

(1)_ أنظر : Eric TAVENARD, ***Op.cit***, page 50.

(2)_ أنظر : Eric TAVENARD, ***Ibid***, page 50.

(3)_ أنظر : Eric TAVENARD, ***Idem***.

(4)_ أنظر النص المادة باللغة الفرنسية :

« Les publications de toute nature présentant un danger pour la jeunesse en raison de leur caractère licencieux ou pornographiques ou de la place faite au crime ou à la violence ».

(5)_ أنظر : Eric TAVENARD, ***Op.cit***, page 50.

عرض هذه المنشورات لنظر الجمهور في أي مكان كانت، و بما فيها خارج أو داخل المحلات التجارية أو الأكشاك، و قيام بعملية إشهارها عن طريق اللافتات.

القيام لصالح هذه المنشورات، بالإشهار عن طريق نشرات و بيانات دعائية أو بواسطة إدخال إشهارات عنها في الصحافة، أو عن طريق رسائل موجهة إلى فئة من جمهور محتملة الإعجاب بها أو عن طريق الحصص الراديو أو التلفزية"[1].

و بالتالي وزير الداخلية في فرنسا ليس بإمكانه أن يتخذ قرار بمنع أو حذف أو حجز أي منشورة إلا بناءا على رأي إستشاري من اللجنة المكلفة بالرقابة و الحراسة في ما يخص المنشورات الخاصة بالطفولة و الشباب[2].

من جهة أخرى و نظرا لظهور و إنتشار فئات جديدة من الدعامات الحاملة لمعطيات قد تشكل خطر على الطفولة مثلما هو الحال بالنسبة للمنشورات الورقية السالفة الذكر، فإن المشرع الفرنسي مدد نظام الرقابة التي وضعها في ما يخص المنشورات الكتابية إلى المحتويات الجديدة المعلوماتية العددية و بما فيها شبكة الأنترنت[3].

ثانيا: تمديد نظام الرقابة إلى التكنولوجيات الحديثة للإتصال و النشر

تمديد نظام الرقابة إلى باقي تكنولوجيات الإتصال و النشر الحديثة لم يتم إلا في 1998 بموجب القانون رقم 98-468 المؤرخ في 17 جويلية 1998 و المتعلق بـــ : "الوقاية و قمع الجرائم الجنسية و كذا حماية القصر"[4].

و بالتالي الإضافات الجديدة التي جاء بها هذا القانون نراها من خلال المواد 32 إلى 39 التي وضعت نظام و مكنزم الرقابة يمتد إلى الوثائق أو المعطيات السمعية البصرية ***Audiovisuels*** التي ستسمح للسلطات الإدارية بمنع تحت طائلة عقوبات جزائية، عملية نشر هذه الوثائق المنشورات أو المعطيات إلى جانب القصر نظرا لطبيعتها المخلة بالحياء اللا أخلاقية، العنيفة أو ذات التمييز العنصري[5].

---

(1) _ أنظر النص باللغة الفرنسية :

« De proposer, de donner ou de vendre à des mineurs de dix-huit ans les publications de toute nature présentant un danger pour la jeunesse en raison de leur caractère licencieux ou pornographique, ou de la place faite au crime ou à la violence.
D'exposer ces publications à la vue du public en quelque lieu que ce soit, et notamment à l'extérieur ou à l'intérieur des magasins ou des kiosques, et de faire pour elles de la publicité par la voie d'affiches.
D'effectuer en faveur de ces publications, de la publicité au moyen de prospectus d'annonce ou insertions publiques dans la presse, de lettres-circulaires adressées aux acquéreurs éventuels ou d'émissions radiotélévisées ».

(2) _ أنظر : Eric TAVENARD, ***Op.cit***, page 50.

(3) _ أنظر : Eric TAVENARD, ***Ibid***, page 51.

(4) _ أنظر : **ملحق رقم 16**

(5) _ أنظر : Eric TAVENARD, ***Op.cit***, page 51.

بالرجوع إلى المادة 32 الفقرة الأولى من القانون رقم 98-468 يمكن أن نلاحظ بأنها وسعت من نطاق سلطة المنع المخولة لوزير الداخلية بموجب المادة 14 من قانون 1949 حيث جاء نصها كما يلي[1] :

المادة 32 فقرة 1 تنص : "عندما يكون المستند مثبت بواسطة تقنية و التي يمكن قراءتها إلكترونيا، يدويا أو عدديا تشكل خطر على الشبيبة بسبب طبيعتها اللا أخلاقية المخلة بالحياء، فإن الدعامة و كل الملحقات التابعة لها في إنجازها يجب أن تتضمن بصفة واضحة، مقروءة و غير قابلة لحذفها الإشارة "ممنوع وضعها في تصرف القصر (مادة 227-24 ق.ع)". هذه الإشارة تتضمن منع عرض، تسليم، إيجار أو بيع المنتوج محل الإعتبار للقصر ..."[2].

عندما يكون المحتوى أو المستند أيا كانت طبيعته و المنصوص عليه في المادة 32 فقرة 1 يشكل خطر على الشبيبة و القصر بسبب طابعه الغير أخلاقي المخل بالحياء أو بسبب المكانة المفتوحة فيه للإجرام و العنف، فإنه بإمكان السلطات الإدارية التدخل لمنع وفقا للمادة 33 من قانون 98-468 :

المادة 33 : " بإمكان السلطة الإدارية على الأكثر منع :

1° عرض، تسليم، إيجار أو بيع للقصر المستندات المنصوص عليها في المادة 32،

2° إستعراض المستندات المنصوص عليها في المادة 32 لنظر الجمهور في أي مكان كانت. حتى و إن كان الإستعراض ممكن في أماكن التي يكون فيها الدخول ممنوع للقصر،

3° القيام، لصالح هذه المستندات بعملية الإشهار بأي وسيلة كانت. حتى و إن كان الإشهار ممكن في أماكن التي يكون فيها الدخول ممنوع للقصر"[3].

و تجدر الإشارة إلى أنه بإمكان السلطة الإدارية أن تصدر قرار يخص كل حالات المنع الثلاثة المنصوص عليها في المادة 33 في آن واحد حسب الحالات التي ستطرح عليها[4].

---

(1)_ أنظر : Eric TAVENARD, ***Op.cit***, page 51.

(2)_ أنظر نص المادة باللغة الفرنسية :

Art 32 alinéa 1 : « Lorsqu'un document fixé par un procédé déchiffrable par voie électronique en mode analogique ou en mode numérique présente un danger pour la jeunesse en raison de son caractère pornographique, le support et chaque unité de son conditionnement doivent comporter de façon visible, lisible et inaltérable la mention "mise à disposition des mineurs interdite (article 227-24 du code pénal)". Cette mention comporte interdiction de proposer, donner, louer ou vendre le produit en cause aux mineurs… ».

(3)_ أنظر نص المادة باللغة الفرنسية :

Article 33 « L'autorité administrative peut en outre interdire :
1° De proposer, de donner, de louer ou de vendre à des mineurs les documents mentionnés à l'article 32 ;
2° D'exposer les documents mentionnés à l'article 32 à la vue du public en quelque lieu que ce soit. Toutefois, l'exposition demeure possible dans les lieux dont l'accès est interdit aux mineurs ;
3° De faire, en faveur de ces documents, de la publicité par quelque moyen que ce soit. Toutefois, la publicité demeure possible dans les lieux dont l'accès est interdit aux mineurs ».

(4)_ أنظر : Eric TAVENARD, ***Op.cit***, page 51.

الفقرة الثانية : الرقابة الإدارية في مجال شبكة الأنترنت

في الوقت الراهن شبكة الأنترنت أصبحت من بين وسائل الإتصال الأكثر إستعمال في العالم، كما أنها تدخل في فئة وسائل الإتصال السمعية البصرية وفقا للقانون 30 سبتمبر 1986 المتعلق بحرية الإتصال و بالتالي و من هذا المنطلق فإن نظام الرقابة الذي وضع بموجب قانون 1949 تم تمديده إلى شبكة الأنترنت و كل أنواع الإتصال و النشر الحديثة و أن نفس الإجراءات المتعلقة بالمحتويات المكتوبة تمتد هي الأخرى إلى المجال العددي و المنطقي و بما فيها شبكة الأنترنت، و من بين أنواع التدخلات الإدارية في مجال الأنترنت في سبيل مكافحة وقائيا المحتويات التي قد تشكل خطر على القصر : نقطة الإتصال بجمعية موزعي حق الدخول و خدمات الأنترنت في فرنسا ***(A.F.A) Association des fournisseurs d'accès et de service Internet*** (1)، و المصلحة المركزية لمكافحة الإجرام المرتبط بتكنولوجيات الإعلام و الإتصال***(O.C.L.C.T.I.C) Office centrale de lutte contre la criminalité liée aux technologies de l'information et de la communication*** (2)[(1)].

1- نقطة الإتصال بجمعية موزعي حق الدخول في فرنسا

جمعية موزعي حق الدخول و خدمات الأنترنت أنشأت في سنة 1998 نقطة إتصال موحدة في عنوان الأنترنت التالي : ***http://www.pointdecontact.net/***، و الهدف من هذا الموقع هو تلقي الجمعية كل البلاغات و التصريحات بمحتويات متعلقة أساسا بالتصرفات الجنسية المخلة بالحياء إزاء القصر و كذا الدعوى إلى العنف و التمييز العنصري أو تلك التي تضم معلومات أو معطيات أيا كانت طبيعتها عن العنف أو لا أخلاقية، حيث أن الجمعية تعتبر التصرفات الجنسية المخلة بالحياء إزاء القصر[(2)] :

"كل صورة تظهر قاصر في حالة ذات طابع جنسي، أو أيضا في حالة صور مرسومة، و كذا الرسائل التي تحرض على ممارسة العلاقات الجنسية مع الأطفال"[(3)].

يمكن أن يتم التصريح أو الإبلاغ بالمحتويات الغير مشروعة بصفة مجهول الهوية أو العكس، و بإمكان صاحب الإبلاغ أن يصرح بموقع أنترنت، أو مجمعة مستعملي شبكة الأنترنت ***newgroup*** أو بريد غير مرغوب فيه ***Spam***، أو دردشة عبر الشبكة بواسطة برامج الدردشة مثلا، و في هذا السبيل يقترح موقع الأنترنت لهذه الجمعية المبين عنوانها أعلاه إستمارة إلكترونية عبر الشبكة المفتوحة و كذا نماذج رسائل في لغات متعددة، لإرسالها إلى نقطة الإتصال أي إلى موزعي الخدمات المعنية أو إلى السلطات العمومية، و هنا و حسب

---

(1)_ أنظر : Etienne WERY, ***Op.cit***, de la page 68 à 69.

(2)_ أنظر : Etienne WERY, ***Ibid***, page 68.

(3)_ أنظر النص باللغة الفرنسية :

« Toute image présentant un mineur dans une situation à connotation sexuelle, y compris en bande dessinée, ainsi que tout message qui inciterait aux relations sexuelles avec des enfant ».

الحالات نقطة الإتصال ترسل هذه التصريحات و البلاغات إلى موزعي حق الدخول و خدمات الأنترنت المعنيين، إلى السلطات العمومية المختصة[1].

2- نقطة الإتصال بالسلطات العمومية الفرنسية

منذ نوفمبر سنة 2001 مستعملي شبكة الأنترنت أصبحوا بإمكانهم التصريح و الإبلاغ بالمحتويات الغير مشروعة في موقع أنترنت رسمي للسلطات العمومية و الخاص بتجميع التصريحات في كامل التراب الوطني الفرنسي، و التي من خلالها تباشر المصلحة المركزية لمكافحة الإجرام المرتبط بالتكنولوجيات الإعلام و الإتصال في مكافحة كل أنوع المحتويات التي تمر على موزعي التراب الوطني و التي تعد ذات طبيعة غير مشروعة و من شأنها الإضرار بالغير بمعنى القصر[2].

هذا الوقع الحكومي يقترح إستمارة عبر الشبكة التي يمكن إملائها بصفة مجهول الهوية أم العكس ففي ما يخص التصريح أو الإبلاغ للسلطات العمومية بموقع أنترنت أو أي نوع آخر من المحتويات التي سمحت بنشر صور لقصر ذات طابع مخل بالحياء أو رسائل تشجع تحويل القصر، هذا الموقع من جهة أخرى يسمح لزائريه أن يدخل في إتصال مع مصالح الشرطة أو الدرك الأقرب إلى موطنه أو سكنه لإتخاذ الإجراءات الأولية للتصريح بالمحتويات، كما يمكن الإتصال بهذه السلطات المعنية عن طريق البريد الإلكتروني ***"contact@signale.internet-mineurs.gouv.fr"***، أما موقع الأنترنت الرسمي لهذه السلطات فهو بعنوان : ***""http://www.interieur.gouv.fr/sections/contact/police/questions-cybercriminalite***"، و عنوان ***"https://www.internet-signalement.gouv.fr/PortailWeb/planets/Accueil!input.action***، و بالتالي كل تصريح من خلال مواقع الأنترنت أو البريد الإلكتروني يتم تسجيله من طرف المصالح العمومية في قاعدة معطياتها و المنظمة من طرفها و التي تقوم بالتحقيقات الأولية (تحقيقات تقنية و قانونية)، ثم ترسل عند الضرورة البلاغ إلى مصالح الشرطة و الدرك المختصة إقليميا حتى تتخذ الإجراءات اللازمة، و الشخص الذي قام بالتصريح الإلكتروني في هذه الحالة يتحصل على بريد يتضمن رقم التصريح عندما يكون قد ترك للمصالح عنوان بريده الإلكتروني أو أي معلومة تسمح بتبليغه برقم التصريح الذي قام به[3].

---

(1)_ أنظر : Etienne WERY, ***Op.cit***, page 68.

(2)_ أنظر : Etienne WERY, ***Ibid***, page 69.

(3)_ أنظر : Etienne WERY, ***Idem***.

المبحث الخامس : جريمة الإرهاب المعلوماتي

يعد الإرهاب المعلوماتي من أخطر أصناف الجرائم المرتبطة بتكنولوجيا المعلوماتية نظرا لأثرها ***Son impact***، و دوافعها ***Ses buts et enjeux***، لذا سنحاول في هذا المبحث وضع تعريف محكم لهذا الصنف المستحدث من الجرائم و الذي يعد خليفة لجريمة الإرهاب بمفهومها التقليدي (المطلب الأول)، ثم سنحاول تفرقة هذا التعريف المستحدث عن جريمة الإرهاب بمفهومها التقليدي (المطلب الثاني)، ثم سنبين خصوصيات جرائم الإرهاب في حيز معلوماتي أو منطقي غير ملموس (المطلب الثالث)، و أخيرا سنتحدث بإيجاز عن دوافع و أسباب ظهور هذا النوع الجديد من الجرائم المستحدثة (المطلب الرابع).

المطلب الأول : تعريف جريمة الإرهاب المعلوماتي

يمكن أن نعرض تعرفان جاء بهما باتريك قالي ***Patrick Galley*** و التي تعبر بصفة واقعية و منطقية على هذا الصنف المستحدث لجرائم التكنولجيات العالية كما يلي[1] :

"الإرهاب المعلوماتي هو تحطيم أو إتلاف أنظمة معلوماتية، بهدف المساس أو إحداث خلل يمس بإستقرار دولة[2] أو بهدف الضغط على حكومة ما"[3] [4].

"الإرهاب المعلوماتي هو القيام بعملية من شأنها المساس و إحداث خلل ماس بإستقرار دولة أو بهدف الضغط على حكومة، بإستعمال طرق تدخل في صنف جرائم المعلوماتية"[5] [6].

غير أنه تجدر الإشارة إلى أنه من الصعب وضع تعريف دقيق لهذا النوع الجديد من الجرائم أي جريمة الإرهاب المعلوماتي ***Le terrorisme informatique ou le Cyberterrorisme*** لأنه و في نظر المختصين في هذا الميدان فهذه الجريمة المستحدثة تشمل حالات مختلفة عن بعضها البعض، ففي حالات يمكن أن تتعلق الجريمة إما بتخريب معطيات، أو تحريف مستندات معلوماتية سرية أو تحريف أموال، إتلاف تسجيلات معلوماتية

---

(1)_ أنظر : Patrick GALLEY, projet science, technique & société, ***« terrorisme informatique : quel sont les risques ? »***, école polytechnique fédérale de LAUSANNE, page 22.

(2)_ أنظر الشريط التلفزي تحت عنوان :
Cyber guérilla - Hackers, pirates et guerres secrètesdifusé le 10 mars à 20h35. Une exclusivité France 5

(3)_ أنظر النص باللغة الفرنسية :
« Le terrorisme informatique est le fait de détruire ou de corrompre des systèmes informatique, dont le but de déstabiliser un pays ou de faire pression sur un gouvernement ».

(4)_ أنظر : Patrick GALLEY, ***Op.cit***, page 69.

(5)_ أنظر النص باللغة الفرنسية :
« Le terrorisme informatique est le fait de mener une action destinée à déstabiliser un pays ou à faire pression sur un gouvernement, en utilisant des méthodes classées dans la catégorie des crimes informatiques ».

(6)_ أنظر : Patrick GALLEY, ***Op.cit***, page 69.

معلوماتية مهمة أو القيام بعمليات التجسس مثلا : عسكرية و عبر الشبكات المعلوماتية أي عن بعد، و فكل هذه الحالات يعتبر الشخص متهم مجرم معلوماتي خاصة و إن أدت هذه التصرفات بالمساس بأمن دولة أو مجموعة من الأشخاص، كما أنه يمكن تعريف جريمة الإرهاب المعلوماتي على أنه[1] :

"هجوم مع سبق الإصرار، ذو أهداف سياسية ضد المعلومة، للأنظمة المعلوماتية، ضد أهداف مسلحة (الشرطة، الدرك، أو أهداف عسكرية) أو غير مسلحة (كالإدارات المدنية الوطنية)، من طرف جماعات وطنية أو خفية"[2].

كما يمكن أن نتكلم عن جرائم الإرهاب المعلوماتية في حالة إستعمل الجماعات الإرهابية تكنولوجيات الإتصال الحديثة و بما فيها الأنترنت لشراء الأسلحة أو لإجراء إتصالات أو علاقات مع الغير و في سبيل التخطيط لعمليات إرهابية مستقبلية[3].

على العموم يمكن أن نستقر مبدئيا على التعريف الذي جاءت به السيدة دوروتي دينينق ***Madame Dorothy Denning*** إثر عرض تم بتاريخ 23 ماي 2000 أمام لجنة القواة العسكرية لغرفة الممثلين بالولايات المتحدة الأمريكية ***La commission des forces armées de la chambre des représentants*** الممثلين[4] [5].

و من هذا المنطلق يمكن أن نقول بأن هذا النوع الأخير من الجرائم المعلوماتية يدخل في صنف الجرائم المعلوماتية ضد أنظمة المعالجة الآلية للمعطيات التي سبق و أن تكلمنا عنها بالتفصيل و لكن يتعين القول بأن المساس هنا لن يكون بنظام معلوماتي واحد أو إثنان مثلا و إنما مساس بالملايين من الأنظمة المعلوماتية في أغلب الأحيان في آن واحد أي هجوم معلوماتي من الدرجة الثالثة ***Attaque cybercriminelle de classe 3*** ، و هذا المصطلح في ميدان المعلوماتية يعني أساسا عدد من الأنظمة المعلوماتية يساوي : 16777214 على مستوى شبكة معلوماتية واحدة أي ***Classe A***، و حتى نوضح الصورة أكثر يتعين الإشارة :

---

(1)_ أنظر : Sophie REVOL, (DESS) droit du multimédia et de l'informatique, ***« Terroristes et Internet »***, sous la direction de M. KOSTIC, université Paris II – Panthéon Assas, année 2002-2003 (France), page 9.

(2)_ أنظر النص بالغة الفرنسية :

« Une attaque préméditée, politiquement motivée contre l'information, des systèmes d'information, contre des cibles combattantes ou non, par des groupes subnatiaunaux ou clandestins ».

(3)_ أنظر : Sophie REVOL, ***Op.cit***, page 9.

(4)_ أنظر : Sophie REVOL, ***Ibid***, de la page 9 à 10.

(5)_ أنظر النص بالغة الفرنسية :

« Le cyberterrorisme consiste à se livrer à des activités terroristes dans le cyberespace. L'on entend par-là généralement des attaques illégales et des menaces d'attaques contre les ordinateurs, les réseaux, et les renseignements qui y sont emmagasinés dans le but d'intimider ou de contraindre un gouvernement ou son peuple à la réalisation d'objectifs politiques ou sociaux. En outre, pour répondre à la définition de terrorisme, une attaque doit être suivie de violence contre les biens ou les personnes, ou au moins occasionner suffisamment de dégâts pour créer de la peur. Ainsi, des attaques qui causent la mort ou bien des blessures corporelles, des explosions, des accident d'avions, la contamination de l'eau, ou de graves préjudices économiques seraient de bon exemples. Des attaques sérieuses contre des infrastructures critiques pourraient être qualifiées d'actes de cyberterrorisme, en fonction de leur importance. Ce ne saurait être le cas d'attaques perturbants des services non-essentiels ou qui ne constituent une gène coûteuse ».

أولا : إلى أن المعلوماتية، الأنترنت و كل وسائل الإعلام و الإتصال الحديثة أصبحت لها أهمية كبرى في أن كل التجهيزات الأساسية ***Les infrastructures essentiels*** في الدول المتطورة و المجتمعات المعاصرة لاسيما منها مثلا : الخاصة بالكهرباء و الغاز، الماء، البنوك، الإدارات العمومية من محاكم، مجالس، إدارة الشرطة و الدرك، الإدارة العسكرية، البلديات، الولايات، إدارات الضرائب، البورصة [1] ترتكز أساسا على تكنولوجية المعلوماتية و شبكات الإتصال المستحدثة التي تسمح بإتصال عدد هائل من الأنظمة المعلوماتية فيما بينها في الدولة الواحدة، و في هذا الإطار أي هجمة أو مساس من الدرجة الثالثة بالأنظمة المعلوماتية التي تسير التجهيزات الأساسية قد تسبب أضرارا جسيمة على المستوى الوطني كما ستتسبب في الفوضة و عدم الإستقرار[2].

ثانيا : تعتبر تكنولوجيات الإعلام و الإتصال و بما فيها شبكة الأنترنت وسائل تسمح بالإتصال سواء على المستوى الوطني أو العالمي، بنشر معلومات أو بالدعوى إلى الجهاد مثلا أو في سبيل توظيف أكبر عدد ممكن من الأشخاص في هذه المنظمات مثلا.

هاتين الخاصيتين لوسائل الإتصال الحديثة لم تفلت بطبيعة الحال من نظر الجماعات الإرهابية بمختلف أنواعها إسلامية، صهيونية مثلا[3].

و بالتالي بإمكان الجماعات الإرهابية أن تلجأ إلى وسائل الإتصال المستحدثة لإرتكاب جرائم معلوماتية من الدرجة الثالثة في سبيل إحداث أضرار جسيمة في دولة أو خلق جو من عدم الإستقرار و الرعب و الفوضى أو في سبيل الضغط على أي دولة لتلبية طلباتهم الغير مشروعة بطبيعة الحال[4].

من جهة أخرى تجدر الإشارة إلى أنه و إلى حد الآن لم تسجل أي عملية إرهاربية بتقنية المعلوماتية و من هذا الحجم أي الدرجة الثالثة إلى درجة المساس بإستقرار أي دولة.

---

(1) _ الجزائر حاليا لا تملك تجهيزات معلوماتية متطورة إلى هذه الدرجة بالمقارنة بالدول المتطورة تكنولوجيا كالولايات المتحدة الأمريكية مثلا، و لكن يتعين على المشرع الجزائري أن يأخذ بعين الإعتبار بأن هذا المجال أي مجال تكنولوجيات الإعلام و الإتصال و علاقتها بمختلف قطاعات الدولة الأساسية بالإضافة إلى تطور الشبكات المعلوماتية داخل الدولة لتسمح للأنظمة و التجهيزات المعلوماتية لمختلف هذه القطاعات الإتصال بالقطاعات الأخرى و بالتالي يصبح من الممكن للغير الدخول فيها بطريقة إحتيالية و تحقيق عمليات إرهابية معلوماتية من الدرجة الثالثة، فهذا السيناريو من المحتمل جدا أن يحدث في الجزائر أو في أي دولة أخرى مع تطور تجهيزاتها و أنظمتها و شبكاتها المعلوماتية، و تجدر الإشارة إلى أن كل ما كانت دولة تعتمد بنسبة كبيرة على تكنولوجية المعلوماتية و الشبكات التي تسمح بإتصال مختلف أنظمة قطاعاتها ببعضها كل ما كانت هذه الدولة عرضة للهجمات المعلوماتية من طرف الجماعات الإرهابية بنسبة كبيرة.

(2) _ أنظر : Sophie REVOL, ***Op.cit***, page 8.

(3) _ أنظر : Sophie REVOL, ***Idem***.

(4) _ أنظر : Sophie REVOL, ***Idem***.

بالإضافة إلى ما سلف تبيانه يمكن أيضا للجماعات الإرهابية أن تستعمل هذه التكنولوجية لا في سبيل المساس بالأنظمة الخاصة بتجهيزات الدولة الأساسية كما سلف شرحه و لكن كوسيلة لنشر أفكارهم المتطرفة في أغلب الأحيان و عبر الشبكة العالمية "أنترنت" أو كوسيلة إتصال فيما بين أعضائها و التي تفلت في أغلب الأحيان عن رقابة السلطات العمومية نظر للطابع العالمي للشبكة و الصعوبات التقنية في سبيل وضع مكنزمات الرقابة على عكس ما هو الحال بالنسبة للإتصالات السلكية أو اللاسلكية[1].

المطلب الثاني : التفرقة بين جريمة الإرهاب المعلوماتي و الجريمة في إطارها التقليدي

بكل بساطة تكمن التفرقة في تعريف جريمة الإرهاب المعلوماتي و الجريمة نفسها لكن في إطارها التقليدي في الوسيلة المستعملة لتحقيقها و لكن مع تحقيق نفس النتائج أي نشر الرعب و الخوف و عدم الإستقرار، و هذه الوسيلة المميزة المستعملة في تحقيق نفس النتيجة هي تقنية المعلوماتية و شبكات الإتصال المعلوماتية، بمعنى آخر الإجرام المرتبط بعمليات الإرهاب المعلوماتية كباقي الجرائم المعلوماتية السالفة الذكر تتم في أغلب الأحيان عن بعد و من دون اللجوء إلى العنف الجسدي لتحقيقها، فقط يكفي توافر المعرفة الكافية في ميدان تقنية المعلوماتية حتى تتحقق في ما بعد النتيجة.

المطلب الثالث : خصوصيات جريمة الإرهاب المعلوماتي

هذه الخصوصيات تتعلق أساسا بصفة مرتكبي هذه الجريمة (الفرع الأول)، و بالوسيلة التي تستعمل في تحقيقها (الفرع الثاني).

الفرع الأول : الإرهابيين و الشبكات المعلوماتية

الإرهابيين المعلوماتيين ***Les cyber-terroristes*** يدخلون في صنف المجرمين المعلوماتيين أو قراصنة المعلوماتية ***Les cyber-délinquants ou les pirates informatiques***، القرصنة المعلوماتية على العموم مرتبطة بأربع أنواع من المجرمين الذين يمارسون الإجرام عبر الشبكات المعلوماتية : إذ هنالك ما يسمى بالبايكر ***Les backers*** أو فئة من المجرمين المختصة في الدخول الغير مشروع عن بعد في الأنظمة المعلوماتية، و كذا الكراكر ***Les crackers*** هذه الفئة من المجرمين مختصة في كسر مكنزمات الإئتمان و الحماية و كذا الأرقام و الشفرات السرية للبرامج المعلوماتية أ أيضا يمكن إضافة فئة الفريكار ***Phreacker*** أي المجرمين المختصين في قرصنة وسائل الإتصال السلكية أو اللاسلكية، و أخيرا فئة الهاكرز ***Les hackers*** المختصين في التلاعب بمكنزمان و الوسائل التقنية لحماية الأنظمة المعلوماتية من القرصنة، و بالتالي مهم كان نوع المجرم المعلوماتي أو الفئة التي ينتمي

---

(1)_ أنظر : Sophie REVOL, ***Op.cit***, page 8.

إليها إلا أنه لا يصبح في حقيقة الأمر مرتكبا لجريمة الإرهاب المعلوماتي إلا إذا نتج عن تصرفه إحداث عدم الإستقرار و الخوف في دولة أو مجمعة ***provoquer l'insécurité, la terreur et la peur*** معينة وبالتالي يعد من الجرائم المعلوماتية الإرهابية مثلا إذا إخترق هاكرز النظام المعلوماتي الخاص بإدارة و تنظيم توزيع الكهرباء في ولاية ما و تسبب في إتلافه و نتج عنه إنقطاع الكهرباء لأيام فهذا التصرف حسب رجال القانون يعد بعملية إرهابية[1].

الفرع الثاني : الوسائل المستعملة في جرائم الإرهاب المعلوماتي

المجرمين المعلومتيين في هذا النوع من الجرائم يرتكزون أساسا على تقنية المعلوماتية و تجهيزات إلكترونية مهما كان نوعها و التي ستسهل إرتكاب الجرائم عبر الشبكات المعلوماتية وكذا وسائل منطقية كالبرامج المعلوماتية المقرصنة أو الفيروسات المعلوماتية (أنظر الفصل الأول المبحث الأول)[2].

المطلب الرابع : دوافع إرتكاب جرائم الإرهاب المعلوماتي

هنالك نوعين من الدوافع التي قد تدفع مجموعة أو منظمة إرهابية لإرتكاب جرائم الإرهاب بواسطة تقنية المعلوماتية : أولتها دافع الحصول على الأموال لتمويل منظمتهم أساسا أما الدافع الثاني فهو دافع سياسي بحث، و تجدر الإشارة إلى أن الدوافع السالفة الذكر هي نفس الدوافع الخاصة بنفس الجريمة و لكن في شكلها الكلاسيكي.

---

(1)_ أنظر : Sophie REVOL, ***Op.cit***, de la page 10 à 11.

(2)_ أنظر : Sophie REVOL, ***Ibid***, de la page 11 à 12.

الخاتمـــــة

الخاتمـــــــة

كخلاصة لهذه الدراسة يمكن أن نصل إلى جملة من النتائج المهمة سواء من الناحية الإجرائية أو من الناحية الموضوعية في ما يخص موضوع الجرائم المعلوماتية كجرائم ذات طابع خاص :

فمن الناحية الإجرائية يمكن أن نلاحظ بأن الجرائم المرتكبة في محيط معلوماتي تخضع على العموم لإجراءات خاصة سواء من حيث الإثبات أو من حيث المتابعة، فمن جهة الدليل الإلكتروني كوسيلة إثبات مستحدثة يطرح إشكال مزدوج سواء من حيث قيمته القانونية أمام العدالة لإدانة أو تبرئة المتهم أو من حيث كيفية إتيانها، أما في ما يخص المتابعة فتخضع الجرائم المرتكبة في محيط المعلوماتية و منها الماسة بأنظمة المعالجة الآلية للمعطيات المعلوماتية لإجراءات خاصة نص عليها المشرع الجزائري في القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق لـــ 5 أوت 2009 و المتضمن : "القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها"، كما خصص المشرع أقطاب متخصصة بعدد 4 على مستوى التراب الوطني لمحاكمة مثل هذه الجرائم في حالة ما إذا كان التحقيق التمهيدي يخص جرائم معينة و المتعلقة بـــ : المخدرات، تبييض الأموال أو تلك المتعلقة بالتشريع الخاص بالصرف أو الماسة بأنظمة المعالجة الآلية للمعطيات و الجريمة المنظمة عبر الحدود الوطنية و كذا جرائم الفساد المنصوص و المعاقب عليها بموجب القانون رقم 06-01 المؤرخ في 20 فيفري 2006 و المتعلق بالوقاية و مكافحة الفساد و هذا بموجب القانون رقم 06-01 المؤرخ في 20 ديسمبر 2006 المعدل و المتمم لقانون الإجراءات الجزائية، و هذه الأقطاب منعقدة في كل من (قسنطينة، الجزائر العاصمة – سيدي أمحمد، وهران و ورقلة)، و بالتالي و ما عدا جريمة المساس بأنظمة المعالجة الآلية فباقي الجرائم المعلوماتية الأخرى تختص بمحاكمتها المحاكم العادية.

في ما يخص الموضوع أي الجرائم المعلوماتية كموضوع لمذكرة الحالية، فمن خلال دراستنا قمنا بتقسيمها وفقا للتصنيف التقليدي إلى جرائم ضد الأموال و جرائم ماسة بالأشخاص و الحريات، إلا أن هذا لا يعني عدم وجود طرق أخرى للتصنيف مثلا إلى جرائم مرتكبة ضد النظام المعلوماتي أو تلك المرتكبة بواسطته أو أيضا الجرائم المرتكبة في محيط معلوماتي مغلق أو تلك المرتكبة في محيط مفتوح على الشبكات المعلوماتية، من جهة أخرى و من خلال ما تطرقنا إليه من أنواع من الجرائم يمكن أن نستنتج وجود صنف من الجرائم المعلوماتية البحتة لا مثيل له في الجرائم التقليدية أي جريمة المساس بأنظمة المعالجة الآلية للمعطيات بالإضافة إلى جرائم أخرى لم نتطرق لها في هذه الدراسة، و التي نص عليها المشرع الجزائري بموجب القانون رقم 04-15 المؤرخ في 27 رمضان 1425 الموافق 10 نوفمبر سنة 2004 الذي أدخل إلى قانون

العقوبات قسم سابع مكرر تحت عنوان : "المساس بأنظمة المعالجة الآلية للمعطيات " (المواد من 394 مكرر إلى 394 مكرر 7 ق.ع.جزائري).

من جهة أخرى محيط المعلوماتية و على العموم، زاد صعوبة إضافية للمشرع الجزائري في سبيل مكافحة الإجرام، خاصة و أنه أصبح من بين الوسائل المستحدثة المفضلة للمجرمين لإرتكاب جرائم مستحدثة كالمساس بالأنظمة أو جرائم تقليدية، و حسب رأينا يعود مثل هذا التفضيل لتكنولوجية المعلوماتية و الأنترنت لسبب بسيطة هو صعوبة إكتشاف مرتكب الجريمة و متابعته مع العلم بأن معظم الجرائم المعلوماتية ترتكب بإستعمال الشبكة العالمية أنترنت، كما يطرح أيضا هذا الصنف الجديد من الإجرام صعوبة أخرى بالنسبة للسلطات المحلية و العدالة في ما يخص مدى إمكانية أو عدم إمكانية متابعة المتهم خاصة و إن كان هذا الأخير قد إقتراف الجريمة إنطلاقا من دولة أجنبية للمساس بالأموال أو الأشخاص و الحريات على المستوى الوطني مما يستدعي على سبيل الإستعجال ضرورة توحيد القوانين على المستوى الدولي كما هو معمول بهي في الإتحاد الأوروبي أو تكتلات دولية أخرى بالإضافة إلى تكثيف الإتفاقيات الدولية مع دول أجنبية بما فيها المجاورة للجمهورية الجزائرية بهدف تعزيز التعاون و الشراكة في الميدان القضائي و تسهيل بطبيعة الحال مهمة متابعة و تسليم مرتكبي الجرائم المعلوماتية أينما كانوا بهدف محاكمتهم.

من جهة أخرى و بخصوص الممارسة القضائية في ميدان الجرائم المعلوماتية يمكن أن نستنتج بأنه من الرغم من المحاولات و الإجتهادات القضائية الفرنسية للتهرب من الحلول الكلاسيكية التقليدية لاسيما في مجال السرقة للمال المعنوي، فالفقه جاء متنافيا مع هذه الحلول التي جاءت بها العدالة، و منها الصادرة عن محكمة النقض الفرنسية، و بقي متعنقا بالمفهوم التقليدي لجريمة السرقة أو غيرها من الجرائم، أيضا في أغلب الأحيان لاحظنا بأن القاضي الجزائي الفرنسي يحاول في كل مرة عدم الإعتراف و تمديد النصوص التقليدية إلى الجرائم المستحدثة التي تطرح عليه، متمسكا في ذلك بالمفاهيم التقليدية المتعارف عليها، غير أنه يمكن طرح السؤال التالي في هذا المجال : هو هل أن هذا التصرف يعد حتما نقطة سلبية لتطور الممارسة القضائية و نوعية الأحكام في مجال جرائم المعلوماتية ؟ و الجواب على هذا التساؤل بسيط، و هو عدم إشتراط بالضرورة التطبيق النصوص العقابية التقليدية على ما هو مستحدث كما هو الحال بالنسبة للمال المعنوي و أنه و من خلال ما تم تبيانه في دراستنا هو أن القاضي الجزائي الفرنسي تمكن في العديد من الحالات تفادي القاعدة العامة بخصوص النصوص التقليدية و في مجال معلوماتي و ذلك بإيجاد حيل قانونية من شأنها تمديد بالضرورة التجريم إلى التصرفات و الأموال و التقنيات المستحدثة.

أيضا ما يمكن الوصول إليه كنتيجة هو أنه يتعين عدم التعنق بفكرة وجود فراغ قانوني في ما يخص الجرائم المعلوماتية كون أن الممارسة القضائية و بما فيها الفرنسية على سبيل الخصوص تمكنت في العديد من القضايا المطروحة أمامها من تمديد أثر النصوص العقابية التقليدية إلى الجرائم التقليدية المرتكبة بإستعمال تكنولوجية المعلوماتية و الأنترنت، أما في ما يخص الجرائم المعلوماتية البحتة كما هو الحال بالنسبة لجريمة المساس بأنظمة المعالجة الآلية للمعطيات فهنا الأمر يختلف فلولا تخصيص المشرع سواء الفرنسي أو الجزائري نصوص عقابية خاصة بمثل هذه التصرفات لما كان بإمكان العدالة متابعة و إدانة مرتكبيها.

إذا النصوص التقليدية قابلة للتطبيق على الجرائم التقليدية المرتكبة بتكنولوجية المعلوماتية و الأنترنت حسب الحالات، أما في ما يخص الجرائم المعلوماتية البحتة و المستحدثة التي لا مثيل لها في الجرائم التقليدية كنا لا بد على المشرع تجريمها بنصوص خاصة حتى تكون محل متابعة.

أيضا لاحظنا من خلال هذه الدراسة بأنه توجد حلول وقائية كمرحلة قبلية لإيداع شكاوي على مستوى السلطات القضائية لتحريك الدعوى العمومية و هو حسن إستعمال تقنية المعلوماتية و الأنترنت كاللجو ء إلى إستعمال البرامج المضادة للفيروسات و كذا إستعمال أرقام و شفراة سرية محكمة لحماية المعطيات و كذا اللجوء إلى سلطات إدارية مختصة في سبيل الرقابة و الوقاية من التعسف في إستعمال بعض الحقوق كما هو الحال بالنسبة للتجربة الفرنسية مع اللجنة الوطنية للمعلوماتية و الحريات ***"(C.N.I.L) Commission Nationale de l'Informatique et des Libertés"*** .

الـــمـــلاحـــق

ملحق رقم : 1

وثيقة معلومات رقم 6 حول "الإجرام المعلوماتي" إحدى المواضيع محل الدراسة في المؤتمر الحادي عشر للأمم المتحدة حول :

" الوقاية من الجريمة و العدالة الجنائية "

أيام 18 إلى 25 أفريل 2005 ببنكوك (تايلاند)

Fiche d'information n° 6 sur la "délinquance informatique"
l'un des sujets objets d'étude au 11éme congrés des nations unis sur :
"la prévention du crime et la justice pénale"
du 18 au 25 avril 2005 à Bangkok (Thailande)

مستند *(P.D.F)* مستنسخ من صفحة الأنترنت التالية :
http://www.unis.unvienna.org/pdf/05-82112_F_6_pr_SFS.pdf

ملحق رقم : 2

التقرير الصحافي حول أعمال اللجنة الثانية في الجلسة التاسعة مساءا يوم 22 أفريل 2005
من المؤتمر الحادية عشر للأمم المتحدة "للوقاية من الإجرام و العدالة الجنائية"
لدراسة وسائل إستدراك عجز الأنظمة القضائية في مواجهة الإجرام المعلوماتي

Le rapport de presse sur les travaux de la commission II à la 9éme séance - aprés-midi du 22 avril 2005
du 11éme congrès des nations unis pour la "prévention du crime et la justice pénale"
pour étudier les moyens de remédier à l'impuissance des systèmes judiciaires
face à la cybercriminalité

مستند *(P.D.F)* مستنسخ من صفحة الأنترنت التالية :
http://www.un.org/events/11thcongress/docs/bkkcp19f.pdf

Nations Unies 60 A l'heure du renouvellement

Onzième Congrès des Nations Unies pour la prévention du crime et la justice pénale

Bangkok, Thaïlande 18-25 avril 2005

Commission II BKK/CP/19
9e séance* - après-midi 22 avril 2005

Le onzième Congrès de l'ONU pour la prévention du crime étudie les moyens de remédier à l'impuissance des systèmes judiciaires face à la cybercriminalité

À la veille de la deuxième partie du Sommet mondial sur la société de l'information, qui se tiendra à Tunis, du 16 au 18 novembre 2005, le onzième Congrès des Nations Unies pour la prévention du crime et la justice pénale a tenu, cet après-midi, au sein de l'une de ses deux Commission, une discussion sur les moyens de remédier à l'impuissance des systèmes judiciaires face à la criminalité liée à l'informatique dite cybercriminalité. La discussion a été organisée en collaboration avec l'Institut coréen de criminologie.

La prolifération des nouvelles technologies de l'information et des communications (TIC) a suscité une multiplication de nouveaux types de délits qui constituent une menace non seulement pour la confidentialité, l'intégrité et la disponibilité des systèmes informatiques mais aussi pour la sécurité d'infrastructures critiques. La cybercriminalité montre aujourd'hui trois tendances, à savoir: la sophistication, la commercialisation et à l'intégration, a expliqué un professeur de l'Université nationale d'Australie qui a aussi dénoncé le danger du cyberterrorisme.

Le danger de la cybercriminalité ne concerne pas que les pays industrialisés, a alerté le Directeur de la Section des TIC du Département de la justice du Canada qui a d'abord souligné que les deux extrémités du fossé numérique se rapprochent depuis l'émergence des 12 « info-États » du Sud. Les pays en développement sont désormais exposés aux virus qui ne s'attaquent qu'aux téléphones mobiles. Si ces virus ne peuvent détruire les infrastructures mêmes, ils peuvent servir de vecteur à d'autres crimes comme l'usurpation d'identité.

La lutte contre cette cybercriminalité a été qualifiée de complexe, compte tenu de la grande difficulté à collecter des preuves intangibles et éphémères par nature. La difficulté vient aussi du fait qu'il faut souvent retracer l'activité criminelle et ses effets à travers toute une série de prestataires de services Internet ou d'entreprises parfois situées dans des pays différents. Cette difficulté a été illustrée par le Directeur adjoint de la Direction des crimes spécialisés d'Interpol qui a invoqué les cas de pornographie impliquant des enfants. Les solutions proposées aujourd'hui ont été résumées en sept points par le représentant de la France.

** Il n'existe pas de communiqué de presse pour la 8e séance.*

(à suivre)

À l'instar des participants, il a préconisé l'établissement d'une typologie précise de la cybercriminalité pour en définir les moyens d'analyse et d'information; l'intensification de la formation des personnels concernés, services de détection et de répression, procureurs et juges compris; et le renforcement de la capacité d'enquête par la création d'organes spécialisés. Le représentant français a aussi prôné, la sensibilisation des particuliers et des entreprises, avec le concours des prestataires de services; la surveillance des contenus illicites véhiculés sur l'Internet; le décloisonnement des connaissances afin que chaque progrès profite à tous les services, et le renforcement de la coopération internationale par une adhésion aux conventions internationales dont celle du Conseil de l'Europe, spécifiquement sur la cybercriminalité, entrée en vigueur le 1er juillet 2003, et son Protocole sur l'incrimination d'actes de nature raciste et xénophobe.

De tels efforts, a-t-il dit, encourageait l'adaptation de la législation nationale et faciliterait l'entraide judiciaire. Pour ce faire, le renforcement de l'assistance technique s'avère urgente, ont souligné de nombreuses délégations, en réclamant la mise à jour régulière du Manuel des Nations Unies sur la cybercriminalité, conformément à l'évolution rapide des TIC et à celle de la cybercriminalité.

La Commission poursuivra ce débat demain, samedi 23 avril, à partir de 10 heures, alors que commencera le débat de haut niveau au cours duquel de nombreux ministres de la justice commenteront les cinq questions inscrites à l'ordre du jour du Congrès, avant d'adopter, le 25 avril, la Déclaration de Bangkok. Placé sous le signe des « Alliances stratégiques », le Congrès tient ses travaux au sein de la Plénière, de ses deux Commission et de six ateliers pour étudier les questions de la lutte contre la criminalité organisée, de la coopération internationale contre le terrorisme, de la corruption et de l'application des règles et des normes de l'ONU en matière de prévention du crime et de la justice pénale.

Parmi les panélistes qui son intervenus aujourd'hui dans les discussions, il faut signaler la présence du Président de l'Institut coréen de criminologie, Taehoon Lee; du Secrétaire permanent du Ministère des technologies de l'information et des communications de la Thaïlande, Krainsorn Pornsutee; du Professeur à l'Université nationale d'Australie, Peter Grabosky; et du Directeur de la Section des politiques de justice pénale, de la technologie et de l'analyse du Département de la justice du Canada, Gareth Sansom. Il faut signaler également la présence de la Conseillère juridique à la Section de la propriété intellectuelle et de la criminalité liée à l'informatique du Département de la justice des États-Unis, Amanda Hubbard; de la Procureure attachée à la Haute Cour de justice de la Roumanie, Ioana Albani; et du Directeur adjoint du Directorat des crimes spécialisés d'Interpol, Hamish McCulloch.

MESURES DE LUTTE CONTRE LA CRIMINALITÉ LIÉE À L'INFORMATIQUE

Présentations

M. TAEHOON LEE, Président de l'Institut coréen de criminologie, a dit que la criminalité liée à l'informatique est en hausse. L'espace cybernétique est de plus en plus le lieu où des millions de gens paient leurs factures, consultent des professionnels, font des recherches d'information, font leurs courses, et restent en contact avec leurs familles, leurs amis, des institutions publiques, ou leurs employeurs. La cybercriminalité pose des défis jusqu'ici inconnus du système judiciaire. La nature globale de la cybercriminalité pose des problèmes légaux difficiles à résoudre parce que les criminels peuvent agir en utilisant des serveurs situés en dehors des territoires où ils commettent leurs méfaits, sans courir le risque d'être arrêtés et soumis aux sanctions des règlements nationaux. Les différents crimes informatiques, comme le blanchiment d'argent, le jeu, la fraude par Internet, le harcèlement des personnes et le terrorisme cybernétique, peuvent être commis à tout moment de manière instantanée. Les prédateurs peuvent s'attaquer à des gens vivant à l'autre bout du monde sans que leurs actions soient tout de suite repérées et sans que la police puisse enquêter. L'espace cybernétique est aussi devenu la cible des organisations terroristes et des organisations du crime organisé, ce qui risque d'avoir des impacts désastreux sur les sociétés. Les questions à résoudre rapidement sont celles de la mise en place de cadres de justice pénale adaptés à la cybercriminalité; de la création de nouvelles méthodes d'enquête; et de saisie des informations électroniques, a dit M. Lee. Malheureusement, le monde dispose de très peu de traités ou conventions multilatérales traitant de la cybercriminalité, a-t-il déploré. Le Conseil de l'Europe est l'auteur de la seule convention contre la cybercriminalité existant à l'heure actuelle, a relevé le représentant.

M. KRAISORN PORNSUTEE, Secrétaire permanent au Ministère des technologies de l'information et des communications de la Thaïlande, a souligné qu'il convient d'abord de cerner les actes de cybercriminalité, en faisant observer que les délits varient d'un pays à l'autre. Ce qui serait considéré comme une entrave à la liberté d'expression ailleurs peut être un crime grave en Thaïlande, a-t-il dit en donnant l'exemple de propos offensants à l'égard de la famille royale. La cybercriminalité pose des défis énormes et les organes de détection et de répression ont du mal à suivre. Il est temps de réfléchir à des mesures ambitieuses pour rattraper les retards, a-t-il dit en espérant la création, au cours de ce Congrès, de partenariats solides.

M. PETER GRABOSKY, professeur à l'Université nationale d'Australie, a dit que le fossé numérique et l'absence de lois contre la cybercriminalité dans les pays qui se trouvent de l'autre coté du fossé de l'univers informatique sont favorables aux criminels qui peuvent profiter de ces lacunes pour perpétrer leurs crimes. Le *physing*, qui consiste à utiliser des sites web légitimes pour tromper des gens et se procurer leurs informations personnelles à des fins criminelles est en train de se développer rapidement. Le commerce électronique est devenu la cible de toutes sortes d'attaques qui posent une menace à l'expansion des activités économiques. Les attaques cybernétiques se basant sur l'usage des ordinateurs personnels de personnes non averties afin de s'en prendre à des institutions ou à des individus sont devenues monnaie courante. Le cyberterrorisme comprend les activités informatiques illicites ayant pour objet final d'exercer des pressions ou des actes d'intimidation sur des personnes, des groupes, des institutions ou des pays, a dit M. Grabosky. L'Internet peut aussi être un puissant vecteur de propagande.

M. GARETH SANSOM, Directeur de la Section des politiques de droit pénal, de la technologie et de l'analyse du Département de la justice du Canada, a estimé que le fossé numérique ne devrait pas être présenté comme les deux falaises opposées d'un canyon, compte tenu de l'existence d'un groupe d'« info-États » d'une douzaine de pays qui se trouvent entre les deux extrêmes. Le fossé se réduit peu à peu, mais il faudra des générations pour que les pays en bas de liste parviennent au niveau des pays qui se situent aujourd'hui au milieu. La réduction du fossé numérique semble être le fruit de l'accès à de nouvelles techniques comme la téléphonie mobile. Des tendances différentes, en la matière, exposent les régions à des vulnérabilités différentes en matière de cybercriminalité. Dans les pays en développement, les nouvelles techniques peuvent susciter des nouvelles menaces jusqu'à ce que leur système s'affirme et les normes de sécurité soient introduites. En l'occurrence, une réponse unique n'est pas viable.

En 2001, des recherches ont été faites sur les virus et sur les *worms* –vers. L'étude épidémiologique a permis de déceler quelques tendances. Ainsi, selon cette étude, les virus varient dans leur vitesse et dans leur capacité de propagation et il semble que les pays industrialisés y sont plus vulnérables. Cela n'est plus vrai aujourd'hui, a prévenu le Directeur en mettant en garde les pays en développement contre les virus qui visent spécifiquement les téléphones mobiles. La nouvelle tendance est que ces vers-virus ne peuvent plus réellement attaquer les infrastructures, mais le danger est qu'ils peuvent servir de vecteur à un autre crime comme le vol ou l'usurpation. Cette nouvelle utilisation des vers peut exposer les pays en développement à de nouvelles menaces alors que leur croissance passe par l'accès aux nouvelles technologies de l'information et de la communication.

Mme AMANDA HUBBARD, Juriste à la Section du Ministère de la justice des États-Unis, chargée des affaires criminelles ayant trait à l'informatique et à la propriété intellectuelle, a déclaré que le 16 juillet dernier son service avait reçu un appel d'urgence venant d'un de ses fonctionnaires travaillant dans un pays d'Amérique du Sud. Le fonctionnaire transmettait une demande d'aide judiciaire de la police du pays concerné aux autorités américaines. Une personne avait été enlevée, et ses kidnappeurs demandaient le versement d'une rançon à travers un courrier électronique envoyé d'un serveur situé sur le territoire américain. Le Département américain de la justice a pu contacter les opérateurs du serveur après avoir identifié sa location. Le Département a pu obtenir une injonction légale permettant de saisir l'opérateur du serveur et d'obtenir le nom de la personne qui avait ouvert le compte e-mail à partir duquel la demande de rançon avait été envoyée. Les agents chargés de l'enquête ont pu déterminer que la personne se servant de ce compte d'adresse e-mail se trouvait dans le pays où avait eu lieu l'enlèvement, et que le courrier électronique exigeant la rançon avait été envoyé depuis un ordinateur situé dans un cybercafé de la capitale de ce pays. Les autorités américaines ont transmis ces informations à la police du pays où avait été perpétré le crime. Celui à qui appartenait l'adresse e-mail a été identifié et arrêté, a dit Mme Hubbard en indiquant que ce cas avait été résolu grâce à la rapidité des contacts entre le Département américain de la justice et les autorités du pays où le crime avait été perpétré. Malheureusement, la plupart des crimes informatiques ne connaissent pas ce genre de conclusion heureuse.

Mme IOANA ALBANI, Procureure attachée à la Haute Cour de justice de la Roumanie, a déclaré que devant l'impuissance de l'appareil judiciaire face à la cybercriminalité, son pays a d'abord créé une Section chargée d'enquêter sur ce type de criminalité ainsi qu'une structure sur les fraudes par Internet, au sein de la police. C'est en 2000 que la Roumanie a lancé ses premières enquêtes qui ont conduit, l'année suivante, à des condamnations qui, faute de loi spécifique, se sont fondées sur les articles relatifs à la fraude ou à l'usurpation prévues par le Code pénal. Le caractère étendu de ce type de crimes conjugué à l'absence de cadre juridique a conduit à un conflit de juridiction. La Roumanie a alors décidé d'adopter la Convention sur la cybercriminalité du Conseil de l'Europe et en juin 2002, et promulgué une loi sur le commerce électronique pour sanctionner la fraude par cartes de crédit, puisque l'article du Code pénal sur la fausse monnaie ne pouvait s'appliquer. La loi, qui s'est avérée un outil très efficace pour les services de détection et de répression, pénalise aussi l'accès illégal à des donnés sur l'Internet ou leur effacement.

En 2003, a poursuivi la Procureure, la Roumanie a enfin adopté sa loi sur la lutte contre la cybercriminalité. Elle définit les concepts et précise les procédures et a permis la création d'un Bureau chargé des demandes d'entraide judiciaire au sein de la Haute Cour de justice. Par ailleurs, un Service permanent de lutte contre la cybercriminalité a été établi au sein du Bureau chargé de la criminalité transnationale organisée et du terrorisme, de la police nationale. La Roumanie a aussi jugé utile d'ouvrir un site Internet pour recevoir des plaintes sur les violations éventuelles des dispositions prévues mais surtout pour diffuser la législation pertinente ou encore lancer des avertissements quant aux nouveaux types de fraude. Avec les institutions mises en place, la Roumanie est désormais capable de répondre aux demandes d'entraide et de coordonner ses actions avec d'autres pays, a assuré la Procureure.

M. HAMISH MCCULLOCH, Directeur adjoint du Directorat des crimes spéciaux d'Interpol, a déclaré que les abus contre les enfants, notamment la pornographie, avaient connu une expansion extraordinaire à travers l'usage de l'Internet. Plus de trois millions d'images de pornographie enfantine circulant sur le web sont stockées dans la base de données d'Interpol, a-t-il indiqué. Les images représentent 20 000 victimes différentes, a-t-il dit. La première question qui se pose à un enquêteur, a dit M. McCulloch, est de chercher à identifier l'enfant dont l'image circule dans le cyberespace. Ensuite, il faut chercher à savoir où se trouve géographiquement l'enfant, et si les images qui circulent ont été vues auparavant ou font partie d'une série de photos dont certaines ont auparavant fait l'objet d'enquêtes. S'il s'agit de nouvelles images, on cherche à identifier l'enfant et l'environnement dans lequel la photo a été prise. La base de données d'Interpol ne peut être utilisée que par des personnels autorisés, a dit Hamish McCulloch. Deux agents sont responsables de sa gestion. Quatorze pays participent à l'enrichissement de cette base de données, alors que les services spécialisés savent que les enfants sont victimes d'abus dans un plus grand nombre de pays. Interpol espère donc que d'autres États se joindront à la tâche qui doit être menée au niveau international, a dit le responsable d'Interpol.

Discussion

En lançant la discussion, le représentant du Canada s'est demandé s'il serait utile de publier des documents d'informations techniques tels que le Manuel des Nations Unies sur la prévention et la répression de la criminalité liée à l'informatique. Il a aussi demandé s'il était possible d'incorporer des appareils de prévention dans les technologies de l'information et des communications (TIC) avant leur lancement sur le marché. Qui devrait financer une telle initiative? Le secteur public ou le secteur privé, s'est-t-il interrogé. Techniquement, peut-on, utiliser les mêmes technologies pour combattre la cybercriminalité? Les intervenants ont jugé important de réviser régulièrement le Manuel de l'ONU, en arguant de l'évolution rapide des technologies et des nouvelles formes de criminalité. Un représentant de Microsoft a reconnu le rôle du secteur privé dans la protection des usagers. Ce secteur, a-t-il dit, doit aussi collaborer avec les services de détection et de répression pour dissuader la cybercriminalité et là, les vendeurs ont une responsabilité à assumer. Le Secteur privé pourrait aussi former les services spécialisés. La collecte de preuves exige une formation très poussée, a prévenu le Directeur du Département de la justice du Canada, en insistant sur la complexité de la tâche. Les services spécialisés, a ajouté le représentant de Microsoft, auraient tout intérêt à développer des relations de travail avec les fournisseurs de services qui sont les meilleurs informateurs en cas de délits.

Le représentant de l'Ukraine a dit que son pays qui avance dans la voie de la démocratie, était en train de mettre en place des réglementations contre les crimes informatiques et cybernétiques. Ce qui s'est passé au cours des récents scrutins politiques en Ukraine a montré combien il était important de créer un cadre législatif sain sur l'usage des outils informatiques. L'Ukraine espère que la communauté internationale parviendra à s'accorder sur la mise en place d'un cadre de lutte contre la cybercriminalité qui soit applicable de manière universelle. Le représentant de l'Autriche a demandé aux panélistes quel était le principal obstacle se posant aux enquêtes sur les crimes cybernétiques. Que devraient faire les pays pour lever cet obstacle? Le représentant de la Jamahiriya arabe libyenne a dit que son pays venait d'entrer dans l'ère des paiements bancaires électroniques. La Libye s'inquiète des dangers qui pourraient menacer cette pratique et aimerait que les victimes d'actes criminels soient protégées.

Répondant à la question de l'Autriche, M. Gareth Sanson a dit que le principal obstacle aux enquêtes contre les actes de cybercriminalité se trouvait dans l'absence de lois et de procédures au niveau national des pays. La recherche de preuves est généralement difficile, à cause de l'absence d'environnement légal adapté au monde informatique. M. McCulloch a pour sa part indiqué qu'Interpol avait du mal à mener ses enquêtes parce que de nombreux pays sont réticents à reconnaître que des actes de pornographie enfantine sont perpétrés sur leur territoire. Certains gouvernements refusent même de transmettre des photos à la base de données d'Interpol, a-t-il dit. **Mme Iona Albani**, a dit que les fournisseurs et prestataires devraient mieux coopérer avec les institutions de recherche policière et d'enquêtes contre les crimes liés à l'informatique.

Le représentant de la France a estimé que la réponse à la cybercriminalité devait être conduite de manière globale. La France a décidé d'accroître les moyens d'analyse et d'information consacrés à la lutte contre ce crime. Elle renforce ses services d'enquête et d'investigation. Son administration et ses entreprises sont de plus en plus sensibilisées aux crimes cybernétiques, et des actions sont menées pour sensibiliser l'opinion quant au contenu illicite de certains sites Internet. La France estime qu'il faut d'autre part développer la coopération internationale en demandant aux États de signer et ratifier les conventions contre les crimes liés à l'informatique, a dit le représentant.

À son tour, le représentant de l'Espagne a annoncé le projet de créer un observatoire pour mettre au point une série d'indicateurs sur le réseau Internet dans sa partie publique et privée, comme Intranet. Il sera question de faire l'inventaire des technologies mais aussi de recenser tous les programmes d'innovation, de mise au point et de développement existants pour devancer les utilisations criminelles éventuelles de ces technologies nouvelles. À ce titre, il a posé une question aux présentateurs consistant à en savoir un peu plus des autres programmes existants. Il a proposé que l'ONUDC envisage la création de points de contacts d'experts qui pourraient échanger leurs expériences et les enseignements qu'ils ont pu en tirer.

Interpol, a répondu son Directeur adjoint, a installé une Sous-Direction spécialisée sur la cybercriminalité financière. L'orateur a aussi fait part de l'organisation d'une réunion en la matière qui a bénéficié d'une audience internationale très large. Interpol, a-t-il poursuivi, est représenté dans le Groupe de liaison du G-8 par sa Centrale d'appels 24/7 qui permet de maintenir le contact. Quelque 39 pays participent désormais à cette Centrale, a précisé le représentant du Royaume-Uni avant de s'interroger sur le type de recommandation à faire sur les programmes de formation. Peut-on recommander l'établissement d'un réseau d'institutions? Est-il possible de créer une base de données à l'intention des services de détection et de répression? a-t-il encore demandé.

Le Directeur adjoint d'Interpol lui a répondu que des activités de formation ont déjà été lancées, il y a dix ans. Aujourd'hui, l'on envisage des stages de formation réguliers, conformes à l'évolution rapide de la cybercriminalité. La Conseillère spéciale du Département américain de la justice a attiré l'attention des participants sur le « Advocacy Center » qui a organisé un stage de formation à la lutte contre la cybercriminalité. Toutes ces initiatives disparates devraient peut-être être réunies au sein d'un programme d'action élaboré, sous les auspices des Nations Unies, a estimé la représentante de l'Argentine en demandant aux présentateurs s'ils pensent qu'un des programmes, fonds ou institutions des Nations Unies pourrait jouer le rôle de coordonnateur. Nous avons besoin de synergie, a-t-elle insisté, appuyé en cela par le représentant du Canada qui a appelé à plus de coordination, en matière de formation des différents agents du système judiciaire dont les procureurs.

Aucune base de données centralisée n'existe encore, a reconnu la représentante du Département américain de la justice qui a dénoncé les conséquences des restrictions budgétaires. Elle a invité les participants à établir des contacts et à partager les idées et les ressources disponibles. Beaucoup de personnes travaillent d'arrache-pied pour mettre en place des réseaux, a souligné le Directeur adjoint d'Interpol en rappelant une nouvelle fois la création de la Centrale d'appels 24/7. La cybercriminalité évoluant très rapidement, il faudra du temps pour avoir une réponse coordonnée au niveau international.

Le représentant du Maroc a dit que son pays avait lancé une réforme judiciaire visant à réprimer la criminalité informatique. Le Maroc se heurte en ce moment à la question des preuves. Il a besoin d'une assistance technique au niveau juridique et au niveau des avocats. La transposition des dispositions légales d'un système juridique à un autre étant parfois difficile, le Maroc, qui applique essentiellement des normes de droit latin, aimerait savoir quelle assistance pouvait être apportée aux pays pour les aider à intégrer dans leurs systèmes des concepts juridiques venus de systèmes différents.

Mme Iona Albani a indiqué que des programmes d'aide et d'assistance pouvant aider les pays qui ont besoin de soutien pour intégrer des notions de droit d'origine étrangère dans leurs systèmes juridiques existaient. M. Gareth Sansom a dit que des lois-types avaient été élaborées par certains pays du G-8 en ce qui concerne la cybercriminalité. Le représentant de la France a dit que son pays, qui a mené des études sur ces questions, pouvait répondre à la demande du Maroc.

M. Elson Baty, Juge et expert des questions liées aux abus contre les enfants, a dit que la pornographie mettant en scène des enfants devrait être érigée en infraction pénale. Même le fait de visiter des sites abritant ces photos devrait être criminalisé, a-t-il proposé. M. McCulloch lui a répondu qu'Interpol concentrait d'abord ses efforts sur la situation des enfants victimes de sévices sexuels. Concernant la criminalisation de la visite de sites pornographiques, jusqu'à maintenant, cette question relève des législations nationales, a dit M. McCulloch. Une autre difficulté vient du fait que les pays n'ont pas de définition commune de ce qui constitue de la pornographie, a-t-il poursuivi. D'autre part, l'introduction d'images virtuelles dans les iconographies pornographiques complique la tâche des enquêteurs. Le représentant de la Jamahiriya arabe libyenne a évoqué la difficulté de l'établissement des preuves dans les procédures concernant les poursuites contre la pornographie. Le représentant du Chili a souligné que sans une définition des crimes constitutifs de la cybercriminalité, tous les efforts seraient vains.

Faisant part de son sentiment que l'accent a surtout été mis sur les victimes en tant qu'individus, le représentant du Centre international pour la culture scientifique a regretté que le débat soit passé à côté de la menace plus large qui pèse sur les sociétés. La cybercriminalité est surtout dangereuse, a-t-il estimé, pour les grandes entreprises privées: une attaque sur ces dernières pouvant avoir des répercussions sur l'ensemble de la scène internationale. Il a, en effet, souligné que dans presque tous les pays, ces sociétés contrôlent les infrastructure critiques dont les systèmes bancaires, les barrages hydrauliques, le contrôle du trafic aérien ou encore la production d'énergie qui utilisent toutes les techniques informatiques.

Ces sociétés investissent massivement dans la protection de leurs actifs, a rassuré le professeur à l'Université nationale de l'Australie, en rappelant qu'il s'agit d'une obligation juridique et surtout de bons sens. L'ONU a aussi fait un gros travail dans le domaine de la cybersécurité, au sein d'un Groupe d'experts dont le rapport sera présenté à la soixantième session de l'Assemblée générale, a indiqué, à son tour, la Conseillère spéciale du Département américain de la justice.

Documentation

Document de travail (A/CONF.203/14)

Le document souligne que la prolifération, partout dans le monde, des nouvelles technologies de l'information et de la communication (TIC) a suscité une multiplication de nouveaux types de délits liés à l'information. Ces derniers constituent une menace non seulement pour la confidentialité, l'intégrité et la disponibilité des systèmes informatiques mais aussi pour la sécurité d'infrastructures critiques. Les menaces reflètent les différences qui existent aux extrémités du « fossé numérique ». De leur côté les enquêteurs et les procureurs comme les juges se heurtent à un certain nombre de problèmes découlant de ce que les preuves numériques sont à la fois intangibles et éphémères. La difficulté vient aussi du fait qu'il faut souvent retracer l'activité criminelle et ses effets à travers toute une série de prestataires de servies Internet ou d'entreprises parfois situées dans des pays différents, ce qui peut susciter d'épineuses questions de compétence et de souveraineté.

La complexité des défis engendrés par la criminalité liée à l'informatique exige inévitablement une coopération internationale, ce qui signifie qu'en définitive, les pays doivent se doter des outils nécessaires en matière de législation, de procédure et de réglementation. L'approche doit être large et inclusive et aller au-delà du droit pénal, des procédures pénales et de l'action des services de répression. L'accent doit être mis sur les conditions qui doivent être remplies pour qu'une cyberéconomie fonctionne en toute sécurité. Tous les États doivent néanmoins être encouragés à actualiser leur législation pénale. Ils doivent aussi moderniser leurs règles de procédure ainsi que les lois, accords ou arrangements relatifs à l'entraide judiciaire et, lorsqu'ils entreprennent d'élaborer de nouvelles lois, s'inspirer des dispositions de la Convention relative à la cybercriminalité du Conseil de l'Europe. Quant au onzième Congrès, il doit porter son attention sur la nécessité d'établir des mécanismes visant à promouvoir l'échange d'informations au plan international, l'alerte rapide, l'intervention policière et la limitation des dommages. Toujours au plan international, des efforts doivent être déployés pour établir des mécanismes de financement propres à faciliter la recherche appliquée.

Le document contient sept chapitres de fond expliquant les différents types de criminalité liée à l'informatique; les initiatives de l'ONU pour combler le fossé numérique; les difficultés rencontrées par les services de répression; les lacunes existant dans les législations nationales; les moyens de renforcer la coopération internationale; la recherche; et la coopération entre les secteurs public et privé.

* *** *

ملحق رقم : 3

قانون رقم 09-04 مؤرخ في 14 شعبان عام 1430 الموافق 5 جويلية 2009

المتضمن : " القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها "

الجريدة الرسمية الصادرة في 16 أوت 2009 / العـــدد : 47

Loi n° 09-04 du 14 chaabane 1430 correspondant au 5 aout 2009 portant :

"Règles particulières relatives à la prévention et à la lutte contre les infractions liées aux technologies de l'information et de la communication"

Journal officiel du 16 aout 2009 / numéro : 47

الجرائد الرسمية للجمهورية الجزائرية يمكن الإطلاع عليها و إستنساخها بالغة العربية أو الفرنسية في شكل مستندات من نوع *(P.D.F)* في موقع الأنترنت التالي :

http://www.joradp.dz/HAR/Index.htm

قوانين

قانون رقم 09 – 04 مؤرّخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

إن رئيس الجمهورية،

– بناء على الدستور، لا سيما المواد 119 و120 و122 – 7 و126 منه،

– وبمقتضى الأمر رقم 66 – 155 المؤرّخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، المعدّل والمتمّم،

– وبمقتضى الأمر رقم 66 – 156 المؤرّخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات، المعدّل والمتمّم،

– وبمقتضى الأمر رقم 75 – 58 المؤرّخ في 20 رمضان عام 1395 الموافق 26 سبتمبر سنة 1975 والمتضمن القانون المدني، المعدّل والمتمّم،

– وبمقتضى القانون رقم 2000 – 03 المؤرّخ في 5 جمادى الأولى عام 1421 الموافق 5 غشت سنة 2000 الذي يحدّد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية، المعدّل والمتمّم،

– وبمقتضى الأمر رقم 03 – 05 المؤرّخ في 19 جمادى الأولى عام 1424 الموافق 19 يوليو سنة 2003 والمتعلق بحقوق المؤلف والحقوق المجاورة،

– وبمقتضى القانون رقم 08 – 09 المؤرّخ في 18 صفر عام 1429 الموافق 25 فبراير سنة 2008 والمتضمن قانون الإجراءات المدنية والإدارية،

– وبعد رأي مجلس الدولة،

– وبعد مصادقة البرلمان،

يصدر القانون الآتي نصه :

الفصل الأول
أحكام عامة

الهدف

المادّة الأولى : يهدف هذا القانون إلى وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

المصطلحات

المادّة 2 : يقصد في مفهوم هذا القانون بما يأتي :

أ – الجرائم المتصلة بتكنولوجيات الإعلام والاتصال : 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،

ب – منظومة معلوماتية : أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين،

ج – معطيات معلوماتية : أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها،

د – مقدمو الخدمات :

1 – أي كيان عام أو خاص يقدم لمستعملي خدماته، القدرة على الاتصال بواسطة منظومة معلوماتية و/أو نظام للاتصالات،

2 – وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها،

هـ – المعطيات المتعلقة بحركة السير: أي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا في حلقة اتصالات، توضح مصدر الاتصال، والوجهة المرسل إليها، والطريق الذي يسلكه، ووقت وتاريخ وحجم ومدة الاتصال ونوع الخدمة،

و – الاتصالات الإلكترونية : أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية.

مجال التطبيق

المادّة 3 : مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات، يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية.

الفصل الثاني
مراقبة الاتصالات الإلكترونية

الحالات التي تسمح باللجوء إلى المراقبة الإلكترونية

المادّة 4 : يمكن القيام بعمليات المراقبة المنصوص عليها في المادة 3 أعلاه في الحالات الآتية :

أ – للوقاية من الأفعال الموصوفة بجرائم الإرهاب أوالتخريب أوالجرائم الماسة بأمن الدولة،

ب – في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني،

ج – لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية،

د – في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

لا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه إلا بإذن مكتوب من السلطة القضائية المختصة.

عندما يتعلق الأمر بالحالة المنصوص عليها في الفقرة "أ " من هذه المادة، يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المنتمين للهيئة المنصوص عليها في المادة 13 أدناه، إذنا لمدة ستة (6) أشهر قابلة للتجديد وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها.

تكون الترتيبات التقنية الموضوعة للأغراض المنصوص عليها في الفقرة "أ " من هذه المادة موجهة حصريا لتجميع وتسجيل معطيات ذات صلة بالوقاية من الأفعال الإرهابية والاعتداءات على أمن الدولة ومكافحتهما، وذلك تحت طائلة العقوبات المنصوص عليها في قانون العقوبات بالنسبة للمساس بالحياة الخاصة للغير.

الفصل الثالث
القواعد الإجرائية

تفتيش المنظومات المعلوماتية

المادّة 5 : يجوز للسلطات القضائية المختصة وكذا ضبّاط الشرطة القضائية، في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 4 أعلاه، الدخول، بغرض التفتيش، ولو عن بعد، إلى :

أ – منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.

ب – منظومة تخزين معلوماتية.

في الحالة المنصوص عليها في الفقرة "أ " من هذه المادة، إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول إليها، انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك.

إذا تبين مسبقا بأن 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 الصلة ووفقا لمبدأ المعاملة بالمثل.

يمكن السلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها.

حجز المعطيات المعلوماتية

المادّة 6 : عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة

تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية.

يجب في كل الأحوال على السلطة التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية.

غير أنه يجوز لها استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات، قصد جعلها قابلة للاستغلال لأغراض التحقيق، شرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات.

الحجز عن طريق منع الوصول إلى المعطيات

المادّة 7 : إذا استحال إجراء الحجز وفقا لما هو منصوص عليه في المادة 6 أعلاه، لأسباب تقنية، يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية، أو إلى نسخها، الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة.

المعطيات المحجوزة ذات المحتوى المجرم

المادّة 8 : يمكن السلطة التي تباشر التفتيش أن تأمر باتخاذ الإجراءات اللازمة لمنع الاطلاع على المعطيات التي يشكل محتواها جريمة ، لا سيما عن طريق تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك.

حدود استعمال المعطيات المتحصل عليها

المادّة 9 : تحت طائلة العقوبات المنصوص عليها في التشريع المعمول به، لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة المنصوص عليها في هذا القانون، إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية.

الفصل الرابع

التزامات مقدمي الخدمات

مساعدة السلطات

المادّة 10 : في إطار تطبيق أحكام هذا القانون، يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها وبوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11 أدناه، تحت تصرف السلطات المذكورة.

ويتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق.

حفظ المعطيات المتعلقة بحركة السير

المادّة 11 : مع مراعاة طبيعة ونوعية الخدمات، يلتزم مقدمو الخدمات بحفظ :

أ – المعطيات التي تسمح بالتعرف على مستعملي الخدمة،

ب – المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال،

ج – الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال،

د – المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها،

هـ – المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال وكذا عناوين المواقع المطلع عليها.

بالنسبة لنشاطات الهاتف، يقوم المتعامل بحفظ المعطيات المذكورة في الفقرة "أ " من هذه المادة وكذا تلك التي تسمح بالتعرف على مصدر الاتصال وتحديد مكانه.

تحدد مدة حفظ المعطيات المذكورة في هذه المادة بسنة واحدة ابتداء من تاريخ التسجيل.

دون الإخلال بالعقوبات الإدارية المترتبة على عدم احترام الالتزامات المنصوص عليها في هذه المادة، تقوم المسؤولية الجزائية للأشخاص الطبيعيين والمعنويين عندما يؤدي ذلك إلى عرقلة حسن سير التحريات القضائية، ويعاقب الشخص الطبيعي بالحبس من ستة (6) أشهر إلى خمس (5) سنوات وبغرامة من 50.000 دج إلى 500.000 دج.

يعاقب الشخص المعنوي بالغرامة وفقا للقواعد المقررة في قانون العقوبات.

تحدد كيفيات تطبيق الفقرات 1 و2 و3 من هذه المادة، عند الحاجة، عن طريق التنظيم.

الالتزامات الخاصة بمقدمي خدمة "الإنترنت"

المادّة 12 : زيادة على الالتزامات المنصوص عليها في المادة 11 أعلاه، يتعين على مقدمي خدمات "الإنترنت" ما يأتي :

أ – التدخل الفوري لسحب المحتويات التي يتيحون الاطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن،

ب – وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام أو الآداب العامة وإخبار المشتركين لديهم بوجودها.

الفصل الخامس

الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته

إنشاء الهيئة

المادّة 13 : تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

تحدد تشكيلة الهيئة وتنظيمها وكيفيات سيرها عن طريق التنظيم.

مهام الهيئة

المادّة 14 : تتولى الهيئة المذكورة في المادة 13 أعلاه، خصوصا المهام الآتية :

أ – تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته،

ب – مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية،

ج – تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم.

الفصل السادس

التعاون والمساعدة القضائية الدولية

الاختصاص القضائي

المادّة 15 : زيادة على قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية، تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني، عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني.

المساعدة القضائية الدولية المتبادلة

المادّة 16 : في إطار التحريات أو التحقيقات القضائية الجارية لمعاينة الجرائم المشمولة بهذا القانون وكشف مرتكبيها، يمكن السلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني.

يمكن، في حالة الاستعجال، ومع مراعاة الاتفاقيات الدولية ومبدأ المعاملة بالمثل، قبول طلبات المساعدة القضائية المذكورة في الفقرة الأولى أعلاه، إذا وردت عن طريق وسائل الاتصال السريعة بما في ذلك أجهزة الفاكس أوالبريد الإلكتروني وذلك بقدر ما توفره هذه الوسائل من شروط أمن كافية للتأكد من صحتها.

تبادل المعلومات واتخاذ الإجراءات التحفظية

المادّة 17 : تتم الاستجابة لطلبات المساعدة الرامية لتبادل المعلومات أو اتخاذ أي إجراءات تحفظية وفقا للاتفاقيات الدولية ذات الصلة والاتفاقات الدولية الثنائية ومبدأ المعاملة بالمثل.

القيود الواردة على طلبات المساعدة القضائية الدولية

المادّة 18 : يرفض تنفيذ طلبات المساعدة إذا كان من شأنها المساس بالسيادة الوطنية أو النظام العام.

يمكن أن تكون الاستجابة لطلبات المساعدة مقيدة بشرط المحافظة على سرية المعلومات المبلغة أو بشرط عدم استعمالها في غير ما هو موضح في الطلب.

المادّة 19 : ينشر هذا القانون في الجريدة الرّسميّة للجمهوريّة الجزائريّة الدّيمقراطيّة الشّعبيّة.

حرّر بالجزائر في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009.

عبد العزيز بوتفليقة

LOIS

Loi n° 09-04 du 14 Chaâbane 1430 correspondant au 5 août 2009 portant règles particulières relatives à la prévention et à la lutte contre les infractions liées aux technologies de l'information et de la communication.

———

Le Président de la République,

Vu la Constitution, notamment ses articles 119, 120, 122-7° et 126 ;

Vu l'ordonnance n° 66-155 du 8 juin 1966, modifiée et complétée, portant code de procédure pénale ;

Vu l'ordonnance n° 66-156 du 8 juin 1966, modifiée et complétée, portant code pénal ;

Vu l'ordonnance n° 75-58 du 26 septembre 1975, modifiée et complétée, portant code civil ;

Vu la loi n° 2000-03 du 5 Joumada El Oula 1421 correspondant au 5 août 2000, modifiée et complétée, fixant les règles générales relatives à la poste et aux télécommunications ;

Vu l'ordonnance n° 03-05 du 19 Joumada El Oula 1424 correspondant au 19 juillet 2003 relative aux droits d'auteur et aux droits voisins ;

Vu la loi n° 08-09 du 18 Safar 1429 correspondant au 25 février 2008 portant code de procédure civile et administrative ;

Après avis du Conseil d'Etat,

Après adoption par le Parlement,

Promulgue la loi dont la teneur suit :

CHAPITRE I

DISPOSITIONS GENERALES

Objet

Article 1er. — La présente loi vise à mettre en place des règles particulières de prévention et de lutte contre les infractions liées aux technologies de l'information et de la communication.

Terminologie

Art. 2. — Au sens de la présente loi, on entend par :

a - **Infractions liées aux technologies de l'information et de la communication** : les infractions portant atteinte aux systèmes de traitement automatisé de données telles que définies par le code pénal ainsi que toute autre infraction commise ou dont la commission est facilitée par un système informatique ou un système de communication électronique.

b - **Système informatique** : tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données.

c - **Données informatiques** : 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.

d - **Fournisseurs de services** :

1 - toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique et/ou d'un système de télécommunication ;

2 - et toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs.

e - **Données relatives au trafic** : toute donnée ayant trait à une communication passant par un système informatique, produite par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ainsi que le type de service.

f - **Communications électroniques** : toute transmission, émission ou réception de signes, de signaux, d'écrits, d'images, de sons ou de renseignements de toute nature, par tout moyen électronique.

CHAMP D'APPLICATION

Art. 3. — Conformément aux règles prévues par le code de procédure pénale et par la présente loi et sous réserve des dispositions légales garantissant le secret des correspondances et des communications, il peut être procédé, pour des impératifs de protection de l'ordre public ou pour les besoins des enquêtes ou des

informations judiciaires en cours, à la mise en place de dispositifs techniques pour effectuer des opérations de surveillance des communications électroniques, de collecte et d'enregistrement en temps réel de leur contenu ainsi qu'à des perquisitions et des saisies dans un système informatique.

CHAPITRE II

SURVEILLANCE DES COMMUNICATIONS ELECTRONIQUES

Cas autorisant le recours à la surveillance électronique

Art. 4. — Les opérations de surveillance prévues par l'article 3 ci-dessus peuvent être effectuées dans les cas suivants :

a) pour prévenir les infractions qualifiées d'actes terroristes ou subversifs et les infractions contre la sûreté de l'Etat.

b) lorsqu' il existe des informations sur une atteinte probable à un système informatique représentant une menace pour l'ordre public, la défense nationale, les institutions de l'Etat ou l'économie nationale ;

c) pour les besoins des enquêtes et des informations judiciaires lorsqu'il est difficile d'aboutir à des résultats intéressant les recherches en cours sans recourir à la surveillance électronique ;

d) dans le cadre de l'exécution des demandes d'entraide judiciaire internationale.

Les opérations de surveillance ci-dessus mentionnées ne peuvent être effectuées que sur autorisation écrite de l'autorité judiciaire compétente.

Lorsqu'il s'agit du cas prévu au paragraphe (a) du présent article, l'autorisation est délivrée aux officiers de police judiciaire relevant de l'organe visé à l'article 13 ci-après, par le procureur général près la Cour d'Alger, pour une durée de six (6) mois renouvelable, sur la base d'un rapport indiquant la nature du procédé technique utilisé et les objectifs qu'il vise.

Sous peine des sanctions prévues par le code pénal en matière d'atteinte à la vie privée d'autrui, les dispositifs techniques mis en place aux fins désignées au paragraphe (a) du présent article doivent être orientés, exclusivement, vers la collecte et l'enregistrement de données en rapport avec la prévention et la lutte contre les actes terroristes et les atteintes à la sûreté de l'Etat.

CHAPITRE III

REGLES DE PROCEDURE

Perquisition des systèmes informatiques

Art. 5. — Les autorités judiciaires compétentes ainsi que les officiers de police judiciaire, agissant dans le cadre du code de procédure pénale et dans les cas prévus par l'article 4 ci-dessus, peuvent, aux fins de perquisition, accéder, y compris à distance :

a) à un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui y sont stockées ;

b) à un système de stockage informatique.

Lorsque, dans le cas prévu par le paragraphe (a) du présent article, l'autorité effectuant la perquisition a des raisons de croire que les données recherchées sont stockées dans un autre système informatique et que ces données sont accessibles à partir du système initial, elle peut étendre, rapidement, la perquisition au système en question ou à une partie de celui-ci après information préalable de l'autorité judiciaire compétente.

S'il est préalablement avéré que les données recherchées, accessibles au moyen du premier système, sont stockées dans un autre système informatique situé en dehors du territoire national, leur obtention se fait avec le concours des autorités étrangères compétentes conformément aux accords internationaux pertinents et suivant le principe de la réciprocité.

Les autorités en charge de la perquisition sont habilitées à réquisitionner toute personne connaissant le fonctionnement du système informatique en question ou les mesures appliquées pour protéger les données informatiques qu'il contient, afin de les assister et leur fournir toutes les informations nécessaires à l'accomplissement de leur mission.

Saisie de données informatiques

Art. 6. — Lorsque l'autorité effectuant la perquisition découvre, dans un système informatique, des données stockées qui sont utiles à la recherche des infractions ou leurs auteurs, et que la saisie de l'intégralité du système n'est pas nécessaire, les données en question de même que celles qui sont nécessaires à leur compréhension, sont copiées sur des supports de stockage informatique pouvant être saisis et placés sous scellés dans les conditions prévues par le code de procédure pénale.

L'autorité effectuant la perquisition et la saisie doit, en tout état de cause, veiller à l'intégrité des données du système informatique en question.

Toutefois, elle peut employer les moyens techniques requis pour mettre en forme ou reconstituer ces données en vue de les rendre exploitables pour les besoins de l'enquête, à la condition que cette reconstitution ou mise en forme des données n'en altère pas le contenu.

Saisie par l'interdiction d'accès aux données

Art. 7. — Si, pour des raisons techniques, l'autorité effectuant la perquisition se trouve dans l'impossibilité de procéder à la saisie conformément à l'article 6 ci-dessus, elle doit utiliser les techniques adéquates pour empêcher l'accès aux données contenues dans le système informatique ou aux copies de ces données qui sont à la disposition des personnes autorisées à utiliser ce système.

Données saisies au contenu incriminé

Art. 8. — L'autorité ayant procédé à la perquisition peut ordonner les mesures nécessaires pour rendre inaccessible les données dont le contenu constitue une infraction, notamment en désignant toute personne qualifiée pour employer les moyens techniques appropriés à cet effet.

Limites à l'utilisation des données collectées

Art. 9. — Sous peine de sanctions édictées par la législation en vigueur, les données obtenues au moyen des opérations de surveillance prévues à la présente loi ne peuvent être utilisées à des fins autres que les enquêtes et les informations judiciaires.

CHAPITRE IV
OBLIGATIONS DES FOURNISSEURS DE SERVICES

Assistance aux autorités

Art. 10. — Dans le cadre de l'application des dispositions de la présente loi, les fournisseurs de services sont tenus de prêter leur assistance aux autorités chargées des enquêtes judiciaires pour la collecte ou l'enregistrement, en temps réel, des données relatives au contenu des communications et de mettre à leur disposition les données qu'ils sont tenus de conserver en vertu de l'article 11 ci-dessous.

Sous peine des sanctions prévues en matière de violation du secret de l'enquête et de l'instruction, les fournisseurs de services sont tenus de garder la confidentialité des opérations qu'ils effectuent sur réquisition des enquêteurs et les informations qui s'y rapportent.

Conservation des données relatives au trafic

Art. 11. — Selon la nature et les types de services, les fournisseurs de services s'engagent à conserver :

a) les données permettant l'identification des utilisateurs du service ;

b) les données relatives aux équipements terminaux des communications utilisées ;

c) les caractéristiques techniques ainsi que la date, le temps et la durée de chaque communication ;

d) les données relatives aux services complémentaires requis ou utilisés et leurs fournisseurs ;

e) les données permettant d'identifier le ou les destinataires de la communication ainsi que les adresses des sites visités.

Pour les activités de téléphonie, l'opérateur conserve les données citées au paragraphe (a) du présent article et celles permettant d'identifier et de localiser l'origine de la communication.

La durée de conservation des données citées au présent article est fixée à une (1) année à compter du jour de l'enregistrement.

Sans préjudice des sanctions administratives découlant du non-respect des obligations prévues par le présent article, la responsabilité pénale des personnes physiques et morales est engagée lorsque cela a eu pour conséquence d'entraver le bon déroulement des enquêtes judiciaires. La peine encourue par la personne physique est l'emprisonnement de six (6) mois à cinq (5) ans et l'amende de 50.000 DA à 500.000 DA.

La personne morale encourt la peine d'amende suivant les modalités prévues par le code pénal.

Les modalités d'application des alinéas 1, 2 et 3 du présent article sont, en tant que de besoin, précisées par voie réglementaire.

Obligations des fournisseurs d'accès à internet

Art. 12. — Outre les obligations prévues par l'article 11 ci-dessus, les fournisseurs d'accès à internet sont tenus :

a) d'intervenir, sans délai, pour retirer les contenus dont ils autorisent l'accès en cas d'infraction aux lois, les stocker ou les rendre inaccessibles dès qu'ils en ont pris connaissance directement ou indirectement ;

b) de mettre en place des dispositifs techniques permettant de limiter l'accessibilité aux distributeurs contenant des informations contraires à l'ordre public ou aux bonnes mœurs et en informer les abonnés.

CHAPITRE V

ORGANE NATIONAL DE PREVENTION ET DE LUTTE CONTRE LES INFRACTIONS LIEES AUX TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Création de l'organe

Art. 13. — Il est créé un organe national de prévention et de lutte contre la criminalité liée aux technologies de l'information et de la communication.

La composition, l'organisation et les modalités de fonctionnement de l'organe sont fixées par voie réglementaire.

Missions de l'organe

Art. 14. — L'organe visé à l'article 13 ci-dessus est chargé notamment de :

a) la dynamisation et la coordination des opérations de prévention et de lutte contre la criminalité liée aux technologies de l'information et de la communication ;

b) l'assistance des autorités judiciaires et des services de police judiciaire en matière de lutte contre la criminalité liée aux technologies de l'information et de la communication, y compris à travers la collecte de l'information et les expertises judiciaires ;

c) l'échange d'informations avec ses interfaces à l'étranger aux fins de réunir toutes données utiles à la localisation et à l'identification des auteurs des infractions liées aux technologies de l'information et de la communication.

CHAPITRE VI

LA COOPERATION ET L'ENTRAIDE JUDICIAIRE INTERNATIONALES

Compétence judiciaire

Art. 15. — Outre les règles de compétence prévues par le code de procédure pénale, les juridictions algériennes sont compétentes pour connaître des infractions liées aux technologies de l'information et de la communication commises en dehors du territoire national, lorsque leur auteur est un étranger et qu'elles ont pour cible les institutions de l'Etat algérien, la défense nationale ou les intérêts stratégiques de l'économie nationale.

Entraide judiciaire internationale

Art. 16. — Dans le cadre des investigations ou des informations judiciaires menées pour la constatation des infractions comprises dans le champ d'application de la présente loi et la recherche de leurs auteurs, les autorités compétentes peuvent recourir à l'entraide judiciaire internationale pour recueillir des preuves sous forme électronique.

En cas d'urgence, et sous réserve des conventions internationales et du principe de réciprocité, les demandes d'entraide judiciaire visées à l'alinéa précédent sont recevables si elles sont formulées par des moyens rapides de communication, tels que la télécopie ou le courrier électronique pour autant que ces moyens offrent des conditions suffisantes de sécurité et d'authentification.

Echange d'informations et les mesures conservatoires

Art. 17. — Les demandes d'entraide tendant à l'échange d'informations ou à prendre toute mesure conservatoire sont satisfaites conformément aux conventions internationales pertinentes, aux accords bilatéraux et en application du principe de réciprocité.

Restrictions aux demandes d'entraide internationale

Art. 18. — L'exécution de la demande d'entraide est refusée si elle est de nature à porter atteinte à la souveraineté nationale ou à l'ordre public.

La satisfaction des demandes d'entraide peut être subordonnée à la condition de conserver la confidentialité des informations communiquées ou à la condition de ne pas les utiliser à des fins autres que celles indiquées dans la demande.

Art. 19. — La présente loi sera publiée au *Journal officiel* de la République algérienne démocratique et populaire.

Fait à Alger, le 14 Chaâbane 1430 correspondant au 5 août 2009

Abdelaziz BOUTEFLIKA.

ملحق رقم : 4

القانون رقم 88-19 لـــ 5 جانفي 1988 المتعلق بالغش المعلوماتي

الجريدة الرسمية لـــ 6 جانفي 1988

Loi n° 88-19 du 5 Janvier 1988 relative à la fraude informatique, dite "loi Godfrain"

Journal officiel du 6 janvier 1988

L'Assemblée nationale et le Sénat ont adopté.
Le Président de la République promulgue la loi dont la teneur suit:

Article unique
Dans le titre II du livre III du code pénal, il est inséré, après le chapitre II, un chapitre III ainsi rédigé :

Chapitre III
De certaines infractions en matière informatique

Article 462-2

Quiconque, frauduleusement, aura accédé ou se sera maintenu dans tout ou partie d'un système de traitement automatisé de données sera puni d'un emprisonnement de deux mois à un an et d'une amende de 2.000F à 50.000F ou de l'une de ces deux peines. Lorsqu'il en sera résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, l'emprisonnement sera de deux mois à deux ans et l'amende de 10.000F à 100.000F.

Article 462-3

Quiconque aura, intentionnellement et au mépris des droits d'autrui, entravé ou faussé le fonctionnement d'un système de traitement automatisé de données sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 10.000F à 100.000F ou de l'une de ces deux peines.

Article 462-4

Quiconque aura, intentionnellement et au mépris des droits d'autrui, directement ou indirectement, introduit des données dans un système de traitement automatisé ou supprimé ou modifié les données qu'il contient ou leurs modes de traitement ou de transmission, sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 2.000F à 500.000F ou de l'une de ces deux peines.

Article 462-5

Quiconque aura procédé à la falsification de documents informatisés, quelle que soit leur forme, de nature à causer un préjudice à autrui, sera puni d'un emprisonnement d'un an à cinq ans et d'une amende de 20.000F à 2.000.000F.

Article 462-6

Quiconque aura sciemment fait usage des documents informatisés visés à l'article 462-5 sera puni d'un emprisonnement d'un an à cinq ans et d'une amende de 20.000F à 2.000.000F ou de l'une de ces deux peines.

Article 462-7

La tentative des délits prévus par les articles 462-2 à 462-6 est punie des mêmes peines que le délit lui-même.

Article 462-8

Quiconque aura participé à une association formée ou à une entente établie en vue de la préparation, concrétisée par un ou plusieurs faits matériels, d'une ou de plusieurs infractions prévues par les articles 462-2 à 462-6 sera puni des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Article 462-9

Le tribunal pourra prononcer la confiscation des matériels appartenant au condamné et ayant servi à commettre les infractions prévues au présent chapitre.

La présente loi sera exécutée comme loi de l'Etat.
Fait à Paris, le 5 Janvier 1988.

Par le Président de la République : François Mitterand

Le Premier ministre, Jacques Chirac

Le garde des sceaux, ministre de la justice, Albin Chalandon

ملحق رقم : 5

قانون رقم 78-17 لـــ 6 جانفي 1978 المتعلق بالمعلوماتية، المعطيات و الحريات المعدل بموجب قانون 2009-526 لـــ 12 ماي 2009

(الجريدة الرسمية الفرنسية لـــ 13 ماي 2009)

Loi n° 78-17 du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifié par la loi n° 2009-526 du 12 mai 2009 (Journal officiel français du 13 mai 2009)

Textes modifiant la loi النصوص المعدلة للقانون :

Loi n° 88-227 du 11 mars 1988 (Journal officiel du 12 mars 1988),
Loi n° 92-1336 du 16 décembre 1992 (Journal officiel du 23 décembre 1992),
Loi n° 94-548 du ler juillet 1994 (Journal officiel du 2 juillet 1994),
Loi n° 99-641 du 27 juillet 1999, (Journal officiel du 28 juillet 1999).
Loi n° 2000-321 du 12 avril 2000, (Journal officiel du 13 avril 2000).
Loi n° 2002-303 du 4 mars 2002, (Journal officiel du 5 Mars 2002).
Loi n° 2003-239 du 18 mars 2003 (Journal officiel du 19 mars 2003).
Loi n° 2004-801 du 6 août 2004 (Journal officiel du 7 août 2004)
Loi n° 2006-64 du 23 janvier 2006 (Journal officiel du 24 janvier 2006)
Loi n°2009-526 du 12 mai 2009 (Journal officiel du 13 mai 2009)

Articles :

****

Loi n° 78-17 du 6 janvier 1978
relative à l'informatique, aux fichiers et aux libertés

L'Assemblée nationale et le Sénat ont adopté.
Le Président de la République promulgue la loi dont la teneur suit :

CHAPITRE Ier - PRINCIPES ET DÉFINITIONS

Article 1er

L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

Article 2

La présente loi s’applique aux traitements automatisés de données à caractère personnel, ainsi qu’aux traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans des fichiers, à l’exception des traitements mis en oeuvre pour l’exercice d’activités exclusivement personnelles, lorsque leur responsable remplit les conditions prévues à l’article 5.
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.
Constitue un traitement de données à caractère personnel toute opération ou tout ensemble d’opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l’enregistrement, l’organisation, la conservation, l’adaptation ou la modification, l’extraction, la consultation, l’utilisation, la communication par transmission, diffusion ou toute

autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.
Constitue un fichier de données à caractère personnel tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés.
La personne concernée par un traitement de données à caractère personnel est celle à laquelle se rapportent les données qui font l'objet du traitement.

Article 3

I. - Le responsable d'un traitement de données à caractère personnel est, sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens.
II. - Le destinataire d'un traitement de données à caractère personnel est toute personne habilitée à recevoir communication de ces données autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, en raison de leurs fonctions, sont chargées de traiter les données. Toutefois, les autorités légalement habilitées, dans le cadre d'une mission particulière ou de l'exercice d'un droit de communication, à demander au responsable du traitement de leur communiquer des données à caractère personnel ne constituent pas des destinataires.

Article 4

Les dispositions de la présente loi ne sont pas applicables aux copies temporaires qui sont faites dans le cadre des activités techniques de transmission et de fourniture d'accès à un réseau numérique, en vue du stockage automatique, intermédiaire et transitoire des données et à seule fin de permettre à d'autres destinataires du service le meilleur accès possible aux informations transmises.

Article 5

I. - Sont soumis à la présente loi les traitements de données à caractère personnel :

1° Dont le responsable est établi sur le territoire français. Le responsable d'un traitement qui exerce une activité sur le territoire français dans le cadre d'une installation, quelle que soit sa forme juridique, y est considéré comme établi ;

2° Dont le responsable, sans être établi sur le territoire français ou sur celui d'un autre État membre de la Communauté européenne, recourt à des moyens de traitement situés sur le territoire français, à l'exclusion des traitements qui ne sont utilisés qu'à des fins de transit sur ce territoire ou sur celui d'un autre État membre de la Communauté européenne.

II. - Pour les traitements mentionnés au 2° du I, le responsable désigne à la Commission nationale de l'informatique et des libertés un représentant établi sur le territoire français, qui se substitue à lui dans l'accomplissement des obligations prévues par la présente loi ; cette désignation ne fait pas obstacle aux actions qui pourraient être introduites contre lui.

CHAPITRE II - CONDITIONS DE LICÉITÉ DES TRAITEMENTS DE DONNÉES À CARACTÈRE PERSONNEL

Section 1 : Dispositions générales

Article 6

Un traitement ne peut porter que sur des données à caractère personnel qui satisfont aux conditions suivantes :

1° Les données sont collectées et traitées de manière loyale et licite ;

2° Elles sont collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités. Toutefois, un traitement ultérieur de données à des fins statistiques ou à des fins de recherche scientifique ou historique est considéré comme compatible avec les finalités initiales de la collecte des données, s'il est réalisé dans le respect des principes et des procédures prévus au présent chapitre, au chapitre IV et à la section 1 du chapitre V ainsi qu'aux chapitres IX et X et s'il n'est pas utilisé pour prendre des décisions à l'égard des personnes concernées ;

3° Elles sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs ;

4° Elles sont exactes, complètes et, si nécessaire, mises à jour ; les mesures appropriées doivent être prises pour que les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées soient effacées ou rectifiées ;

5° Elles sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées.

Article 7

Un traitement de données à caractère personnel doit avoir reçu le consentement de la personne concernée ou satisfaire à l'une des conditions suivantes :

1° Le respect d'une obligation légale incombant au responsable du traitement ;

2° La sauvegarde de la vie de la personne concernée ;

3° L'exécution d'une mission de service public dont est investi le responsable ou le destinataire du traitement ;

4° L'exécution, soit d'un contrat auquel la personne concernée est partie, soit de mesures précontractuelles prises à la demande de celle-ci ;

5° La réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée.

Section 2 : Dispositions propres à certaines catégories de données

Article 8

I. - Il est interdit de collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci.

II. - Dans la mesure où la finalité du traitement l'exige pour certaines catégories de données, ne sont pas soumis à l'interdiction prévue au I :

1° Les traitements pour lesquels la personne concernée a donné son consentement exprès, sauf dans le cas où la loi prévoit que l'interdiction visée au I ne peut être levée par le consentement de la personne concernée ;

2° Les traitements nécessaires à la sauvegarde de la vie humaine, mais auxquels la personne concernée ne peut donner son consentement par suite d'une incapacité juridique ou d'une impossibilité matérielle ;

3° Les traitements mis en oeuvre par une association ou tout autre organisme à but non lucratif et à caractère religieux, philosophique, politique ou syndical :

- pour les seules données mentionnées au I correspondant à l'objet de ladite association ou dudit organisme ;

- sous réserve qu'ils ne concernent que les membres de cette association ou de cet organisme et, le cas échéant, les personnes qui entretiennent avec celui-ci des contacts réguliers dans le cadre de son activité ;

- et qu'ils ne portent que sur des données non communiquées à des tiers, à moins que les personnes concernées n'y consentent expressément ;

4° Les traitements portant sur des données à caractère personnel rendues publiques par la personne concernée ;

5° Les traitements nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice ;

6° Les traitements nécessaires aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de services de santé et mis en oeuvre par un membre d'une profession de santé, ou par une autre personne à laquelle s'impose en raison de ses fonctions l'obligation de secret professionnel prévue par l'article 226-13 du code pénal ;

7° Les traitements statistiques réalisés par l'Institut national de la statistique et des études économiques ou l'un des services statistiques ministériels dans le respect de la loi n° 51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques, après avis du Conseil national de l'information statistique et dans les conditions prévues à l'article 25 de la présente loi ;

8° Les traitements nécessaires à la recherche dans le domaine de la santé selon les modalités prévues au chapitre IX.

III. - Si les données à caractère personnel visées au I sont appelées à faire l'objet à bref délai d'un procédé d'anonymisation préalablement reconnu conforme aux dispositions de la présente loi par la Commission nationale de l'informatique et des libertés, celle-ci peut autoriser, compte tenu de leur finalité, certaines catégories de traitements selon les modalités prévues à l'article 25. Les dispositions des chapitres IX et X ne sont pas applicables.

IV. - De même, ne sont pas soumis à l'interdiction prévue au I les traitements, automatisés ou non, justifiés par l'intérêt public et autorisés dans les conditions prévues au I de l'article 25 ou au II de l'article 26.

Article 9

Les traitements de données à caractère personnel relatives aux infractions, condamnations et mesures de sûreté ne peuvent être mis en oeuvre que par :

1° Les juridictions, les autorités publiques et les personnes morales gérant un service public, agissant dans le cadre de leurs attributions légales ;

2° Les auxiliaires de justice, pour les stricts besoins de l'exercice des missions qui leur sont confiées par la loi ;

3° [Dispositions déclarées non conformes à la Constitution par décision du Conseil constitutionnel n° 2004-499 DC du 29 juillet 2004 ;]

4° Les personnes morales mentionnées aux articles L. 321-1 et L. 331-1 du code de la propriété intellectuelle, agissant au titre des droits dont elles assurent la gestion ou pour le compte des victimes d'atteintes aux droits prévus aux livres Ier, II et III du même code aux fins d'assurer la défense de ces droits.

Article 10

Aucune décision de justice impliquant une appréciation sur le comportement d'une personne ne peut avoir pour fondement un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de sa personnalité.

Aucune autre décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé de données destiné à définir le profil de l'intéressé ou à évaluer certains aspects de sa personnalité.

Ne sont pas regardées comme prises sur le seul fondement d'un traitement automatisé les décisions prises dans le cadre de la conclusion ou de l'exécution d'un contrat et pour lesquelles la personne concernée a été mise à même de présenter ses observations, ni celles satisfaisant les demandes de la personne concernée.

CHAPITRE III - LA COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS

Article 11

La Commission nationale de l'informatique et des libertés est une autorité administrative indépendante. Elle exerce les missions suivantes :
1° Elle informe toutes les personnes concernées et tous les responsables de traitements de leurs droits et obligations ;

2° Elle veille à ce que les traitements de données à caractère personnel soient mis en oeuvre conformément aux dispositions de la présente loi.
A ce titre :
a) Elle autorise les traitements mentionnés à l'article 25, donne un avis sur les traitements mentionnés aux articles 26 et 27 et reçoit les déclarations relatives aux autres traitements ;

b) Elle établit et publie les normes mentionnées au I de l'article 24 et édicte, le cas échéant, des règlements types en vue d'assurer la sécurité des systèmes ;

c) Elle reçoit les réclamations, pétitions et plaintes relatives à la mise en oeuvre des traitements de données à caractère personnel et informe leurs auteurs des suites données à celles-ci ;

d) Elle répond aux demandes d'avis des pouvoirs publics et, le cas échéant, des juridictions, et conseille les personnes et organismes qui mettent en oeuvre ou envisagent de mettre en oeuvre des traitements automatisés de données à caractère personnel ;

e) Elle informe sans délai le procureur de la République, conformément à l'article 40 du code de procédure pénale, des infractions dont elle a connaissance, et peut présenter des observations dans les procédures pénales, dans les conditions prévues à l'article 52 ;
f) Elle peut, par décision particulière, charger un ou plusieurs de ses membres ou des agents de ses services, dans les conditions prévues à l'article 44, de procéder à des vérifications portant sur tous traitements et, le cas échéant, d'obtenir des copies de tous documents ou supports d'information utiles à ses missions ;

g) Elle peut, dans les conditions définies au chapitre VII, prononcer à l'égard d'un responsable de traitement l'une des mesures prévues à l'article 45 ;

h) Elle répond aux demandes d'accès concernant les traitements mentionnés aux articles 41 et 42 ;
3° A la demande d'organisations professionnelles ou d'institutions regroupant principalement des responsables de traitements :
a) Elle donne un avis sur la conformité aux dispositions de la présente loi des projets de règles professionnelles et des produits et procédures tendant à la protection des personnes à l'égard du traitement de données à caractère personnel, ou à l'anonymisation de ces données, qui lui sont soumis ;

b) Elle porte une appréciation sur les garanties offertes par des règles professionnelles qu'elle a précédemment reconnues conformes aux dispositions de la présente loi, au regard du respect des droits fondamentaux des personnes ;

c) Elle délivre un label à des produits ou à des procédures tendant à la protection des personnes à l'égard du traitement des données à caractère personnel, après qu'elles les a reconnus conformes aux dispositions de la présente loi ; dans le cadre de l'instruction préalable à la délivrance du label par la commission, le président peut, lorsque la complexité du produit ou de la procédure le justifie, recourir à toute personne indépendante qualifiée pour procéder à leur évaluation. Le coût de cette évaluation est pris en charge par l'entreprise qui demande le label ;
4° Elle se tient informée de l'évolution des technologies de l'information et rend publique le cas échéant son appréciation des conséquences qui en résultent pour l'exercice des droits et libertés mentionnés à l'article 1er ;
A ce titre :
a) Elle est consultée sur tout projet de loi ou de décret relatif à la protection des personnes à l'égard des traitements automatisés. A la demande du président de l'une des commissions permanentes prévue à l'article 43 de la Constitution, l'avis de la commission sur tout projet de loi est rendu public ;

b) Elle propose au Gouvernement les mesures législatives ou réglementaires d'adaptation de la protection des libertés à l'évolution des procédés et techniques informatiques ;

c) A la demande d'autres autorités administratives indépendantes, elle peut apporter son concours en matière de protection des données ;

d) Elle peut être associée, à la demande du Premier ministre, à la préparation et à la définition de la position française dans les négociations internationales dans le domaine de la protection des données à caractère personnel. Elle peut participer, à la demande du Premier ministre, à la représentation française dans les organisations internationales et communautaires compétentes en ce domaine.
Pour l'accomplissement de ses missions, la commission peut procéder par voie de recommandation et prendre des décisions individuelles ou réglementaires dans les cas prévus par la présente loi.

La commission présente chaque année au Président de la République, au Premier ministre et au Parlement un rapport public rendant compte de l'exécution de sa mission.

Article 12

La Commission nationale de l'informatique et des libertés dispose des crédits nécessaires à l'accomplissement de ses missions. Les dispositions de la loi du 10 août 1922 relative au contrôle financier ne sont pas applicables à leur gestion. Les comptes de la commission sont présentés au contrôle de la Cour des comptes.

Article 13

I. - La Commission nationale de l'informatique et des libertés est composée de dix-sept membres :
1° Deux députés et deux sénateurs, désignés respectivement par l'Assemblée nationale et par le Sénat ;

2° Deux membres du Conseil économique et social, élus par cette assemblée ;

3° Deux membres ou anciens membres du Conseil d'État, d'un grade au moins égal à celui de conseiller, élus par l'assemblée générale du Conseil d'État ;

4° Deux membres ou anciens membres de la Cour de cassation, d'un grade au moins égal à celui de conseiller, élus par l'assemblée générale de la Cour de cassation ;
5° Deux membres ou anciens membres de la Cour des comptes, d'un grade au moins égal à celui de conseiller maître, élus par l'assemblée générale de la Cour des comptes ;

6° Trois personnalités qualifiées pour leur connaissance de l'informatique ou des questions touchant aux libertés individuelles, nommées par décret ;

7° Deux personnalités qualifiées pour leur connaissance de l'informatique, désignées respectivement par le Président de l'Assemblée nationale et par le Président du Sénat.
La commission élit en son sein un président et deux vice-présidents, dont un vice-président délégué. Ils composent le bureau.

La formation restreinte de la commission est composée du président, des vice-présidents et de trois membres élus par la commission en son sein pour la durée de leur mandat.

En cas de partage égal des voix, celle du président est prépondérante.

II. - Le mandat des membres de la commission mentionnés aux 3°, 4°, 5°, 6° et 7° du I est de cinq ans ; il est renouvelable une fois. Les membres mentionnés aux 1° et 2° siègent pour la durée du mandat à l'origine de leur désignation ; leurs mandats de membre de la Commission nationale de l'informatique et des libertés ne peuvent excéder une durée de dix ans.

Le membre de la commission qui cesse d'exercer ses fonctions en cours de mandat est remplacé, dans les mêmes conditions, pour la durée de son mandat restant à courir.

Sauf démission, il ne peut être mis fin aux fonctions d'un membre qu'en cas d'empêchement constaté par la commission dans les conditions qu'elle définit.

La commission établit un règlement intérieur. Ce règlement fixe les règles relatives à l'organisation et au fonctionnement de la commission. Il précise notamment les règles relatives aux délibérations, à l'instruction des dossiers et à leur présentation devant la commission, ainsi que les modalités de mise en œuvre de la procédure de labellisation prévue au c du 3° de l'article 11.

Article 14

I. - La qualité de membre de la commission est incompatible avec celle de membre du Gouvernement.

II. - Aucun membre de la commission ne peut :
- participer à une délibération ou procéder à des vérifications relatives à un organisme au sein duquel il détient un intérêt, direct ou indirect, exerce des fonctions ou détient un mandat ;
- participer à une délibération ou procéder à des vérifications relatives à un organisme au sein duquel il a, au cours des trente-six mois précédant la délibération ou les vérifications, détenu un intérêt direct ou indirect, exercé des fonctions ou détenu un mandat.
III. - Tout membre de la commission doit informer le président des intérêts directs ou indirects qu'il détient ou vient à détenir, des fonctions qu'il exerce ou vient à exercer et de tout mandat qu'il détient ou vient à détenir au sein d'une personne morale. Ces informations, ainsi que celles concernant le président, sont tenues à la disposition des membres de la commission.

Le président de la commission prend les mesures appropriées pour assurer le respect des obligations résultant du présent article.

Article 15

Sous réserve des compétences du bureau et de la formation restreinte, la commission se réunit en formation plénière.

En cas de partage égal des voix, la voix du président est prépondérante.

La commission peut charger le président ou le vice-président délégué d'exercer celles de ses attributions mentionnées :
- au troisième alinéa du I de l'article 23 ;
- aux e et f du 2° de l'article 11 ;
- au c du 2° de l'article 11 ;
- au d du 4° de l'article 11 ;
- aux articles 41 et 42 ;
- à l'article 54 ;
- aux articles 63, 64 et 65 ;
- aux deux derniers alinéas de l'article 69, à l'exception des traitements mentionnés aux I ou II de l'article 26 ;
- au premier alinéa de l'article 70.

Article 16

Le bureau peut être chargé par la commission d'exercer les attributions de celle-ci mentionnées :
- au dernier alinéa de l'article 19 ;
- à l'article 25, en cas d'urgence ;
- au second alinéa de l'article 70.

Le bureau peut aussi être chargé de prendre, en cas d'urgence, les décisions mentionnées au premier alinéa du I de l'article 45.

Article 17

La formation restreinte de la commission prononce les mesures prévues au I et au 1° du II de l'article 45.

Article 18

Un commissaire du Gouvernement, désigné par le Premier ministre, siège auprès de la commission. Des commissaires adjoints peuvent être désignés dans les mêmes conditions.

Le commissaire du Gouvernement assiste à toutes les délibérations de la commission réunie en formation plénière ou en formation restreinte, ainsi qu'à celles des réunions de son bureau qui ont pour objet l'exercice des attributions déléguées en vertu de l'article 16 ; il est rendu destinataire de tous ses avis et décisions.

Il peut, sauf en matière de sanctions, provoquer une seconde délibération, qui doit intervenir dans les dix jours de la délibération initiale.

Article 19

La commission dispose de services dirigés par le président et placés sous son autorité.

Les agents de la commission sont nommés par le président.

En cas de besoin, le vice-président délégué exerce les attributions du président.

Le secrétaire général est chargé du fonctionnement et de la coordination des services sous l'autorité du président.

Ceux des agents qui peuvent être appelés à participer à la mise en oeuvre des missions de vérification mentionnées à l'article 44 doivent y être habilités par la commission ; cette habilitation ne dispense pas de l'application des dispositions définissant les procédures autorisant l'accès aux secrets protégés par la loi.

Article 20

Les membres et les agents de la commission sont astreints au secret professionnel pour les faits, actes ou renseignements dont ils ont pu avoir connaissance en raison de leurs fonctions, dans les conditions prévues à l'article 413-10 du code pénal et, sous réserve de ce qui est nécessaire à l'établissement du rapport annuel, à l'article 226-13 du même code.

Article 21

Dans l'exercice de leurs attributions, les membres de la commission ne reçoivent d'instruction d'aucune autorité.

Les ministres, autorités publiques, dirigeants d'entreprises publiques ou privées, responsables de groupements divers et plus généralement les détenteurs ou utilisateurs de traitements ou de fichiers de données à caractère personnel ne peuvent s'opposer à l'action de la commission ou de ses membres et doivent au contraire prendre toutes mesures utiles afin de faciliter sa tâche.

Sauf dans les cas où elles sont astreintes au secret professionnel, les personnes interrogées dans le cadre des vérifications faites par la commission en application du f du 2° de l'article 11 sont tenues de fournir les renseignements demandés par celle-ci pour l'exercice de ses missions.

CHAPITRE IV - FORMALITÉS PRÉALABLES À LA MISE EN ŒUVRE DES TRAITEMENTS

Article 22

I. - A l'exception de ceux qui relèvent des dispositions prévues aux articles 25, 26 et 27 ou qui sont visés au deuxième alinéa de l'article 36, les traitements automatisés de données à caractère personnel font l'objet d'une déclaration auprès de la Commission nationale de l'informatique et des libertés.

II. - Toutefois, ne sont soumis à aucune des formalités préalables prévues au présent chapitre :
1° Les traitements ayant pour seul objet la tenue d'un registre qui, en vertu de dispositions législatives ou réglementaires, est destiné exclusivement à l'information du public et est ouvert à la consultation de celui-ci ou de toute personne justifiant d'un intérêt légitime ;

2° Les traitements mentionnés au 3° du II de l'article 8.
III. - Les traitements pour lesquels le responsable a désigné un correspondant à la protection des données à caractère personnel chargé d'assurer, d'une manière indépendante, le respect des obligations prévues dans la présente loi sont dispensés des formalités prévues aux articles 23 et 24, sauf lorsqu'un transfert de données à caractère personnel à destination d'un État non membre de la Communauté européenne est envisagé.

La désignation du correspondant est notifiée à la Commission nationale de l'informatique et des libertés. Elle est portée à la connaissance des instances représentatives du personnel.

Le correspondant est une personne bénéficiant des qualifications requises pour exercer ses missions. Il tient une liste des traitements effectués immédiatement accessible à toute personne en faisant la demande et ne peut faire l'objet d'aucune sanction de la part de l'employeur du fait de l'accomplissement de ses missions. Il peut saisir la Commission nationale de l'informatique et des libertés des difficultés qu'il rencontre dans l'exercice de ses missions.

En cas de non-respect des dispositions de la loi, le responsable du traitement est enjoint par la Commission nationale de l'informatique et des libertés de procéder aux formalités prévues aux articles 23 et 24. En cas de manquement constaté à ses devoirs, le correspondant est déchargé de ses fonctions sur demande, ou après consultation, de la Commission nationale de l'informatique et des libertés.

IV. - Le responsable d'un traitement de données à caractère personnel qui n'est soumis à aucune des formalités prévues au présent chapitre communique à toute personne qui en fait la demande les informations relatives à ce traitement mentionnées aux 2° à 6° du I de l'article 31.

Section 1 : Déclaration

Article 23

I. - La déclaration comporte l'engagement que le traitement satisfait aux exigences de la loi.

Elle peut être adressée à la Commission nationale de l'informatique et des libertés par voie électronique.

La commission délivre sans délai un récépissé, le cas échéant par voie électronique. Le demandeur peut mettre en oeuvre le traitement dès réception de ce récépissé ; il n'est exonéré d'aucune de ses responsabilités.

II. - Les traitements relevant d'un même organisme et ayant des finalités identiques ou liées entre elles peuvent faire l'objet d'une déclaration unique. Dans ce cas, les informations requises en application de l'article 30 ne sont fournies pour chacun des traitements que dans la mesure où elles lui sont propres.

Article 24

I. - Pour les catégories les plus courantes de traitements de données à caractère personnel, dont la mise en oeuvre n'est pas susceptible de porter atteinte à la vie privée ou aux libertés, la Commission nationale de l'informatique et des libertés établit et publie, après avoir reçu le cas échéant les propositions formulées par les représentants des organismes publics et privés représentatifs, des normes destinées à simplifier l'obligation de déclaration.

Ces normes précisent :
1° Les finalités des traitements faisant l'objet d'une déclaration simplifiée ;

2° Les données à caractère personnel ou catégories de données à caractère personnel traitées ;

3° La ou les catégories de personnes concernées ;

4° Les destinataires ou catégories de destinataires auxquels les données à caractère personnel sont communiquées ;

5° La durée de conservation des données à caractère personnel.

Les traitements qui correspondent à l'une de ces normes font l'objet d'une déclaration simplifiée de conformité envoyée à la commission, le cas échéant par voie électronique.
II. - La commission peut définir, parmi les catégories de traitements mentionnés au I, celles qui, compte tenu de leurs finalités, de leurs destinataires ou catégories de destinataires, des données à caractère personnel traitées, de la durée de conservation de celles-ci et des catégories de personnes concernées, sont dispensées de déclaration.

Dans les mêmes conditions, la commission peut autoriser les responsables de certaines catégories de traitements à procéder à une déclaration unique selon les dispositions du II de l'article 23.

Section 2 : Autorisation

Article 25

I. - Sont mis en oeuvre après autorisation de la Commission nationale de l'informatique et des libertés, à l'exclusion de ceux qui sont mentionnés aux articles 26 et 27 :
1° Les traitements, automatisés ou non, mentionnés au 7° du II, au III et au IV de l'article 8 ;

2° Les traitements automatisés portant sur des données génétiques, à l'exception de ceux d'entre eux qui sont mis en oeuvre par des médecins ou des biologistes et qui sont nécessaires aux fins de la médecine préventive, des diagnostics médicaux ou de l'administration de soins ou de traitements ;

3° Les traitements, automatisés ou non, portant sur des données relatives aux infractions, condamnations ou mesures de sûreté, sauf ceux qui sont mis en oeuvre par des auxiliaires de justice pour les besoins de leurs missions de défense des personnes concernées ;
4° Les traitements automatisés susceptibles, du fait de leur nature, de leur portée ou de leurs finalités, d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat en l'absence de toute disposition législative ou réglementaire ;

5° Les traitements automatisés ayant pour objet :
- l'interconnexion de fichiers relevant d'une ou de plusieurs personnes morales gérant un service public et dont les finalités correspondent à des intérêts publics différents ;
- l'interconnexion de fichiers relevant d'autres personnes et dont les finalités principales sont différentes.
6° Les traitements portant sur des données parmi lesquelles figure le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques et ceux qui requièrent une consultation de ce répertoire sans inclure le numéro d'inscription à celui-ci des personnes ;

7° Les traitements automatisés de données comportant des appréciations sur les difficultés sociales des personnes ;

8° Les traitements automatisés comportant des données biométriques nécessaires au contrôle de l'identité des personnes.
II. - Pour l'application du présent article, les traitements qui répondent à une même finalité, portent sur des catégories de données identiques et ont les mêmes destinataires ou catégories de destinataires peuvent être autorisés par une décision unique de la commission. Dans ce cas, le responsable de chaque traitement adresse à la commission un engagement de conformité de celui-ci à la description figurant dans l'autorisation.

III. - La Commission nationale de l'informatique et des libertés se prononce dans un délai de deux mois à compter de la réception de la demande. Toutefois, ce délai peut être renouvelé une fois sur décision motivée de son président. Lorsque la commission ne s'est pas prononcée dans ces délais, la demande d'autorisation est réputée rejetée.

Article 26

I. - Sont autorisés par arrêté du ou des ministres compétents, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés, les traitements de données à caractère personnel mis en oeuvre pour le compte de l'État et :
1° Qui intéressent la sûreté de l'État, la défense ou la sécurité publique ;

2° Ou qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté.
L'avis de la commission est publié avec l'arrêté autorisant le traitement.

II. - Ceux de ces traitements qui portent sur des données mentionnées au I de l'article 8 sont autorisés par décret en Conseil d'État pris après avis motivé et publié de la commission ; cet avis est publié avec le décret autorisant le traitement.

III. - Certains traitements mentionnés au I et au II peuvent être dispensés, par décret en Conseil d'État, de la publication de l'acte réglementaire qui les autorise ; pour ces traitements, est publié, en même temps que le décret autorisant la dispense de publication de l'acte, le sens de l'avis émis par la commission.

IV. - Pour l'application du présent article, les traitements qui répondent à une même finalité, portent sur des catégories de données identiques et ont les mêmes destinataires ou catégories de destinataires peuvent être autorisés par un acte réglementaire unique. Dans ce cas, le responsable de chaque traitement adresse à la commission un engagement de conformité de celui-ci à la description figurant dans l'autorisation.
Article 27
I. - Sont autorisés par décret en Conseil d'État, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés :
1° Les traitements de données à caractère personnel mis en oeuvre pour le compte de l'État, d'une personne morale de droit public ou d'une personne morale de droit privé gérant un service public, qui portent sur des données parmi lesquelles figure le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques ;

2° Les traitements de données à caractère personnel mis en oeuvre pour le compte de l'État qui portent sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes.
II. - Sont autorisés par arrêté ou, en cas de traitement opéré pour le compte d'un établissement public ou d'une personne morale de droit privé gérant un service public, par décision de l'organe délibérant chargé de leur organisation, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés :
1° Les traitements mis en oeuvre par l'État ou les personnes morales mentionnées au I qui requièrent une consultation du répertoire national d'identification des personnes physiques sans inclure le numéro d'inscription à ce répertoire ;

2° Ceux des traitements mentionnés au I :
- qui ne comportent aucune des données mentionnées au I de l'article 8 ou à l'article 9 ;
- qui ne donnent pas lieu à une interconnexion entre des traitements ou fichiers correspondant à des intérêts publics différents ;

- et qui sont mis en oeuvre par des services ayant pour mission, soit de déterminer les conditions d'ouverture ou l'étendue d'un droit des administrés, soit d'établir l'assiette, de contrôler ou de recouvrer des impositions ou taxes de toute nature, soit d'établir des statistiques ;
3° Les traitements relatifs au recensement de la population, en métropole et dans les collectivités situées outre-mer ;
4° Les traitements mis en oeuvre par l'État ou les personnes morales mentionnées au I aux fins de mettre à la disposition des usagers de l'administration un ou plusieurs téléservices de l'administration électronique, si ces traitements portent sur des données parmi lesquelles figurent le numéro d'inscription des personnes au répertoire national d'identification ou tout autre identifiant des personnes physiques.
III. - Les dispositions du IV de l'article 26 sont applicables aux traitements relevant du présent article.

Article 28

I. - La Commission nationale de l'informatique et des libertés, saisie dans le cadre des articles 26 ou 27, se prononce dans un délai de deux mois à compter de la réception de la demande. Toutefois, ce délai peut être renouvelé une fois sur décision motivée du président.

II. - L'avis demandé à la commission sur un traitement, qui n'est pas rendu à l'expiration du délai prévu au I, est réputé favorable.

Article 29

Les actes autorisant la création d'un traitement en application des articles 25, 26 et 27 précisent :
1° La dénomination et la finalité du traitement ;

2° Le service auprès duquel s'exerce le droit d'accès défini au chapitre VII ;

3° Les catégories de données à caractère personnel enregistrées ;

4° Les destinataires ou catégories de destinataires habilités à recevoir communication de ces données ;

5° Le cas échéant, les dérogations à l'obligation d'information prévues au V de l'article 32.

Section 3 : Dispositions communes

Article 30

Modifié par Loi n°2006-64 du 23 janvier 2006 art. 13 (JORF 24 janvier 2006)
I. - Les déclarations, demandes d'autorisation et demandes d'avis adressées à la Commission nationale de l'informatique et des libertés en vertu des dispositions des sections 1 et 2 précisent :
1° L'identité et l'adresse du responsable du traitement ou, si celui-ci n'est établi ni sur le territoire national ni sur celui d'un autre État membre de la Communauté européenne, celle de son représentant et, le cas échéant, celle de la personne qui présente la demande ;

2° La ou les finalités du traitement, ainsi que, pour les traitements relevant des articles 25, 26 et 27, la description générale de ses fonctions ;

3° Le cas échéant, les interconnexions, les rapprochements ou toutes autres formes de mise en relation avec d'autres traitements ;

4° Les données à caractère personnel traitées, leur origine et les catégories de personnes concernées par le traitement ;

5° La durée de conservation des informations traitées ;

6° Le ou les services chargés de mettre en oeuvre le traitement ainsi que, pour les traitements relevant des articles 25, 26 et 27, les catégories de personnes qui, en raison de leurs fonctions ou pour les besoins du service, ont directement accès aux données enregistrées ;

7° Les destinataires ou catégories de destinataires habilités à recevoir communication des données ;

8° La fonction de la personne ou le service auprès duquel s'exerce le droit d'accès prévu à l'article 39, ainsi que les mesures relatives à l'exercice de ce droit ;

9° Les dispositions prises pour assurer la sécurité des traitements et des données et la garantie des secrets protégés par la loi et, le cas échéant, l'indication du recours à un sous-traitant ;

10° Le cas échéant, les transferts de données à caractère personnel envisagés à destination d'un État non membre de la Communauté européenne, sous quelque forme que ce soit, à l'exclusion des traitements qui ne sont utilisés qu'à des fins de transit sur le territoire français ou sur celui d'un autre État membre de la Communauté européenne au sens des dispositions du 2° du I de l'article 5.
Les demandes d'avis portant sur les traitements intéressant la sûreté de l'Etat, la défense ou la sécurité publique peuvent ne pas comporter tous les éléments d'information énumérés ci-dessus. Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, fixe la liste de ces traitements et des informations que les demandes d'avis portant sur ces traitements doivent comporter au minimum.
II. - Le responsable d'un traitement déjà déclaré ou autorisé informe sans délai la commission :
- de tout changement affectant les informations mentionnées au I ;
- de toute suppression du traitement.

Article 31

I. - La commission met à la disposition du public la liste des traitements automatisés ayant fait l'objet d'une des formalités prévues par les articles 23 à 27, à l'exception de ceux mentionnés au III de l'article 26.

Cette liste précise pour chacun de ces traitements :
1° L'acte décidant la création du traitement ou la date de la déclaration de ce traitement ;

2° La dénomination et la finalité du traitement ;

3° L'identité et l'adresse du responsable du traitement ou, si celui-ci n'est établi ni sur le territoire national ni sur celui d'un autre État membre de la Communauté européenne, celles de son représentant ;

4° La fonction de la personne ou le service auprès duquel s'exerce le droit d'accès prévu à l'article 39 ;

5° Les catégories de données à caractère personnel faisant l'objet du traitement, ainsi que les destinataires et catégories de destinataires habilités à en recevoir communication ;

6° Le cas échéant, les transferts de données à caractère personnel envisagés à destination d'un État non membre de la Communauté européenne.
II. - La commission tient à la disposition du public ses avis, décisions ou recommandations.

III. - La Commission nationale de l'informatique et des libertés publie la liste des États dont la Commission des Communautés européennes a établi qu'ils assurent un niveau de protection suffisant à l'égard d'un transfert ou d'une catégorie de transferts de données à caractère personnel.

CHAPITRE V - OBLIGATIONS INCOMBANT AUX RESPONSABLES DE TRAITEMENTS ET DROITS DES PERSONNES

Section 1 : Obligations incombant aux responsables de traitements

Article 32

I. - La personne auprès de laquelle sont recueillies des données à caractère personnel la concernant est informée, sauf si elle l'a été au préalable, par le responsable du traitement ou son représentant :
1° De l'identité du responsable du traitement et, le cas échéant, de celle de son représentant ;

2° De la finalité poursuivie par le traitement auquel les données sont destinées ;

3° Du caractère obligatoire ou facultatif des réponses ;

4° Des conséquences éventuelles, à son égard, d'un défaut de réponse ;

5° Des destinataires ou catégories de destinataires des données ;

6° Des droits qu'elle tient des dispositions de la section 2 du présent chapitre ;

7° Le cas échéant, des transferts de données à caractère personnel envisagés à destination d'un État non membre de la Communauté européenne.
Lorsque de telles données sont recueillies par voie de questionnaires, ceux-ci doivent porter mention des prescriptions figurant aux 1°, 2°, 3° et 6°.

II. - Toute personne utilisatrice des réseaux de communications électroniques doit être informée de manière claire et complète par le responsable du traitement ou son représentant :
- de la finalité de toute action tendant à accéder, par voie de transmission électronique, à des informations stockées dans son équipement terminal de connexion, ou à inscrire, par la même voie, des informations dans son équipement terminal de connexion ;

- des moyens dont elle dispose pour s'y opposer.
Ces dispositions ne sont pas applicables si l'accès aux informations stockées dans l'équipement terminal de l'utilisateur ou l'inscription d'informations dans l'équipement terminal de l'utilisateur :
- soit a pour finalité exclusive de permettre ou faciliter la communication par voie électronique ;
- soit est strictement nécessaire à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur.
III. - Lorsque les données à caractère personnel n'ont pas été recueillies auprès de la personne concernée, le responsable du traitement ou son représentant doit fournir à cette dernière les informations énumérées au I dès l'enregistrement des données ou, si une communication des données à des tiers est envisagée, au plus tard lors de la première communication des données.

Lorsque les données à caractère personnel ont été initialement recueillies pour un autre objet, les dispositions de l'alinéa précédent ne s'appliquent pas aux traitements nécessaires à la conservation de ces données à des fins historiques, statistiques ou scientifiques, dans les conditions prévues au livre II du code du patrimoine ou à la réutilisation de ces données à des fins statistiques dans les conditions de l'article 7 bis de la loi n° 51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques. Ces dispositions ne s'appliquent pas non plus lorsque la personne concernée est déjà informée ou quand son information se révèle impossible ou exige des efforts disproportionnés par rapport à l'intérêt de la démarche.

IV. - Si les données à caractère personnel recueillies sont appelées à faire l'objet à bref délai d'un procédé d'anonymisation préalablement reconnu conforme aux dispositions de la présente loi par la Commission nationale de l'informatique et des libertés, les informations délivrées par le responsable du traitement à la personne concernée peuvent se limiter à celles mentionnées au 1° et au 2° du I.

V. - Les dispositions du I ne s'appliquent pas aux données recueillies dans les conditions prévues au III et utilisées lors d'un traitement mis en oeuvre pour le compte de l'Etat et intéressant la sûreté de l'État, la défense, la sécurité publique ou ayant pour objet l'exécution de condamnations pénales ou de mesures de sûreté, dans la mesure où une telle limitation est nécessaire au respect des fins poursuivies par le traitement.

VI. - Les dispositions du présent article ne s'appliquent pas aux traitements de données ayant pour objet la prévention, la recherche, la constatation ou la poursuite d'infractions pénales.

Article 33

Sauf consentement exprès de la personne concernée, les données à caractère personnel recueillies par les prestataires de services de certification électronique pour les besoins de la délivrance et de la conservation des certificats liés aux signatures électroniques doivent l'être directement auprès de la personne concernée et ne peuvent être traitées que pour les fins en vue desquelles elles ont été recueillies.

Article 34

Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

Des décrets, pris après avis de la Commission nationale de l'informatique et des libertés, peuvent fixer les prescriptions techniques auxquelles doivent se conformer les traitements mentionnés au 2° et au 6° du II de l'article 8.

Article 35

Les données à caractère personnel ne peuvent faire l'objet d'une opération de traitement de la part d'un sous-traitant, d'une personne agissant sous l'autorité du responsable du traitement ou de celle du sous-traitant, que sur instruction du responsable du traitement.

Toute personne traitant des données à caractère personnel pour le compte du responsable du traitement est considérée comme un sous-traitant au sens de la présente loi.

Le sous-traitant doit présenter des garanties suffisantes pour assurer la mise en oeuvre des mesures de sécurité et de confidentialité mentionnées à l'article 34. Cette exigence ne décharge pas le responsable du traitement de son obligation de veiller au respect de ces mesures.

Le contrat liant le sous-traitant au responsable du traitement comporte l'indication des obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données et prévoit que le sous-traitant ne peut agir que sur instruction du responsable du traitement.

Article 36

Les données à caractère personnel ne peuvent être conservées au-delà de la durée prévue au 5° de l'article 6 qu'en vue d'être traitées à des fins historiques, statistiques ou scientifiques ; le choix des données ainsi conservées est opéré dans les conditions prévues à l'article L. 212-4 du code du patrimoine.

Les traitements dont la finalité se limite à assurer la conservation à long terme de documents d'archives dans le cadre du livre II du même code sont dispensés des formalités préalables à la mise en oeuvre des traitements prévues au chapitre IV de la présente loi.

Il peut être procédé à un traitement ayant des finalités autres que celles mentionnées au premier alinéa :
- soit avec l'accord exprès de la personne concernée ;
- soit avec l'autorisation de la Commission nationale de l'informatique et des libertés ;
- soit dans les conditions prévues au 8° du II et au IV de l'article 8 s'agissant de données mentionnées au I de ce même article.

Article 37

Les dispositions de la présente loi ne font pas obstacle à l'application, au bénéfice de tiers, des dispositions du titre Ier de la loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal et des dispositions du livre II du code du patrimoine.

En conséquence, ne peut être regardé comme un tiers non autorisé au sens de l'article 34 le titulaire d'un droit d'accès aux documents administratifs ou aux archives publiques exercé conformément à la loi n° 78-753 du 17 juillet 1978 précitée et au livre II du même code.

Section 2 : Droits des personnes à l'égard des traitements de données à caractère personnel

Article 38

Toute personne physique a le droit de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement.

Elle a le droit de s'opposer, sans frais, à ce que les données la concernant soient utilisées à des fins de prospection, notamment commerciale, par le responsable actuel du traitement ou celui d'un traitement ultérieur.

Les dispositions du premier alinéa ne s'appliquent pas lorsque le traitement répond à une obligation légale ou lorsque l'application de ces dispositions a été écartée par une disposition expresse de l'acte autorisant le traitement.

Article 39

I. - Toute personne physique justifiant de son identité a le droit d'interroger le responsable d'un traitement de données à caractère personnel en vue d'obtenir :
1° La confirmation que des données à caractère personnel la concernant font ou ne font pas l'objet de ce traitement ;

2° Des informations relatives aux finalités du traitement, aux catégories de données à caractère personnel traitées et aux destinataires ou aux catégories de destinataires auxquels les données sont communiquées ;

3° Le cas échéant, des informations relatives aux transferts de données à caractère personnel envisagés à destination d'un État non membre de la Communauté européenne ;

4° La communication, sous une forme accessible, des données à caractère personnel qui la concernent ainsi que de toute information disponible quant à l'origine de celles-ci ;

5° Les informations permettant de connaître et de contester la logique qui sous-tend le traitement automatisé en cas de décision prise sur le fondement de celui-ci et produisant des effets juridiques à l'égard de l'intéressé. Toutefois, les informations communiquées à la personne concernée ne doivent pas porter atteinte au droit d'auteur au sens des dispositions du livre Ier et du titre IV du livre III du code de la propriété intellectuelle.
Une copie des données à caractère personnel est délivrée à l'intéressé à sa demande. Le responsable du traitement peut subordonner la délivrance de cette copie au paiement d'une somme qui ne peut excéder le coût de la reproduction.

En cas de risque de dissimulation ou de disparition des données à caractère personnel, le juge compétent peut ordonner, y compris en référé, toutes mesures de nature à éviter cette dissimulation ou cette disparition.

II. - Le responsable du traitement peut s'opposer aux demandes manifestement abusives, notamment par leur nombre, leur caractère répétitif ou systématique. En cas de contestation, la charge de la preuve du caractère manifestement abusif des demandes incombe au responsable auprès duquel elles sont adressées.

Les dispositions du présent article ne s'appliquent pas lorsque les données à caractère personnel sont conservées sous une forme excluant manifestement tout risque d'atteinte à la vie privée des personnes concernées et pendant une durée n'excédant pas celle nécessaire aux seules finalités d'établissement de statistiques ou de recherche scientifique ou historique. Hormis les cas mentionnés au deuxième alinéa de l'article 36, les dérogations envisagées par le responsable du traitement sont mentionnées dans la demande d'autorisation ou dans la déclaration adressée à la Commission nationale de l'informatique et des libertés.

Article 40

Toute personne physique justifiant de son identité peut exiger du responsable d'un traitement que soient, selon les cas, rectifiées, complétées, mises à jour, verrouillées ou effacées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite.

Lorsque l'intéressé en fait la demande, le responsable du traitement doit justifier, sans frais pour le demandeur, qu'il a procédé aux opérations exigées en vertu de l'alinéa précédent.

En cas de contestation, la charge de la preuve incombe au responsable auprès duquel est exercé le droit d'accès sauf lorsqu'il est établi que les données contestées ont été communiquées par l'intéressé ou avec son accord.

Lorsqu'il obtient une modification de l'enregistrement, l'intéressé est en droit d'obtenir le remboursement des frais correspondant au coût de la copie mentionnée au I de l'article 39.

Si une donnée a été transmise à un tiers, le responsable du traitement doit accomplir les diligences utiles afin de lui notifier les opérations qu'il a effectuées conformément au premier alinéa.

Les héritiers d'une personne décédée justifiant de leur identité peuvent, si des éléments portés à leur connaissance leur laissent présumer que les données à caractère personnel la concernant faisant l'objet d'un traitement n'ont pas été actualisées, exiger du responsable de ce traitement qu'il prenne en considération le décès et procède aux mises à jour qui doivent en être la conséquence.

Lorsque les héritiers en font la demande, le responsable du traitement doit justifier, sans frais pour le demandeur, qu'il a procédé aux opérations exigées en vertu de l'alinéa précédent.

Article 41

Par dérogation aux articles 39 et 40, lorsqu'un traitement intéresse la sûreté de l'État, la défense ou la sécurité publique, le droit d'accès s'exerce dans les conditions prévues par le présent article pour l'ensemble des informations qu'il contient.

La demande est adressée à la commission qui désigne l'un de ses membres appartenant ou ayant appartenu au Conseil d'État, à la Cour de cassation ou à la Cour des comptes pour mener les investigations utiles et faire procéder aux modifications nécessaires. Celui-ci peut se faire assister d'un agent de la commission. Il est notifié au requérant qu'il a été procédé aux vérifications.
Lorsque la commission constate, en accord avec le responsable du traitement, que la communication des données qui y sont contenues ne met pas en cause ses finalités, la sûreté de l'État, la défense ou la sécurité publique, ces données peuvent être communiquées au requérant.

Lorsque le traitement est susceptible de comprendre des informations dont la communication ne mettrait pas en cause les fins qui lui sont assignées, l'acte réglementaire portant création du fichier peut prévoir que ces informations peuvent être communiquées au requérant par le gestionnaire du fichier directement saisi.

Article 42

Les dispositions de l'article 41 sont applicables aux traitements mis en oeuvre par les administrations publiques et les personnes privées chargées d'une mission de service public qui ont pour mission de prévenir, rechercher ou constater des infractions, ou de contrôler ou recouvrer des impositions, si un tel droit a été prévu par l'autorisation mentionnée aux articles 25, 26 ou 27.

Article 43

Lorsque l'exercice du droit d'accès s'applique à des données de santé à caractère personnel, celles-ci peuvent être communiquées à la personne concernée, selon son choix, directement ou par l'intermédiaire d'un médecin qu'elle désigne à cet effet, dans le respect des dispositions de l'article L. 1111-7 du code de la santé publique.

CHAPITRE VI - LE CONTRÔLE DE LA MISE EN ŒUVRE DES TRAITEMENTS

Article 44

I. - Les membres de la Commission nationale de l'informatique et des libertés ainsi que les agents de ses services habilités dans les conditions définies au dernier alinéa de l'article 19 ont accès, de 6 heures à 21 heures, pour l'exercice de leurs missions, aux lieux, locaux, enceintes, installations ou établissements servant à la mise en oeuvre d'un traitement de données à caractère personnel et qui sont à usage professionnel, à l'exclusion des parties de ceux-ci affectées au domicile privé.

Le procureur de la République territorialement compétent en est préalablement informé.
II. - En cas d'opposition du responsable des lieux, la visite ne peut se dérouler qu'avec l'autorisation du président du tribunal de grande instance dans le ressort duquel sont situés les locaux à visiter ou du juge délégué par lui.

Ce magistrat est saisi à la requête du président de la commission. Il statue par une ordonnance motivée, conformément aux dispositions prévues aux articles 493 à 498 du nouveau code de procédure civile. La procédure est sans représentation obligatoire.

La visite s'effectue sous l'autorité et le contrôle du juge qui l'a autorisée. Celui-ci peut se rendre dans les locaux durant l'intervention. A tout moment, il peut décider l'arrêt ou la suspension de la visite.

III. - Les membres de la commission et les agents mentionnés au premier alinéa du I peuvent demander communication de tous documents nécessaires à l'accomplissement de leur mission, quel qu'en soit le support, et en prendre copie ; ils peuvent recueillir, sur place ou sur convocation, tout renseignement et toute justification utiles ; ils peuvent accéder aux programmes informatiques et aux données, ainsi qu'en demander la transcription par tout traitement approprié dans des documents directement utilisables pour les besoins du contrôle.

Ils peuvent, à la demande du président de la commission, être assistés par des experts désignés par l'autorité dont ceux-ci dépendent.

Seul un médecin peut requérir la communication de données médicales individuelles incluses dans un traitement nécessaire aux fins de la médecine préventive, de la recherche médicale, des diagnostics médicaux, de l'administration de soins ou de traitements, ou à la gestion de service de santé, et qui est mis en oeuvre par un membre d'une profession de santé.

Il est dressé contradictoirement procès-verbal des vérifications et visites menées en application du présent article.

IV. - Pour les traitements intéressant la sûreté de l'État et qui sont dispensés de la publication de l'acte réglementaire qui les autorise en application du III de l'article 26, le décret en Conseil d'État qui prévoit cette dispense peut également prévoir que le traitement n'est pas soumis aux dispositions du présent article.

CHAPITRE VII - SANCTIONS PRONONCÉES PAR LA COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS

Article 45

I. - La Commission nationale de l'informatique et des libertés peut prononcer un avertissement à l'égard du responsable d'un traitement qui ne respecte pas les obligations découlant de la présente loi. Elle peut également mettre en demeure ce responsable de faire cesser le manquement constaté dans un délai qu'elle fixe.

Si le responsable d'un traitement ne se conforme pas à la mise en demeure qui lui est adressée, la commission peut prononcer à son encontre, après une procédure contradictoire, les sanctions suivantes :
1° Une sanction pécuniaire, dans les conditions prévues par l'article 47, à l'exception des cas où le traitement est mis en oeuvre par l'État ;

2° Une injonction de cesser le traitement, lorsque celui-ci relève des dispositions de l'article 22, ou un retrait de l'autorisation accordée en application de l'article 25.
II. - En cas d'urgence, lorsque la mise en oeuvre d'un traitement ou l'exploitation des données traitées entraîne une violation des droits et libertés mentionnés à l'article 1er, la commission peut, après une procédure contradictoire :
1° Décider l'interruption de la mise en oeuvre du traitement, pour une durée maximale de trois mois, si le traitement n'est pas au nombre de ceux qui sont mentionnés au I et au II de l'article 26, ou de ceux mentionnés à l'article 27 mis en oeuvre par l'État ;

2° Décider le verrouillage de certaines des données à caractère personnel traitées, pour une durée maximale de trois mois, si le traitement n'est pas au nombre de ceux qui sont mentionnés au I et au II de l'article 26 ;

3° Informer le Premier ministre pour qu'il prenne, le cas échéant, les mesures permettant de faire cesser la violation constatée, si le traitement en cause est au nombre de ceux qui sont mentionnés au I et au II de l'article 26 ; le Premier ministre fait alors connaître à la commission les suites qu'il a données à cette information au plus tard quinze jours après l'avoir reçue.
III. - En cas d'atteinte grave et immédiate aux droits et libertés mentionnés à l'article 1er, le président de la commission peut demander, par la voie du référé, à la juridiction compétente d'ordonner, le cas échéant sous astreinte, toute mesure de sécurité nécessaire à la sauvegarde de ces droits et libertés.

Article 46

Les sanctions prévues au I et au 1° du II de l'article 45 sont prononcées sur la base d'un rapport établi par l'un des membres de la Commission nationale de l'informatique et des libertés, désigné par le président de celle-ci parmi les membres n'appartenant pas à la formation restreinte. Ce rapport est notifié au responsable du traitement, qui peut déposer des observations et se faire représenter ou assister. Le rapporteur peut présenter des observations orales à la commission mais ne prend pas part à ses délibérations. La commission peut entendre toute personne dont l'audition lui paraît susceptible de contribuer utilement à son information.

La commission peut rendre publics les avertissements qu'elle prononce. Elle peut également, en cas de mauvaise foi du responsable du traitement, ordonner l'insertion des autres sanctions qu'elle prononce dans des publications, journaux et supports qu'elle désigne. Les frais sont supportés par les personnes sanctionnées.

Les décisions prises par la commission au titre de l'article 45 sont motivées et notifiées au responsable du traitement. Les décisions prononçant une sanction peuvent faire l'objet d'un recours de pleine juridiction devant le Conseil d'État.

Article 47

Le montant de la sanction pécuniaire prévue au I de l'article 45 est proportionné à la gravité des manquements commis et aux avantages tirés de ce manquement.

Lors du premier manquement, il ne peut excéder 150 000 €. En cas de manquement réitéré dans les cinq années à compter de la date à laquelle la sanction pécuniaire précédemment prononcée est devenue définitive, il ne peut excéder 300 000 € ou, s'agissant d'une entreprise, 5 % du chiffre d'affaires hors taxes du dernier exercice clos dans la limite de 300 000 €.

Lorsque la Commission nationale de l'informatique et des libertés a prononcé une sanction pécuniaire devenue définitive avant que le juge pénal ait statué définitivement sur les mêmes faits ou des faits connexes, celui-ci peut ordonner que la sanction pécuniaire s'impute sur l'amende qu'il prononce.

Les sanctions pécuniaires sont recouvrées comme les créances de l'État étrangères à l'impôt et au domaine.

Article 48

La commission peut exercer les pouvoirs prévus à l'article 44 ainsi qu'au I, au 1° du II et au III de l'article 45 à l'égard des traitements dont les opérations sont mises en oeuvre, en tout ou partie, sur le territoire national, y compris lorsque le responsable du traitement est établi sur le territoire d'un autre État membre de la Communauté européenne.

Article 49

La commission peut, à la demande d'une autorité exerçant des compétences analogues aux siennes dans un autre État membre de la Communauté européenne, procéder à des vérifications dans les mêmes conditions, selon les mêmes procédures et sous les mêmes sanctions que celles prévues à l'article 45, sauf s'il s'agit d'un traitement mentionné au I ou au II de l'article 26.

La commission est habilitée à communiquer les informations qu'elle recueille ou qu'elle détient, à leur demande, aux autorités exerçant des compétences analogues aux siennes dans d'autres États membres de la Communauté européenne.

CHAPITRE VIII - DISPOSITIONS PÉNALES

Article 50

Les infractions aux dispositions de la présente loi sont prévues et réprimées par les articles 226-16 à 226-24 du code pénal.

Article 51

Est puni d'un an d'emprisonnement et de 15 000 € d'amende le fait d'entraver l'action de la Commission nationale de l'informatique et des libertés :
1° Soit en s'opposant à l'exercice des missions confiées à ses membres ou aux agents habilités en application du dernier alinéa de l'article 19 ;

2° Soit en refusant de communiquer à ses membres ou aux agents habilités en application du dernier alinéa de l'article 19 les renseignements et documents utiles à leur mission, ou en dissimulant lesdits documents ou renseignements, ou en les faisant disparaître ;

3° Soit en communiquant des informations qui ne sont pas conformes au contenu des enregistrements tel qu'il était au moment où la demande a été formulée ou qui ne présentent pas ce contenu sous une forme directement accessible.

Article 52

Le procureur de la République avise le président de la Commission nationale de l'informatique et des libertés de toutes les poursuites relatives aux infractions aux dispositions de la section 5 du chapitre VI du titre II du livre II du code pénal et, le cas

échéant, des suites qui leur sont données. Il l'informe de la date et de l'objet de l'audience de jugement par lettre recommandée adressée au moins dix jours avant cette date.

La juridiction d'instruction ou de jugement peut appeler le président de la Commission nationale de l'informatique et des libertés ou son représentant à déposer ses observations ou à les développer oralement à l'audience.

Chapitre IX - TRAITEMENTS DE DONNÉES À CARACTÈRE PERSONNEL AYANT POUR FIN LA RECHERCHE DANS LE DOMAINE DE LA SANTÉ

Article 53

Les traitements de données à caractère personnel ayant pour fin la recherche dans le domaine de la santé sont soumis aux dispositions de la présente loi, à l'exception des articles 23 à 26, 32 et 38.
Les traitements de données ayant pour fin le suivi thérapeutique ou médical individuel des patients ne sont pas soumis aux dispositions du présent chapitre. Il en va de même des traitements permettant d'effectuer des études à partir des données ainsi recueillies si ces études sont réalisées par les personnels assurant ce suivi et destinées à leur usage exclusif.

Article 54

Pour chaque demande de mise en oeuvre d'un traitement de données à caractère personnel, un comité consultatif sur le traitement de l'information en matière de recherche dans le domaine de la santé, institué auprès du ministre chargé de la recherche et composé de personnes compétentes en matière de recherche dans le domaine de la santé, d'épidémiologie, de génétique et de biostatistique, émet un avis sur la méthodologie de la recherche au regard des dispositions de la présente loi, la nécessité du recours à des données à caractère personnel et la pertinence de celles-ci par rapport à l'objectif de la recherche, préalablement à la saisine de la Commission nationale de l'informatique et des libertés.
Le comité consultatif dispose d'un mois pour transmettre son avis au demandeur. A défaut, l'avis est réputé favorable. En cas d'urgence, ce délai peut être ramené à quinze jours.
Le président du comité consultatif peut mettre en oeuvre une procédure simplifiée.
La mise en œuvre du traitement de données est ensuite soumise à l'autorisation de la Commission nationale de l'informatique et des libertés, qui se prononce dans les conditions prévues à l'article 25.
Pour les catégories les plus usuelles de traitements automatisés ayant pour finalité la recherche dans le domaine de la santé et portant sur des données ne permettant pas une identification directe des personnes concernées, la commission peut homologuer et publier des méthodologies de référence, établies en concertation avec le comité consultatif ainsi qu'avec les organismes publics et privés représentatifs, et destinées à simplifier la procédure prévue aux quatre premiers alinéas du présent article.
Ces méthodologies précisent, eu égard aux caractéristiques mentionnées à l'article 30, les normes auxquelles doivent correspondre les traitements pouvant faire l'objet d'une demande d'avis et d'une demande d'autorisation simplifiées.
Pour les traitements répondant à ces normes, seul un engagement de conformité à l'une d'entre elles est envoyé à la commission. Le président de la commission peut autoriser ces traitements à l'issue d'une procédure simplifiée d'examen.
Pour les autres catégories de traitements, le comité consultatif fixe, en concertation avec la Commission nationale de l'informatique et des libertés, les conditions dans lesquelles son avis n'est pas requis.

Article 55

Nonobstant les règles relatives au secret professionnel, les membres des professions de santé peuvent transmettre les données à caractère personnel qu'ils détiennent dans le cadre d'un traitement de données autorisé en application de l'article 53.
Lorsque ces données permettent l'identification des personnes, elles doivent être codées avant leur transmission. Toutefois, il peut être dérogé à cette obligation lorsque le traitement de données est associé à des études de pharmacovigilance ou à des protocoles de recherche réalisés dans le cadre d'études coopératives nationales ou internationales ; il peut également y être dérogé si une particularité de la recherche l'exige. La demande d'autorisation comporte la justification scientifique et technique de la dérogation et l'indication de la période nécessaire à la recherche. À l'issue de cette période, les données sont conservées et traitées dans les conditions fixées à l'article 36.
La présentation des résultats du traitement de données ne peut en aucun cas permettre l'identification directe ou indirecte des personnes concernées.
Les données sont reçues par le responsable de la recherche désigné à cet effet par la personne physique ou morale autorisée à mettre en oeuvre le traitement. Ce responsable veille à la sécurité des informations et de leur traitement, ainsi qu'au respect de la finalité de celui-ci.
Les personnes appelées à mettre en oeuvre le traitement de données ainsi que celles qui ont accès aux données sur lesquelles il porte sont astreintes au secret professionnel sous les peines prévues à l'article 226-13 du code pénal.

Article 56

Toute personne a le droit de s'opposer à ce que les données à caractère personnel la concernant fassent l'objet de la levée du secret professionnel rendue nécessaire par un traitement de la nature de ceux qui sont visés à l'article 53.
Dans le cas où la recherche nécessite le recueil de prélèvements biologiques identifiants, le consentement éclairé et exprès des personnes concernées doit être obtenu préalablement à la mise en oeuvre du traitement de données.
Les informations concernant les personnes décédées, y compris celles qui figurent sur les certificats des causes de décès, peuvent faire l'objet d'un traitement de données, sauf si l'intéressé a, de son vivant, exprimé son refus par écrit.

Article 57

Les personnes auprès desquelles sont recueillies des données à caractère personnel ou à propos desquelles de telles données sont transmises sont, avant le début du traitement de ces données, individuellement informées :
1° De la nature des informations transmises ;
2° De la finalité du traitement de données ;
3° Des personnes physiques ou morales destinataires des données ;
4° Du droit d'accès et de rectification institué aux articles 39 et 40 ;
5° Du droit d'opposition institué aux premier et troisième alinéas de l'article 56 ou, dans le cas prévu au deuxième alinéa de cet article, de l'obligation de recueillir leur consentement.

Toutefois, ces informations peuvent ne pas être délivrées si, pour des raisons légitimes que le médecin traitant apprécie en conscience, le malade est laissé dans l'ignorance d'un diagnostic ou d'un pronostic grave.
Dans le cas où les données ont été initialement recueillies pour un autre objet que le traitement, il peut être dérogé à l'obligation d'information individuelle lorsque celle-ci se heurte à la difficulté de retrouver les personnes concernées. Les dérogations à l'obligation d'informer les personnes de l'utilisation de données les concernant à des fins de recherche sont mentionnées dans le dossier de demande d'autorisation transmis à la Commission nationale de l'informatique et des libertés, qui statue sur ce point.

Article 58

Sont destinataires de l'information et exercent les droits prévus aux articles 56 et 57 les titulaires de l'autorité parentale, pour les mineurs, ou le représentant légal, pour les personnes faisant l'objet d'une mesure de tutelle.

Article 59

Une information relative aux dispositions du présent chapitre doit être assurée dans tout établissement ou centre où s'exercent des activités de prévention, de diagnostic et de soins donnant lieu à la transmission de données à caractère personnel en vue d'un traitement visé à l'article 53.

Article 60

La mise en oeuvre d'un traitement de données en violation des conditions prévues par le présent chapitre entraîne le retrait temporaire ou définitif, par la Commission nationale de l'informatique et des libertés, de l'autorisation délivrée en application des dispositions de l'article 54.
Il en est de même en cas de refus de se soumettre aux vérifications prévues par le f du 2° de l'article 11.

Article 61

La transmission vers un État n'appartenant pas à la Communauté européenne de données à caractère personnel non codées faisant l'objet d'un traitement ayant pour fin la recherche dans le domaine de la santé n'est autorisée, dans les conditions prévues à l'article 54, que sous réserve du respect des règles énoncées au chapitre XII.

Chapitre X - TRAITEMENTS DE DONNÉES DE SANTÉ À CARACTÈRE PERSONNEL À DES FINS D'ÉVALUATION OU D'ANALYSE DES PRATIQUES OU DES ACTIVITÉS DE SOINS ET DE PRÉVENTION

Article 62

Les traitements de données de santé à caractère personnel qui ont pour fin l'évaluation des pratiques de soins et de prévention sont autorisés dans les conditions prévues au présent chapitre.
Les dispositions du présent chapitre ne s'appliquent ni aux traitements de données à caractère personnel effectuées à des fins de remboursement ou de contrôle par les organismes chargés de la gestion d'un régime de base d'assurance maladie, ni aux traitements effectués au sein des établissements de santé par les médecins responsables de l'information médicale dans les conditions prévues au deuxième alinéa de l'article L. 6113-7 du code de la santé publique.

Article 63

Les données issues des systèmes d'information visés à l'article L. 6113-7 du code de la santé publique, celles issues des dossiers médicaux détenus dans le cadre de l'exercice libéral des professions de santé, ainsi que celles issues des systèmes d'information des caisses d'assurance maladie, ne peuvent être communiquées à des fins statistiques d'évaluation ou d'analyse des pratiques et des activités de soins et de prévention que sous la forme de statistiques agrégées ou de données par patient constituées de telle sorte que les personnes concernées ne puissent être identifiées.
Il ne peut être dérogé aux dispositions de l'alinéa précédent que sur autorisation de la Commission nationale de l'informatique et des libertés dans les conditions prévues aux articles 64 à 66. Dans ce cas, les données utilisées ne comportent ni le nom, ni le prénom des personnes, ni leur numéro d'inscription au Répertoire national d'identification des personnes physiques.

Article 64

Pour chaque demande, la commission vérifie les garanties présentées par le demandeur pour l'application des présentes dispositions et, le cas échéant, la conformité de sa demande à ses missions ou à son objet social. Elle s'assure de la nécessité de recourir à des données à caractère personnel et de la pertinence du traitement au regard de sa finalité déclarée d'évaluation ou d'analyse des pratiques ou des activités de soins et de prévention. Elle vérifie que les données à caractère personnel dont le traitement est envisagé ne comportent ni le nom, ni le prénom des personnes concernées, ni leur numéro d'inscription au Répertoire national d'identification des personnes physiques. En outre, si le demandeur n'apporte pas d'éléments suffisants pour attester la nécessité de disposer de certaines informations parmi l'ensemble des données à caractère personnel dont le traitement est envisagé, la commission peut interdire la communication de ces informations par l'organisme qui les détient et n'autoriser le traitement que des données ainsi réduites.
La commission détermine la durée de conservation des données nécessaires au traitement et apprécie les dispositions prises pour assurer leur sécurité et la garantie des secrets protégés par la loi.

Article 65

La commission dispose, à compter de sa saisine par le demandeur, d'un délai de deux mois, renouvelable une seule fois, pour se prononcer. A défaut de décision dans ce délai, ce silence vaut décision de rejet.
Les traitements répondant à une même finalité portant sur des catégories de données identiques et ayant des destinataires ou des catégories de destinataires identiques peuvent faire l'objet d'une décision unique de la commission.

Article 66

Les traitements autorisés conformément aux articles 64 et 65 ne peuvent servir à des fins de recherche ou d'identification des personnes. Les personnes appelées à mettre en œuvre ces traitements, ainsi que celles qui ont accès aux données faisant l'objet

de ces traitements ou aux résultats de ceux-ci lorsqu'ils permettent indirectement d'identifier les personnes concernées, sont astreintes au secret professionnel sous les peines prévues à l'article 226-13 du code pénal.
Les résultats de ces traitements ne peuvent faire l'objet d'une communication, d'une publication ou d'une diffusion que si l'identification des personnes sur l'état desquelles ces données ont été recueillies est impossible.

Chapitre XI - TRAITEMENTS DE DONNÉES À CARACTÈRE PERSONNEL AUX FINS DE JOURNALISME ET D'EXPRESSION LITTÉRAIRE ET ARTISTIQUE

Article 67
Le 5° de l'article 6, les articles 8, 9, 22, les 1° et 3° du I de l'article 25, les articles 32, 39, 40 et 68 à 70 ne s'appliquent pas aux traitements de données à caractère personnel mis en oeuvre aux seules fins :
1° D'expression littéraire et artistique ;

2° D'exercice, à titre professionnel, de l'activité de journaliste, dans le respect des règles déontologiques de cette profession.
Toutefois, pour les traitements mentionnés au 2°, la dispense de l'obligation de déclaration prévue par l'article 22 est subordonnée à la désignation par le responsable du traitement d'un correspondant à la protection des données appartenant à un organisme de la presse écrite ou audiovisuelle, chargé de tenir un registre des traitements mis en oeuvre par ce responsable et d'assurer, d'une manière indépendante, l'application des dispositions de la présente loi. Cette désignation est portée à la connaissance de la Commission nationale de l'informatique et des libertés.

En cas de non-respect des dispositions de la loi applicables aux traitements prévus par le présent article, le responsable du traitement est enjoint par la Commission nationale de l'informatique et des libertés de se mettre en conformité avec la loi. En cas de manquement constaté à ses devoirs, le correspondant est déchargé de ses fonctions sur demande, ou après consultation, de la Commission nationale de l'informatique et des libertés.

Les dispositions des alinéas précédents ne font pas obstacle à l'application des dispositions du code civil, des lois relatives à la presse écrite ou audiovisuelle et du code pénal, qui prévoient les conditions d'exercice du droit de réponse et qui préviennent, limitent, réparent et, le cas échéant, répriment les atteintes à la vie privée et à la réputation des personnes.

Chapitre XII - TRANSFERTS DE DONNÉES À CARACTÈRE PERSONNEL VERS DES ÉTATS N'APPARTENANT PAS À LA COMMUNAUTÉ EUROPÉENNE

Article 68
Le responsable d'un traitement ne peut transférer des données à caractère personnel vers un État n'appartenant pas à la Communauté européenne que si cet État assure un niveau de protection suffisant de la vie privée et des libertés et droits fondamentaux des personnes à l'égard du traitement dont ces données font l'objet ou peuvent faire l'objet.

Le caractère suffisant du niveau de protection assuré par un État s'apprécie en fonction notamment des dispositions en vigueur dans cet État, des mesures de sécurité qui y sont appliquées, des caractéristiques propres du traitement, telles que ses fins et sa durée, ainsi que de la nature, de l'origine et de la destination des données traitées.

Article 69
Toutefois, le responsable d'un traitement peut transférer des données à caractère personnel vers un État ne répondant pas aux conditions prévues à l'article 68 si la personne à laquelle se rapportent les données a consenti expressément à leur transfert ou si le transfert est nécessaire à l'une des conditions suivantes :
1° A la sauvegarde de la vie de cette personne ;

2° A la sauvegarde de l'intérêt public ;

3° Au respect d'obligations permettant d'assurer la constatation, l'exercice ou la défense d'un droit en justice ;

4° A la consultation, dans des conditions régulières, d'un registre public qui, en vertu de dispositions législatives ou réglementaires, est destiné à l'information du public et est ouvert à la consultation de celui-ci ou de toute personne justifiant d'un intérêt légitime ;

5° A l'exécution d'un contrat entre le responsable du traitement et l'intéressé, ou de mesures précontractuelles prises à la demande de celui-ci ;

6° A la conclusion ou à l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers.
Il peut également être fait exception à l'interdiction prévue à l'article 68, par décision de la Commission nationale de l'informatique et des libertés ou, s'il s'agit d'un traitement mentionné au I ou au II de l'article 26, par décret en Conseil d'État pris après avis motivé et publié de la commission, lorsque le traitement garantit un niveau de protection suffisant de la vie privée ainsi que des libertés et droits fondamentaux des personnes, notamment en raison des clauses contractuelles ou règles internes dont il fait l'objet.

La Commission nationale de l'informatique et des libertés porte à la connaissance de la Commission des Communautés européennes et des autorités de contrôle des autres États membres de la Communauté européenne les décisions d'autorisation de transfert de données à caractère personnel qu'elle prend au titre de l'alinéa précédent.

Article 70
Si la Commission des Communautés européennes a constaté qu'un État n'appartenant pas à la Communauté européenne n'assure pas un niveau de protection suffisant à l'égard d'un transfert ou d'une catégorie de transferts de données à caractère personnel, la Commission nationale de l'informatique et des libertés, saisie d'une déclaration déposée en application des articles 23 ou 24 et faisant apparaître que des données à caractère personnel seront transférées vers cet État, délivre le récépissé avec mention de l'interdiction de procéder au transfert des données.

Lorsqu'elle estime qu'un État n'appartenant pas à la Communauté européenne n'assure pas un niveau de protection suffisant à l'égard d'un transfert ou d'une catégorie de transferts de données, la Commission nationale de l'informatique et des libertés en informe sans délai la Commission des Communautés européennes. Lorsqu'elle est saisie d'une déclaration déposée en application des articles 23 ou 24 et faisant apparaître que des données à caractère personnel seront transférées vers cet État, la Commission nationale de l'informatique et des libertés délivre le récépissé et peut enjoindre au responsable du traitement de suspendre le transfert des données. Si la Commission des Communautés européennes constate que l'État vers lequel le transfert est envisagé assure un niveau de protection suffisant, la Commission nationale de l'informatique et des libertés notifie au responsable du traitement la cessation de la suspension du transfert. Si la Commission des Communautés européennes constate que l'État vers lequel le transfert est envisagé n'assure pas un niveau de protection suffisant, la Commission nationale de l'informatique et des libertés notifie au responsable du traitement l'interdiction de procéder au transfert de données à caractère personnel à destination de cet État.

Chapitre XIII - DISPOSITIONS DIVERSES

Article 71
Des décrets en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés, fixent les modalités d'application de la présente loi.

Article 72
La présente loi est applicable en Polynésie française, dans les îles Wallis et Futuna, dans les Terres australes et antarctiques françaises, en Nouvelle-Calédonie et à Mayotte.

Par dérogation aux dispositions du deuxième alinéa de l'article 54, le comité consultatif dispose d'un délai de deux mois pour transmettre son avis au demandeur lorsque celui-ci réside dans l'une de ces collectivités. En cas d'urgence, ce délai peut être ramené à un mois.

أنظر صفحة الأنترنت التالية :
http://www.cnil.fr/

ملحق رقم : 6

مقتطف من قانون العقوبات الفرنسي : المواد من 226 مكرر 16 إلى 226 مكرر 24

Extrait du Code Pénal Français : Articles 226-16 à 226-24

SECTION 5 : DES ATTEINTES AUX DROITS DE LA PERSONNE RESULTANT DES FICHIERS OU DES TRAITEMENTS INFORMATIQUES

Art. 226-16

Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 € d'amende.
Est puni des mêmes peines le fait, y compris par négligence, de procéder ou de faire procéder à un traitement qui a fait l'objet de l'une des mesures prévues au 2° du I de l'article 45 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Art. 226-16-1 A

Lorsqu'il a été procédé ou fait procéder à un traitement de données à caractère personnel dans les conditions prévues par le I ou le II de l'article 24 de la loi n° 78-17 du 6 janvier 1978 précitée, le fait de ne pas respecter, y compris par négligence, les normes simplifiées ou d'exonération établies à cet effet par la Commission nationale de l'informatique et des libertés est puni de cinq ans d'emprisonnement et de 300 000 € d'amende.

Art. 226-16-1

Le fait, hors les cas où le traitement a été autorisé dans les conditions prévues par la loi n° 78-17 du 6 janvier 1978 précitée, de procéder ou faire procéder à un traitement de données à caractère personnel incluant parmi les données sur lesquelles il porte le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques, est puni de cinq ans d'emprisonnement et de 300 000 € d'amende.

Art. 226-17

Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 € d'amende.

Art. 226-18

Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 € d'amende.

Art. 226-18-1

Le fait de procéder à un traitement de données à caractère personnel concernant une personne physique malgré l'opposition de cette personne, lorsque ce traitement répond à des fins de prospection, notamment commerciale, ou lorsque cette opposition est fondée sur des motifs légitimes, est puni de cinq ans d'emprisonnement et de 300 000 € d'amende.

Art. 226-19

Le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée, sans le consentement exprès de l'intéressé, des données à caractère personnel qui, directement ou indirectement, font apparaître les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, ou les appartenances syndicales des personnes, ou qui sont relatives à la santé ou à l'orientation sexuelle de celles-ci, est puni de cinq ans d'emprisonnement et de 300 000 € d'amende.
Est puni des mêmes peines le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée des données à caractère personnel concernant des infractions, des condamnations ou des mesures de sûreté.

Art. 226-19-1

En cas de traitement de données à caractère personnel ayant pour fin la recherche dans le domaine de la santé, est puni de cinq ans d'emprisonnement et de 300 000 € d'amende le fait de procéder à un traitement :
1° Sans avoir préalablement informé individuellement les personnes sur le compte desquelles des données à caractère personnel sont recueillies ou transmises de leur droit d'accès, de rectification et d'opposition, de la nature des données transmises et des destinataires de celles-ci ;
2° Malgré l'opposition de la personne concernée ou, lorsqu'il est prévu par la loi, en l'absence du consentement éclairé et exprès de la personne, ou s'il s'agit d'une personne décédée, malgré le refus exprimé par celle-ci de son vivant.

Art. 226-20

Le fait de conserver des données à caractère personnel au-delà de la durée prévue par la loi ou le règlement, par la demande d'autorisation ou d'avis, ou par la déclaration préalable adressée à la Commission nationale de l'informatique et des libertés, est puni de cinq ans d'emprisonnement et de 300 000 € d'amende, sauf si cette conservation est effectuée à des fins historiques, statistiques ou scientifiques dans les conditions prévues par la loi.
Est puni des mêmes peines le fait, hors les cas prévus par la loi, de traiter à des fins autres qu'historiques, statistiques ou scientifiques des données à caractère personnel conservées au-delà de la durée mentionnée au premier alinéa.

Art. 226-21

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 forme de traitement, de détourner ces informations de leur finalité telle que définie par la disposition législative, l'acte réglementaire ou la décision de la Commission nationale de l'informatique et des 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 300 000 € d'amende.

Art. 226-22

Le fait, par toute personne qui a recueilli, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir est puni de cinq ans d'emprisonnement et de 300 000 € d'amende.
La divulgation prévue à l'alinéa précédent est punie de trois ans d'emprisonnement et de 100 000 € d'amende lorsqu'elle a été commise par imprudence ou négligence.
Dans les cas prévus aux deux alinéas précédents, la poursuite ne peut être exercée que sur plainte de la victime, de son représentant légal ou de ses ayants droit.

Art. 226-22-1

Le fait, hors les cas prévus par la loi, de procéder ou de faire procéder à un transfert de données à caractère personnel faisant l'objet ou destinées à faire l'objet d'un traitement vers un État n'appartenant pas à la Communauté européenne en violation des mesures prises par la Commission des Communautés européennes ou par la Commission nationale de l'informatique et des libertés mentionnées à l'article 70 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 € d'amende.

Art. 226-22-2

Dans les cas prévus aux articles 226-16 à 226-22-1, l'effacement de tout ou partie des données à caractère personnel faisant l'objet du traitement ayant donné lieu à l'infraction peut être ordonné. Les membres et les agents de la Commission nationale de l'informatique et des libertés sont habilités à constater l'effacement de ces données.

Art. 226-23

Les dispositions de l'article 226-19 sont applicables aux traitements non automatisés de données à caractère personnel dont la mise en œuvre ne se limite pas à l'exercice d'activités exclusivement personnelles.

Art. 226-24

Les personnes morales peuvent être déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies à la présente section.
Les peines encourues par les personnes morales sont :
1º L'amende, suivant les modalités prévues par l'article 131-38 ;
2º Les peines mentionnées aux 2º, 3º, 4º, 5º, 7º, 8º et 9º de l'article 131-39.
L'interdiction mentionnée au 2º de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise.

ملحق رقم : 7

القانون رقم 88-19 المعدل و الذي عدل و أدخل إلى قانون العقوبات في 1 جانفي 1994 المواد من 323 مكرر 1 إلى 323 مكرر 7 من قانون العقوبات الفرنسي المتعلقة بـــ : الجرائم ضد أنظمة المعالجة الآلية للمعطيات

Articles 323-1 à 323-7 du code relative aux : délits contre les systèmes de traitement automatisé de données

Article 323-1 :

Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni d'un an d'emprisonnement et de 15 000 euros 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 deux ans d'emprisonnement et de 30 000 euros d'amende.

Article 323-2 :

Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de trois ans d'emprisonnement et de 45 000 euros d'amende.

Article 323-3 :

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 trois ans d'emprisonnement et de 45 000 euros d'amende.

Article 323-4 :

La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Article 323-5 :

Les personnes physiques coupables des délits prévus au présent chapitre encourent également les peines complémentaires suivantes : L'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, suivant les modalités de l'article 131-26 ; L'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise ; La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution ; La fermeture, pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ; l'exclusion, pour une durée de cinq ans au plus, des marchés publics ; L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ; L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35.

Article 323-6 :

Les personnes morales peuvent être déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies au présent chapitre.

Les peines encourues par les personnes morales sont : L'amende, suivant les modalités prévues par l'article 131-38 ; Les peines mentionnées à l'article 131-39.

L'interdiction mentionnée au 2° de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise.

Article 323-7 :

La tentative des délits prévus par les articles 323-1 à 323-3 est punie des mêmes peines.

ملحق رقم : 8

قانون رقم 2004-575 لـــ 21 جوان 2004 "للثقة في الإقتصاد المعلوماتي" متمم في 11 جويلية 2010
الفصل الثاني من الباب الأول تحت عنوان : " عن حرية الإتصال في الشبكة "
و الفصل الثاني من الباب الثالث من هذا القانون تحت عنوان : " مكافحة الإجرام المعلوماتي "
الجريدة الرسمية رقم 143 لـــ 22 جوان 2004

Loi n° 2004-575 du 21 juin 2004 : " pour la confiance dans l'économie numérique "
Version consolidée au 11 juillet 2010
Chapitre II du Titre 1er de cette loi sous le titre de : "De le liberté de communication en ligne "
et Chapitre II du Titre III de cette loi sous le titre de : " Lutte contre la cybercriminalité "
Journal Officiel n° 143 du 22 juin 2004 version consolidée au 11 juillet 2010

CHAPITRE II :
Les prestataires techniques

TITRE Ier :
DE LA LIBERTÉ DE COMMUNICATION EN LIGNE

Article 6
Modifié par LOI n°2010-769 du 9 juillet 2010 - art. 28

I.-1. 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 proposent au moins un de ces moyens.
Les personnes visées à l'alinéa précédent les informent également de l'existence de moyens de sécurisation permettant de prévenir les manquements à l'obligation définie à l'article L. 336-3 du code de la propriété intellectuelle et leur proposent au moins un des moyens figurant sur la liste prévue au deuxième alinéa de l'article L. 331-26 du même code.
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 de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services ne peuvent pas voir leur responsabilité civile engagée du fait des activités ou des informations stockées à la demande d'un destinataire de ces services si elles n'avaient pas effectivement connaissance de leur caractère illicite ou de faits et circonstances faisant apparaître ce caractère ou si, dès le moment où elles en ont eu cette connaissance, elles ont agi promptement pour retirer ces données ou en rendre l'accès impossible.
L'alinéa précédent ne s'applique pas lorsque le destinataire du service agit sous l'autorité ou le contrôle de la personne visée audit alinéa.
3. Les personnes visées au 2 ne peuvent voir leur responsabilité pénale engagée à raison des informations stockées à la demande d'un destinataire de ces services si elles n'avaient pas effectivement connaissance de l'activité ou de l'information illicites ou si, dès le moment où elles en ont eu connaissance, elles ont agi promptement pour retirer ces informations ou en rendre l'accès impossible.
L'alinéa précédent ne s'applique pas lorsque le destinataire du service agit sous l'autorité ou le contrôle de la personne visée audit alinéa.
4. Le fait, pour toute personne, de présenter aux personnes mentionnées au 2 un contenu ou une activité comme étant illicite dans le but d'en obtenir le retrait ou d'en faire cesser la diffusion, alors qu'elle sait cette information inexacte, est puni d'une peine d'un an d'emprisonnement et de 15 000 Euros d'amende.
5. La connaissance des faits litigieux est présumée acquise par les personnes désignées au 2 lorsqu'il leur est notifié les éléments suivants :
-la date de la notification ;
-si le notifiant est une personne physique : ses nom, prénoms, profession, domicile, nationalité, date et lieu de naissance ; si le requérant est une personne morale : sa forme, sa dénomination, son siège social et l'organe qui la représente légalement ;
-les nom et domicile du destinataire ou, s'il s'agit d'une personne morale, sa dénomination et son siège social ;
-la description des faits litigieux et leur localisation précise ;
-les motifs pour lesquels le contenu doit être retiré, comprenant la mention des dispositions légales et des justifications de faits ;
-la copie de la correspondance adressée à l'auteur ou à l'éditeur des informations ou activités litigieuses demandant leur interruption, leur retrait ou leur modification, ou la justification de ce que l'auteur ou l'éditeur n'a pu être contacté.
6. Les personnes mentionnées aux 1 et 2 ne sont pas des producteurs au sens de l'article 93-3 de la loi n° 82-652 du 29 juillet 1982 sur la communication audiovisuelle.
7. Les personnes mentionnées aux 1 et 2 ne sont pas soumises à une obligation générale de surveiller les informations qu'elles transmettent ou stockent, ni à une obligation générale de rechercher des faits ou des circonstances révélant des activités illicites.

Le précédent alinéa est sans préjudice de toute activité de surveillance ciblée et temporaire demandée par l'autorité judiciaire.
Compte tenu de l'intérêt général attaché à la répression de l'apologie des crimes contre l'humanité, de l'incitation à la haine raciale ainsi que de la pornographie enfantine, de l'incitation à la violence , notamment l'incitation aux violences faites aux femmes, ainsi que des atteintes à la dignité humaine, les personnes mentionnées ci-dessus doivent concourir à la lutte contre la diffusion des infractions visées aux cinquième et huitième alinéas de l'article 24 de la loi du 29 juillet 1881 sur la liberté de la presse et aux articles 227-23 et 227-24 du code pénal.
A ce titre, elles doivent mettre en place un dispositif facilement accessible et visible permettant à toute personne de porter à leur connaissance ce type de données. Elles ont également l'obligation, d'une part, d'informer promptement les autorités publiques compétentes de toutes activités illicites mentionnées à l'alinéa précédent qui leur seraient signalées et qu'exerceraient les destinataires de leurs services, et, d'autre part, de rendre publics les moyens qu'elles consacrent à la lutte contre ces activités illicites.
Compte tenu de l'intérêt général attaché à la répression des activités illégales de jeux d'argent, les personnes mentionnées aux 1 et 2 mettent en place, dans des conditions fixées par décret, un dispositif facilement accessible et visible permettant de signaler à leurs abonnés les services de communication au public en ligne tenus pour répréhensibles par les autorités publiques compétentes en la matière. Elles informent également leurs abonnés des risques encourus par eux du fait d'actes de jeux réalisés en violation de la loi.
Tout manquement aux obligations définies aux quatrième et cinquième alinéas est puni des peines prévues au 1 du VI. ;
8.L'autorité judiciaire peut prescrire en référé ou sur requête, à toute personne mentionnée au 2 ou, à défaut, à toute personne mentionnée au 1, toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication au public en ligne.
II.-Les personnes mentionnées aux 1 et 2 du I détiennent et conservent les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires.
Elles fournissent aux personnes qui éditent un service de communication au public en ligne des moyens techniques permettant à celles-ci de satisfaire aux conditions d'identification prévues au III.
L'autorité judiciaire peut requérir communication auprès des prestataires mentionnés aux 1 et 2 du I des données mentionnées au premier alinéa.
Les dispositions des articles 226-17, 226-21 et 226-22 du code pénal sont applicables au traitement de ces données.
Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, définit les données mentionnées au premier alinéa et détermine la durée et les modalités de leur conservation.
II bis (1).-Afin de prévenir [Dispositions déclarées non conformes à la Constitution par la décision du Conseil constitutionnel n° 2005-532 DC du 19 janvier 2006] les actes de terrorisme, les agents individuellement désignés et dûment habilités des services de police et de gendarmerie nationales spécialement chargés de ces missions peuvent exiger des prestataires mentionnés aux 1 et 2 du I la communication des données conservées et traitées par ces derniers en application du présent article.
Les demandes des agents sont motivées et soumises à la décision de la personnalité qualifiée instituée par l'article L. 34-1-1 du code des postes et des communications électroniques selon les modalités prévues par le même article. La Commission nationale de contrôle des interceptions de sécurité exerce son contrôle selon les modalités prévues par ce même article.
Les modalités d'application des dispositions du présent II bis sont fixées par décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés et de la Commission nationale de contrôle des interceptions de sécurité, qui précise notamment la procédure de suivi des demandes et les conditions et durée de conservation des données transmises.
III.-1. Les personnes dont l'activité est d'éditer un service de communication au public en ligne mettent à disposition du public, dans un standard ouvert :
a) S'il s'agit de personnes physiques, leurs nom, prénoms, domicile et numéro de téléphone et, si elles sont assujetties aux formalités d'inscription au registre du commerce et des sociétés ou au répertoire des métiers, le numéro de leur inscription ;
b) S'il s'agit de personnes morales, leur dénomination ou leur raison sociale et leur siège social, leur numéro de téléphone et, s'il s'agit d'entreprises assujetties aux formalités d'inscription au registre du commerce et des sociétés ou au répertoire des métiers, le numéro de leur inscription, leur capital social, l'adresse de leur siège social ;
c) Le nom du directeur ou du codirecteur de la publication et, le cas échéant, celui du responsable de la rédaction au sens de l'article 93-2 de la loi n° 82-652 du 29 juillet 1982 précitée ;
d) Le nom, la dénomination ou la raison sociale et l'adresse et le numéro de téléphone du prestataire mentionné au 2 du I.
2. Les personnes éditant à titre non professionnel un service de communication au public en ligne peuvent ne tenir à la disposition du public, pour préserver leur anonymat, que le nom, la dénomination ou la raison sociale et l'adresse du prestataire mentionné au 2 du I, sous réserve de lui avoir communiqué les éléments d'identification personnelle prévus au 1.
Les personnes mentionnées au 2 du I sont assujetties au secret professionnel dans les conditions prévues aux articles 226-13 et 226-14 du code pénal, pour tout ce qui concerne la divulgation de ces éléments d'identification personnelle ou de toute information permettant d'identifier la personne concernée. Ce secret professionnel n'est pas opposable à l'autorité judiciaire.
IV.-Toute personne nommée ou désignée dans un service de communication au public en ligne dispose d'un droit de réponse, sans préjudice des demandes de correction ou de suppression du message qu'elle peut adresser au service, [Dispositions déclarées non conformes à la Constitution par décision du Conseil constitutionnel n° 2004-496 DC du 10 juin 2004].
La demande d'exercice du droit de réponse est adressée au directeur de la publication ou, lorsque la personne éditant à titre non professionnel a conservé l'anonymat, à la personne mentionnée au 2 du I qui la transmet sans délai au directeur de la publication. Elle est présentée au plus tard dans un délai de trois mois à compter de [Dispositions déclarées non conformes à la Constitution par décision du Conseil constitutionnel n° 2004-496 DC du 10 juin 2004] la mise à disposition du public du message justifiant cette demande.
Le directeur de la publication est tenu d'insérer dans les trois jours de leur réception les réponses de toute personne nommée ou désignée dans le service de communication au public en ligne sous peine d'une amende de 3 750 Euros, sans préjudice des autres peines et dommages-intérêts auxquels l'article pourrait donner lieu.

Les conditions d'insertion de la réponse sont celles prévues par l'article 13 de la loi du 29 juillet 1881 précitée. La réponse sera toujours gratuite.
Un décret en Conseil d'Etat fixe les modalités d'application du présent IV.
V.-Les dispositions des chapitres IV et V de la loi du 29 juillet 1881 précitée sont applicables aux services de communication au public en ligne et la prescription acquise dans les conditions prévues par l'article 65 de ladite loi [Dispositions déclarées non conformes à la Constitution par décision du Conseil constitutionnel n° 2004-496 DC du 10 juin 2004].
[Dispositions déclarées non conformes à la Constitution par décision du Conseil constitutionnel n° 2004-496 DC du 10 juin 2004]
VI.-1. Est puni d'un an d'emprisonnement et de 75 000 Euros d'amende le fait, pour une personne physique ou le dirigeant de droit ou de fait d'une personne morale exerçant l'une des activités définies aux 1 et 2 du I, de ne pas satisfaire aux obligations définies aux quatrième et cinquième alinéas du 7 du I, de ne pas avoir conservé les éléments d'information visés au II ou de ne pas déférer à la demande d'une autorité judiciaire d'obtenir communication desdits éléments.
Les personnes morales peuvent être déclarées pénalement responsables de ces infractions dans les conditions prévues à l'article 121-2 du code pénal. Elles encourent une peine d'amende, suivant les modalités prévues par l'article 131-38 du même code, ainsi que les peines mentionnées aux 2° et 9° de l'article 131-39 de ce code.L'interdiction mentionnée au 2° de cet article est prononcée pour une durée de cinq ans au plus et porte sur l'activité professionnelle dans l'exercice ou à l'occasion de laquelle l'infraction a été commise.
2. Est puni d'un an d'emprisonnement et de 75 000 Euros d'amende le fait, pour une personne physique ou le dirigeant de droit ou de fait d'une personne morale exerçant l'activité définie au III, de ne pas avoir respecté les prescriptions de ce même article.
Les personnes morales peuvent être déclarées pénalement responsables de ces infractions dans les conditions prévues à l'article 121-2 du code pénal. Elles encourent une peine d'amende, suivant les modalités prévues par l'article 131-38 du même code, ainsi que les peines mentionnées aux 2° et 9° de l'article 131-39 de ce code.L'interdiction mentionnée au 2° de cet article est prononcée pour une durée de cinq ans au plus et porte sur l'activité professionnelle dans l'exercice ou à l'occasion de laquelle l'infraction a été commise.

Article 7

Lorsque les personnes visées au 1 du I de l'article 6 invoquent, à des fins publicitaires, la possibilité qu'elles offrent de télécharger des fichiers dont elles ne sont pas les fournisseurs, elles font figurer dans cette publicité une mention facilement identifiable et lisible rappelant que le piratage nuit à la création artistique.

CHAPITRE III :
Régulation de la communication.

TITRE Ier :
DE LA LIBERTÉ DE COMMUNICATION EN LIGNE

Article 10

A modifié les dispositions suivantes :
Modifie Loi n°86-1067 du 30 septembre 1986 - art. 42-1 (M)
Modifie Loi n°86-1067 du 30 septembre 1986 - art. 42-2 (M)

Article 42-1

Modifié par Loi n°2004-575 du 21 juin 2004 - art. 10 JORF 22 juin 2004

Si un éditeur ou un distributeur de services de radiodiffusion sonore ou de télévision ne se conforme pas aux mises en demeure qui lui ont été adressées, le Conseil supérieur de l'audiovisuel peut prononcer à son encontre, compte tenu de la gravité du manquement, une des sanctions suivantes :

1° La suspension de l'édition ou de la distribution du ou des services ou d'une partie du programme pour un mois au plus ;

2° La réduction de la durée de l'autorisation ou de la convention dans la limite d'une année ;

3° Une sanction pécuniaire assortie éventuellement d'une suspension de l'édition ou de la distribution du ou des services ou d'une partie du programme ;

4° Le retrait de l'autorisation ou la résiliation unilatérale de la convention.

Article 42-2

Modifié par Loi n°2004-575 du 21 juin 2004 - art. 10 JORF 22 juin 2004

Le montant de la sanction pécuniaire doit être fonction de la gravité des manquements commis et en relation avec les avantages tirés du manquement, sans pouvoir excéder 3 p. 100 du chiffre d'affaires hors taxes, réalisé au cours du dernier exercice clos calculé sur une période de douze mois. Ce maximum est porté à 5 p. 100 en cas de nouvelle violation de la même obligation.

Lorsque le manquement est constitutif d'une infraction pénale, le montant de la sanction pécuniaire ne peut excéder celui prévu pour l'amende pénale.

Lorsque le Conseil supérieur de l'audiovisuel a prononcé une sanction pécuniaire devenue définitive avant que le juge pénal ait statué définitivement sur les mêmes faits ou des faits connexes, celui-ci peut ordonner que la sanction pécuniaire s'impute sur l'amende qu'il prononce.

Pour l'application du présent article, sont agrégées au montant du chiffre d'affaires l'ensemble des recettes publicitaires provenant de l'activité du service.

Les sanctions pécuniaires sont recouvrées comme les créances de l'Etat étrangères à l'impôt et au domaine.

Article 11

A modifié les dispositions suivantes :

Modifie Loi n°86-1067 du 30 septembre 1986 - art. 42-4 (M)

Article 42-4

Modifié par Loi n°2004-575 du 21 juin 2004 - art. 11 JORF 22 juin 2004

Dans tous les cas de manquement aux obligations incombant aux éditeurs de services de radiodiffusion sonore ou de télévision, le Conseil supérieur de l'audiovisuel peut ordonner l'insertion dans les programmes d'un communiqué dont il fixe les termes et les conditions de diffusion. Le Conseil supérieur de l'audiovisuel demande à l'intéressé de lui présenter ses observations dans un délai de deux jours francs à compter de la réception de cette demande. La décision est ensuite prononcée sans que soit mise en oeuvre la procédure prévue à l'article 42-7. Le refus du titulaire de se conformer à cette décision est passible d'une sanction pécuniaire dans les conditions fixées à l'article 42-2.

Article 12

A modifié les dispositions suivantes :

Modifie Loi n°86-1067 du 30 septembre 1986 - art. 48-2 (V)

Article 48-2

Modifié par Loi n°2004-575 du 21 juin 2004 - art. 12 JORF 22 juin 2004

Si une société mentionnée à l'article 44 ne se conforme pas aux mises en demeure qui lui ont été adressées, le Conseil supérieur de l'audiovisuel peut prononcer à son encontre la suspension d'une partie du programme pour un mois au plus ou une sanction pécuniaire dans les limites définies à l'article 42-2.

Article 13

A modifié les dispositions suivantes :

Modifie Loi n°86-1067 du 30 septembre 1986 - art. 1 (M)

Article 1

Modifié par Loi n°2004-575 du 21 juin 2004 - art. 1 (V) JORF 22 juin 2004
Modifié par Loi n°2004-575 du 21 juin 2004 - art. 13 JORF 22 juin 2004

La communication au public par voie électronique est libre.

L'exercice de cette liberté ne peut être limité que dans la mesure requise, d'une part, par le respect de la dignité de la personne humaine, de la liberté et de la propriété d'autrui, du caractère pluraliste de l'expression des courants de pensée et d'opinion et, d'autre part, par la protection de l'enfance et de l'adolescence, par la sauvegarde de l'ordre public, par les besoins de la défense nationale, par les exigences de service public, par les contraintes techniques inhérentes aux moyens de communication, ainsi que par la nécessité, pour les services audiovisuels, de développer la production audiovisuelle.

Les services audiovisuels comprennent les services de communication audiovisuelle telle que définie à l'article 2 ainsi que l'ensemble des services mettant à disposition du public ou d'une catégorie de public des oeuvres audiovisuelles, cinématographiques ou sonores, quelles que soient les modalités techniques de cette mise à disposition.

TITRE III

DE LA SÉCURITÉ DANS L'ÉCONOMIE NUMÉRIQUE

Chapitre II

Lutte contre la cybercriminalité

Article 41

Modifie CODE DE PROCEDURE PENALE - art. 56 (M)

L'article 56 du code de procédure pénale est ainsi modifié :

1° Au premier alinéa, après le mot : « documents », sont insérés les mots : « , données informatiques » et, après le mot : « pièces », il est inséré le mot : « , informations » ;

2° Au deuxième alinéa, les mots : « ou documents » sont remplacés par les mots : « , documents ou données informatiques » ;

3° Le cinquième alinéa est remplacé par trois alinéas ainsi rédigés :

« Il est procédé à la saisie des données informatiques nécessaires à la manifestation de la vérité en plaçant sous main de justice soit le support physique de ces données, soit une copie réalisée en présence des personnes qui assistent à la perquisition.

« Si une copie est réalisée, il peut être procédé, sur instruction du procureur de la République, à l'effacement définitif, sur le support physique qui n'a pas été placé sous main de justice, des données informatiques dont la détention ou l'usage est illégal ou dangereux pour la sécurité des personnes ou des biens.

« Avec l'accord du procureur de la République, l'officier de police judiciaire ne maintient que la saisie des objets, documents et données informatiques utiles à la manifestation de la vérité. »

Article 42

Modifie CODE DE PROCEDURE PENALE - art. 94 (V)

A l'article 94 du code de procédure pénale, après les mots : « des objets », sont insérés les mots : « ou des données informatiques ».

Article 43

Modifie CODE DE PROCEDURE PENALE - art. 97 (M)

L'article 97 du code de procédure pénale est ainsi modifié :
1° Au premier alinéa, après les mots : « des documents », sont insérés les mots : « ou des données informatiques » ;

2° Au deuxième alinéa, les mots : « les objets et documents » sont remplacés par les mots : « les objets, documents ou données informatiques » ;

3° Au troisième alinéa, les mots : « et documents » sont remplacés par les mots : « , documents et données informatiques » ;

4° Au cinquième alinéa, après le mot : « documents », sont insérés les mots : « ou des données informatiques » ;

5° Après le deuxième alinéa, sont insérés deux alinéas ainsi rédigés :
« Il est procédé à la saisie des données informatiques nécessaires à la manifestation de la vérité en plaçant sous main de justice soit le support physique de ces données, soit une copie réalisée en présence des personnes qui assistent à la perquisition.
« Si une copie est réalisée dans le cadre de cette procédure, il peut être procédé, sur ordre du juge d'instruction, à l'effacement définitif, sur le support physique qui n'a pas été placé sous main de justice, des données informatiques dont la détention ou l'usage est illégal ou dangereux pour la sécurité des personnes ou des biens. »

Article 44

Modifie Code pénal - art. 227-23 (M)

L'article 227-23 du code pénal est ainsi modifié :
1° Le premier alinéa est complété par une phrase ainsi rédigée :
« La tentative est punie des mêmes peines. » ;

2° Au deuxième alinéa, après le mot : « fait », sont insérés les mots : « d'offrir ou ».

Article 45

Modifie Code pénal - art. 323-1 (V)
Modifie Code pénal - art. 323-2 (V)
Modifie Code pénal - art. 323-3 (V)

I. - L'article 323-1 du code pénal est ainsi modifié :

1° Au premier alinéa, les mots : « d'un an » sont remplacés par les mots : « deux ans » et la somme : « 15 000 EUR » est remplacée par la somme : « 30 000 EUR » ;

2° Au second alinéa, les mots : « deux ans » sont remplacés par les mots : « trois ans » et la somme : « 30 000 EUR » est remplacée par la somme : « 45 000 EUR ».

II. - A l'article 323-2 du même code, les mots : « trois ans » sont remplacés par les mots : « cinq ans » et la somme : « 45 000 EUR » est remplacée par la somme : « 75 000 EUR ».

III. - A l'article 323-3 du même code, les mots : « trois ans » sont remplacés par les mots : « cinq ans » et la somme : « 45 000 EUR » est remplacée par la somme : « 75 000 EUR ».

Article 46

A modifié les dispositions suivantes :
Crée Code pénal - art. 323-3-1 (V)
Modifie Code pénal - art. 323-4 (V)
Modifie Code pénal - art. 323-7 (V)

I. - Après l'article 323-3 du code pénal, il est inséré un article 323-3-1 ainsi rédigé :

« Art. 323-3-1. - Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés 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. »

II. - Aux articles 323-4 et 323-7 du même code, les mots : « les articles 323-1 à 323-3 » sont remplacés par les mots : « les articles 323-1 à 323-3-1 ».

Fait à Paris, le 21 juin 2004.

Par le Président de la République : **Jacques Chirac**
Le Premier ministre : **Jean-Pierre Raffarin**
Le ministre d'Etat, ministre de l'économie, des finances et de l'industrie : **Nicolas Sarkozy**
Le garde des sceaux, ministre de la justice : **Dominique Perben**
Le ministre de la culture et de la communication : **Renaud Donnedieu de Vabres**
La ministre de l'outre-mer : **Brigitte Girardin**
Le ministre délégué à l'industrie : **Patrick Devedjian**

يمكن الإطلاع على هذا القانون بكامله في صفحة الأنترنت التالية :
http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=ECOX0200175L

ملحق رقم : 9

قانون 88-19 لــ 5 جانفي 1988 المتعلق : "بالمساسات بأنظمة المعالجة الآلية للمعطيات"

المعدل بموجب القانون رقم 2004-575 المؤرخ في 21 جوان 2004

مقتطف من قانون العقوبات الفرنسي :

Extrait du Code Pénal Français :

Chapitre III : Des atteintes aux systèmes de traitement automatisé de données

Article 323-1 ***(Loi nº 2004-575 du 21 juin 2004 art. 45 I Journal Officiel du 22 juin 2004)***

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 de 30000 euros 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 ans
d'emprisonnement et de 45000 euros d'amende.

Article 323-2 ***(Loi nº 2004-575 du 21 juin 2004 art. 45 II Journal Officiel du 22 juin 2004)***

Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75000 euros d'amende.

Article 323-3 ***(Loi nº 2004-575 du 21 juin 2004 art. 45 III Journal Officiel du 22 juin 2004)***

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.

Article 323-3-1 ***(Inséré par Loi nº 2004-575 du 21 juin 2004 art. 46 I Journal Officiel du 22 juin 2004)***

Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés 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.

Article 323-4 ***(Loi nº 2004-575 du 21 juin 2004 art. 46 II Journal Officiel du 22 juin 2004)***

La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3-1 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Article 323-5
Les personnes physiques coupables des délits prévus au présent chapitre encourent également les peines complémentaires suivantes :

1º L'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, suivant les modalités de l'article 131-26 ;

2º L'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise ;

3º La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution ;

4º La fermeture, pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;

5º L'exclusion, pour une durée de cinq ans au plus, des marchés publics ;

6º L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ;

7º L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35.

Article 323-6

Les personnes morales peuvent être déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies au présent chapitre.

Les peines encourues par les personnes morales sont :
1º L'amende, suivant les modalités prévues par l'article 131-38 ;
2º Les peines mentionnées à l'article 131-39.
L'interdiction mentionnée au 2º de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise.

***Article 323-7** (Loi nº 2004-575 du 21 juin 2004 art. 46 II Journal Officiel du 22 juin 2004)*

La tentative des délits prévus par les articles 323-1 à 323-3-1 est punie des mêmes peines.

أنظر صفحة الأنترنت التالية :

http://www.legifrance.gouv.fr/WAspad/VisuArticleCode?commun=CPENAL&code=&h0=CPENALLL.rcv&h1=3&h3=30

ملحق رقم : 10

إتفاقية بيدابـاست الأوروبية حول الإجرام المعلوماتي
مصادق عليها أمام المجلس الأوروبي في بيدابـاست في 23 نوفمبر 2001

LA CONVENTION DE BUDAPEST SUR LA CYBERCRIMINALITÉ
Ratifié par le conseille européens à Budapest le 23 novembre 2001

Préambule

Les Etats membres du Conseil de l'Europe et les autres Etats signataires,
Considérant que le but du Conseil de l'Europe est de réaliser une union plus étroite entre ses membres;
Reconnaissant l'intérêt d'intensifier la coopération avec les autres Etats parties à la Convention;
Convaincus de la nécessité de mener, en priorité, une politique pénale commune destinée à protéger la société de la criminalité dans le cyberespace, notamment par l'adoption d'une législation appropriée et par l'amélioration de la coopération internationale;
Conscients des profonds changements engendrés par la numérisation, la convergence et la mondialisation permanente des réseaux informatiques;
Préoccupés par le risque que les réseaux informatiques et l'information électronique soient utilisés également pour commettre des infractions pénales et que les preuves de ces infractions soient stockées et transmises par le biais de ces réseaux;
Reconnaissant la nécessité d'une coopération entre les Etats et l'industrie privée dans la lutte contre la cybercriminalité, et le besoin de protéger les intérêts légitimes dans l'utilisation et le développement des technologies de l'information;
Estimant qu'une lutte bien menée contre la cybercriminalité requiert une coopération internationale en matière pénale accrue, rapide et efficace;
Convaincus que la présente Convention est nécessaire pour prévenir les actes portant atteinte à la confidentialité, à l'intégrité et à la disponibilité des systèmes informatiques, des réseaux et des données, ainsi que l'usage frauduleux de tels systèmes, réseaux et données, en assurant l'incrimination de ces comportements, tels que décrits dans la présente Convention, et l'adoption de pouvoirs suffisants pour permettre une lutte efficace contre ces infractions pénales, en en facilitant la détection, l'investigation et la poursuite, tant au plan national qu'au niveau international, et en prévoyant des dispositions matérielles en vue d'une coopération internationale rapide et fiable;
Gardant à l'esprit la nécessité de garantir un équilibre adéquat entre les intérêts de l'action répressive et le respect des droits de l'homme fondamentaux, tels que garantis dans la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales du Conseil de l'Europe (1950), dans le Pacte international relatif aux droits civils et politiques des Nations Unies (1966), ainsi que dans d'autres conventions internationales applicables en matière de droits de l'homme, qui réaffirment le droit à ne pas être inquiété pour ses opinions, le droit à la liberté d'expression, y compris la liberté de rechercher, d'obtenir et de communiquer des informations et des idées de toute nature, sans considération de frontière, ainsi que le droit au respect de la vie privée;
Conscients également du droit à la protection des données personnelles, tel que spécifié, par exemple, par la Convention de 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel;
Considérant la Convention des Nations Unies relative aux droits de l'enfant (1989) et la Convention de l'Organisation internationale du travail sur les pires formes de travail des enfants (1999);
Tenant compte des conventions existantes du Conseil de l'Europe sur la coopération en matière pénale, ainsi que d'autres traités similaires conclus entre les Etats membres du Conseil de l'Europe et d'autres Etats, et soulignant que la présente Convention a pour but de les compléter en vue de rendre plus efficaces les enquêtes et les procédures pénales portant sur des infractions pénales en relation avec des systèmes et des données informatiques, ainsi que de permettre la collecte des preuves électroniques d'une infraction pénale;
Se félicitant des récentes initiatives destinées à améliorer la compréhension et la coopération internationales aux fins de la lutte contre la criminalité dans le cyberespace, notamment des actions menées par les Nations Unies, l'OCDE, l'Union européenne et le G8;
Rappelant les Recommandations du Comité des Ministres n° R (85) 10 concernant l'application pratique de la Convention européenne d'entraide judiciaire en matière pénale relative aux commissions rogatoires pour la surveillance des télécommunications, n° R (88) 2 sur des mesures visant à combattre la piraterie dans le domaine du droit d'auteur et des droits voisins, n° R (87) 15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police, n° R (95) 4 sur la protection des données à caractère personnel dans le domaine des services de télécommunication, eu égard notamment aux services téléphoniques, et n° R (89) 9 sur la criminalité en relation avec l'ordinateur, qui indique aux législateurs nationaux des principes directeurs pour définir certaines infractions informatiques, ainsi que n° R (95) 13 relative aux problèmes de procédure pénale liés à la technologie de l'information;
Eu égard à la Résolution n° 1, adoptée par les ministres européens de la Justice lors de leur 21e Conférence (Prague, 10 et 11 juin 1997), qui recommande au Comité des Ministres de soutenir les activités concernant la cybercriminalité menées par le Comité européen pour les problèmes criminels (CDPC) afin de rapprocher les législations pénales nationales et de permettre l'utilisation de moyens d'investigation efficaces en matière d'infractions informatiques, ainsi qu'à la Résolution n° 3, adoptée lors de la 23e Conférence des ministres européens de la Justice (Londres, 8 et 9 juin 2000), qui encourage les parties aux négociations à poursuivre leurs efforts afin de trouver des solutions permettant au plus grand nombre d'Etats d'être parties à la Convention et qui reconnaît la nécessité de disposer d'un mécanisme rapide et efficace de coopération internationale qui tienne dûment compte des exigences spécifiques de la lutte contre la cybercriminalité;
Prenant également en compte le plan d'action adopté par les chefs d'Etat et de gouvernement du Conseil de l'Europe à l'occasion de leur 2e Sommet (Strasbourg, 10 et 11 octobre 1997) afin de trouver des réponses communes au développement des nouvelles technologies de l'information, fondées sur les normes et les valeurs du Conseil de l'Europe,
Sont convenus de ce qui suit:

Chapitre I – Terminologie

Article 1 – Définitions

Aux fins de la présente Convention,
a) l'expression «système informatique» désigne tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données;
b) l'expression «données informatiques» 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;
c) l'expression «fournisseur de services» désigne:
i tout entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique, et
ii toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs.
d) ***«données relatives au trafic»*** désigne toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent.

Chapitre II – Mesures à prendre au niveau national

Section 1 – Droit pénal matériel

Titre 1 – Infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques

Article 2 – Accès illégal

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'accès intentionnel 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 informatiques ou dans une autre intention délictueuse, ou soit en relation avec un système informatique connecté à un autre système informatique.

Article 3 – Interception illégale

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'interception intentionnelle et sans droit, effectuée par des moyens techniques, de données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques. Une Partie peut exiger que l'infraction soit commise dans une intention délictueuse ou soit en relation avec un système informatique connecté à un autre système informatique.

Article 4 – Atteinte à l'intégrité des données

1) Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à 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 paragraphe 1 entraîne des dommages sérieux.

Article 5 – Atteinte à l'intégrité du système

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'entrave grave, intentionnelle et sans droit, au fonctionnement d'un système informatique, par l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, l'altération ou la suppression de données informatiques.

Article 6 – Abus de dispositifs

1) Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, lorsqu'elles sont commises intentionnellement et sans droit:
a) la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition:
i d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions établies conformément aux articles 2 à 5 ci-dessus;
ii d'un mot de passe, d'un code d'accès ou de données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique, dans l'intention qu'ils soient utilisés afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5; et
b) la possession d'un élément visé aux paragraphes a.i ou ii ci-dessus, dans l'intention qu'il soit utilisé afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5. Une Partie peut exiger en droit interne qu'un certain nombre de ces éléments soit détenu pour que la responsabilité pénale soit engagée.
2) Le présent article ne saurait être interprété comme imposant une responsabilité pénale lorsque la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition mentionnées au paragraphe 1 du présent article n'ont pas pour but de commettre une infraction établie conformément aux articles 2 à 5 de la présente Convention, comme dans le cas d'essai autorisé ou de protection d'un système informatique.
3) Chaque Partie peut se réserver le droit de ne pas appliquer le paragraphe 1 du présent article, à condition que cette réserve ne porte pas sur la vente, la distribution ou toute autre mise à disposition des éléments mentionnés au paragraphe 1.a.ii du présent article.

Titre 2 – Infractions informatiques

Article 7 – Falsification informatique

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'introduction, l'altération, l'effacement ou la suppression intentionnels et sans droit de données informatiques, engendrant des données non authentiques, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient authentiques, qu'elles soient ou non directement lisibles et intelligibles. Une Partie peut exiger une intention frauduleuse ou une intention délictueuse similaire pour que la responsabilité pénale soit engagée.

Article 8 – Fraude informatique

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait intentionnel et sans droit de causer un préjudice patrimonial à autrui:
a) par toute introduction, altération, effacement ou suppression de données informatiques;
b) par toute forme d'atteinte au fonctionnement d'un système informatique, dans l'intention, frauduleuse ou délictueuse, d'obtenir sans droit un bénéfice économique pour soi-même ou pour autrui.

Titre 3 – Infractions se rapportant au contenu

Article 9 – Infractions se rapportant à la pornographie enfantine

1) Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les comportements suivants
lorsqu'ils sont commis intentionnellement et sans droit:
a) la production de pornographie enfantine en vue de sa diffusion par le biais d'un système informatique;
b) l'offre ou la mise à disposition de pornographie enfantine par le biais d'un système informatique;
c) la diffusion ou la transmission de pornographie enfantine par le biais d'un système informatique;
d) le fait de se procurer ou de procurer à autrui de la pornographie enfantine par le biais d'un système informatique;
e) la possession de pornographie enfantine dans un système informatique ou un moyen de stockage de données informatiques.
2) Aux fins du paragraphe 1 ci-dessus, le terme «pornographie enfantine» comprend toute matière pornographique représentant de manière visuelle:
a) un mineur se livrant à un comportement sexuellement explicite;
b) une personne qui apparaît comme un mineur se livrant à un comportement sexuellement explicite;
c) des images réalistes représentant un mineur se livrant à un comportement sexuellement explicite.
3) Aux fins du paragraphe 2 ci-dessus, le terme «mineur» désigne toute personne âgée de moins de 18 ans. Une Partie peut toutefois exiger une limite d'âge inférieure, qui doit être au minimum de 16 ans.
4) Une Partie peut se réserver le droit de ne pas appliquer, en tout ou en partie, les paragraphes 1, alinéas d. et e, et 2, alinéas b. et c.

Titre 4 – Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes

Article 10 – Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes

1) Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les atteintes à la propriété intellectuelle, définies par la législation de ladite Partie, conformément aux obligations que celle-ci a souscrites en application de l'Acte de Paris du 24 juillet 1971 portant révision de la Convention de Berne pour la protection des oeuvres littéraires et artistiques, de l'Accord sur les aspects commerciaux des droits de propriété intellectuelle et du traité de l'OMPI sur la propriété intellectuelle, à l'exception de tout droit moral conféré par ces conventions, lorsque de tels actes sont commis délibérément, à une échelle commerciale et au moyen d'un système informatique.
2) Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour
ériger en infraction pénale, conformément à son droit interne, les atteintes aux droits connexes définis par la législation de ladite Partie, conformément aux obligations que cette dernière a souscrites en application de la Convention internationale pour la protection des artistes interprètes ou exécutants, des producteurs de phonogrammes et des organismes de radiodiffusion (Convention de Rome), de l'Accord relatif aux aspects commerciaux des droits de propriété intellectuelle et du Traité de l'OMPI sur les interprétations et exécutions, et les phonogrammes, à l'exception de tout droit moral conféré par ces conventions, lorsque de tels actes sont commis délibérément, à une échelle commerciale et au moyen d'un système informatique.
3) Une Partie peut, dans des circonstances bien délimitées, se réserver le droit de ne pas imposer de responsabilité pénale au titre des paragraphes 1 et 2 du présent article, à condition que d'autres recours efficaces soient disponibles et qu'une telle réserve ne porte pas atteinte aux obligations internationales incombant à cette Partie en application des instruments internationaux mentionnés aux paragraphes 1 et 2 du présent article.

Titre 5 – Autres formes de responsabilité et de sanctions

Article 11 – Tentative et complicité

1) Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute complicité lorsqu'elle est commise intentionnellement en vue de la perpétration d'une des infractions établies en application des articles 2 à 10 de la présente Convention, dans l'intention qu'une telle infraction soit commise.
2) Chaque Partie adopte les mesures législatives et autres qui se révèlent 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 c de la présente Convention.
3) Chaque Partie peut se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 2 du présent article.

Article 12 – Responsabilité des personnes morales

1) Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour que les personnes morales puissent être tenues pour responsables des infractions établies en application de la présente Convention, lorsqu'elles sont commises pour leur compte par toute personne physique, agissant soit individuellement, soit en tant que membre d'un organe de la personne morale, qui exerce un pouvoir de direction en son sein, fondé:
a) sur un pouvoir de représentation de la personne morale;
b) sur une autorité pour prendre des décisions au nom de la personne morale;
c) sur une autorité pour exercer un contrôle au sein de la personne morale.
2) Outre les cas déjà prévus au paragraphe 1 du présent article, chaque Partie adopte les mesures qui se révèlent nécessaires pour s'assurer qu'une personne morale peut être tenue pour responsable lorsque l'absence de surveillance ou de contrôle de la part d'une personne physique mentionnée au paragraphe 1 a rendu possible la commission des infractions établies en application de la présence Convention pour le compte de ladite personne morale par une personne physique agissant sous son autorité.
3) Selon les principes juridiques de la Partie, la responsabilité d'une personne morale peut être pénale, civile ou administrative.
4) Cette responsabilité est établie sans préjudice de la responsabilité pénale des personnes physiques ayant commis l'infraction.

Article 13 – Sanctions et mesures

1) Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour que les infractions pénales établies en application des articles 2 à 11 soient passibles de sanctions effectives, proportionnées et dissuasives, comprenant des peines privatives de liberté.
2) Chaque Partie veille à ce que les personnes morales tenues pour responsables en application de l'article 12 fassent l'objet de sanctions ou de mesures pénales ou non pénales effectives, proportionnées et dissuasives, comprenant des sanctions pécuniaires.

Section 2 – Droit procédural

Titre 1 – Dispositions communes

Article 14 – Portée d'application des mesures du droit de procédure

1) Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour instaurer les pouvoirs et procédures prévus dans la présente section aux fins d'enquêtes ou de procédures pénales spécifiques.
2) Sauf disposition contraire figurant à l'article 21, chaque Partie applique les pouvoirs et procédures mentionnés dans le paragraphe 1 du présent article:
a) aux infractions pénales établies conformément aux articles 2 à 11 de la présente Convention;
b) à toutes les autres infractions pénales commises au moyen d'un système informatique; et
c) à la collecte des preuves électroniques de toute infraction pénale.
3) a) Chaque Partie peut se réserver le droit de n'appliquer les mesures mentionnées à l'article 20 qu'aux infractions ou catégories d'infractions spécifiées dans la réserve, pour autant que l'éventail de ces infractions ou catégories d'infractions ne soit pas plus réduit que celui des infractions auxquelles elle applique les mesures mentionnées à l'article 21. Chaque Partie envisagera de limiter une telle réserve de manière à permettre l'application la plus large possible de la mesure mentionnée à l'article 20.
b) Lorsqu'une Partie, en raison des restrictions imposées par sa législation en vigueur au moment de l'adoption de la présente Convention, n'est pas en mesure d'appliquer les mesures visées aux articles 20 et 21 aux communications transmises dans un système informatique d'un fournisseur de services:
i qui est mis en œuvre pour le bénéfice d'un groupe d'utilisateurs fermé, et
ii qui n'emploie pas les réseaux publics de télécommunication et qui n'est pas connecté à un autre système informatique, qu'il soit public ou privé, cette Partie peut réserver le droit de ne pas appliquer ces mesures à de telles communications. Chaque Partie envisagera de limiter une telle réserve de manière à permettre l'application la plus large possible de la mesure mentionnée aux articles 20 et 21.

Article 15 – Conditions et sauvegardes

1) Chaque Partie veille à ce que l'instauration, la mise en œuvre et l'application des pouvoirs et procédures prévus dans la présente section soient soumises aux conditions et sauvegardes prévues par son droit interne, qui doit assurer une protection adéquate des droits de l'homme et des libertés, en particulier des droits établis conformément aux obligations que celle-ci a souscrites en application de la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales du Conseil de l'Europe (1950) et du Pacte international relatif aux droits civils et politiques des Nations Unies (1966), ou d'autres instruments internationaux applicables concernant les droits de l'homme, et qui doit intégrer le principe de la proportionnalité.
2) Lorsque cela est approprié, eu égard à la nature de la procédure ou du pouvoir concerné, ces conditions et sauvegardes incluent, entre autres, une supervision judiciaire ou d'autres formes de supervision indépendante, des motifs justifiant l'application ainsi que la limitation du champ d'application et de la durée du pouvoir ou de la procédure en question.
3) Dans la mesure où cela est conforme à l'intérêt public, en particulier à la bonne administration de la justice, chaque Partie examine l'effet des pouvoirs et procédures dans cette section sur les droits, responsabilités et intérêts légitimes des tiers.

Titre 2 – Conservation rapide de données informatiques stockées

Article 16 – Conservation rapide de données informatiques stockées

1) Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour permettre à ses autorités compétentes d'ordonner ou d'imposer d'une autre manière la conservation rapide de données électroniques spécifiées, y compris des données relatives au trafic, stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que celles-ci sont particulièrement susceptibles de perte ou de modification.
2) Lorsqu'une Partie fait application du paragraphe 1 ci-dessus, au moyen d'une injonction ordonnant à une personne de conserver des données stockées spécifiées se trouvant en sa possession ou sous son contrôle, cette Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger cette personne à conserver et à protéger l'intégrité desdites données pendant une durée aussi longue que nécessaire, au maximum de quatre-vingt-dix jours, afin de permettre aux autorités compétentes d'obtenir leur divulgation. Une Partie peut prévoir qu'une telle injonction soit renouvelée par la suite.

3) Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger le gardien des données ou une autre personne chargée de conserver celles-ci à garder le secret sur la mise en œuvre desdites procédures pendant la durée prévue par son droit interne.
4) Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

Article 17 – Conservation et divulgation partielle rapides de données relatives au trafic

1) Afin d'assurer la conservation des données relatives au trafic, en application de l'article 16, chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires:
a) pour veiller à la conservation rapide de ces données relatives au trafic, qu'un seul ou plusieurs fournisseurs de services aient participé à la transmission de cette communication; et
b) pour assurer la divulgation rapide à l'autorité compétente de la Partie, ou à une personne désignée par cette autorité, d'une quantité suffisante de données relatives au trafic pour permettre l'identification par la Partie des fournisseurs de services et de la voie par laquelle la communication a été transmise.
2) Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

Titre 3 – Injonction de produire

Article 18 – Injonction de produire

1) Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner:
a) à une personne présente sur son territoire de communiquer les données informatiques spécifiées, en sa possession ou sous son contrôle, qui sont stockées dans un système informatique ou un support de stockage informatique; et
b) à un fournisseur de services offrant des prestations sur le territoire de la Partie, de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services.
2) Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.
3) Aux fins du présent article, l'expression «données relatives aux abonnés» désigne toute information, sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et se rapportant aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir:
a) le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service;
b) l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services;
c) toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de services.

Titre 4 – Perquisition et saisie de données informatiques stockées

Article 19 – Perquisition et saisie de données informatiques stockées

1) Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à perquisitionner ou à accéder d'une façon similaire:
a) à un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui y sont stockées; et
b) à un support du stockage informatique permettant de stocker des données informatiques
sur son territoire.
2) Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour veiller à ce que, lorsque ses autorités perquisitionnent ou accèdent d'une façon similaire à un système informatique spécifique ou à une partie de celui-ci, conformément au paragraphe 1.a, et ont des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci situé sur son territoire, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour ce système initial, lesdites autorités soient en mesure d'étendre rapidement la perquisition ou l'accès d'une façon similaire à l'autre système.
3) Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à saisir ou à obtenir d'une façon similaire les données informatiques pour lesquelles l'accès a 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 ces données informatiques;
c) préserver l'intégrité des données informatiques stockées pertinentes;
d) rendre inaccessibles ou enlever ces données informatiques du système informatique consulté.
4) Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner à toute personne connaissant le fonctionnement du système informatique ou les mesures appliquées pour protéger les données informatiques qu'il contient de fournir toutes les informations raisonnablement nécessaires, pour permettre l'application des mesures visées par les paragraphes 1 et 2.
5) Les pouvoirs et procédures mentionnés dans cet article doivent être soumis aux articles 14 et 15.

Titre 5 – Collecte en temps réel de données informatiques

Article 20 – Collecte en temps réel des données relatives au trafic

1) Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes:
a) à collecter ou enregistrer par l'application de moyens techniques existant sur son territoire, et
b) à obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes:
i à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, ou
ii à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer, en temps réel, les données relatives au trafic associées à des communications spécifiques transmises sur son territoire au moyen d'un système informatique.

2) Lorsqu'une Partie, en raison des principes établis de son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe 1.a, elle peut à la place, adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données relatives au trafic associées à des communications spécifiques transmises sur son territoire par l'application de moyens techniques existant sur ce territoire.
3) Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté ainsi que toute information à ce sujet.
4) Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

Article 21 – Interception de données relatives au contenu

1) Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes en ce qui concerne un éventail d'infractions graves à définir en droit interne :
a) à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, et
b) à obliger un fournisseur de services, dans le cadre de ses capacités techniques:
i à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, ou
ii à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer, en temps réel, les données relatives au contenu de communications spécifiques sur son territoire, transmises au moyen d'un système informatique.
2) Lorsqu'une Partie, en raison des principes établis dans son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe 1.a, elle peut à la place adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données relatives au contenu de communications spécifiques transmises sur son territoire par l'application de moyens techniques existant sur ce territoire.
3) Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté, ainsi que toute information à ce sujet.
4) Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

Section 3 – Compétence

Article 22 – Compétence

1) Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires 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 Etat.
2) Chaque Partie peut se réserver le droit de ne pas appliquer, ou de n'appliquer que dans des cas ou des conditions spécifiques, les règles de compétence définies aux paragraphes 1.b à 1.d du présent article ou dans une partie quelconque de ces paragraphes.
3) Chaque Partie adopte les mesures qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction mentionnée à l'article 24, paragraphe 1, de la présente Convention, lorsque l'auteur présumé de l'infraction est présent sur son territoire et ne peut être extradé vers une autre Partie au seul titre de sa nationalité, après une demande d'extradition.
4) La présente Convention n'exclut aucune compétence pénale exercée par une Partie conformément à son droit interne.
5) Lorsque plusieurs Parties revendiquent une compétence à l'égard d'une infraction présumée visée dans la présente Convention, les Parties concernées se concertent, lorsque cela est opportun, afin de déterminer la mieux à même d'exercer les poursuites.

Chapitre III – Coopération internationale

Section 1 – Principes généraux

Titre 1 – Principes généraux relatifs à la coopération internationale

Article 23 – Principes généraux relatifs à la coopération internationale

Les Parties coopèrent les unes avec les autres, conformément aux dispositions du présent chapitre, en application des instruments internationaux pertinents sur la coopération internationale en matière pénale, des arrangements reposant sur des législations uniformes ou réciproques et de leur droit national, dans la mesure la plus large possible, aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et des données informatiques ou pour recueillir les preuves, sous forme électronique, d'une infraction pénale.

Titre 2 – Principes relatifs à l'extradition

Article 24 – Extradition

1) a Le présent article s'applique à l'extradition entre les Parties pour les infractions pénales définies conformément aux articles 2 à 11 de la présente Convention, à condition qu'elles soient punissables dans la législation des deux Parties concernées par une peine privative de liberté pour une période maximale d'au moins un an, ou par une peine plus sévère.
b) Lorsqu'il est exigé une peine minimale différente, sur la base d'un traité d'extradition tel qu'applicable entre deux ou plusieurs parties, y compris la Convention européenne d'extradition (STE n° 24), ou d'un arrangement reposant sur des législations uniformes ou réciproques, la peine minimale prévue par ce traité ou cet arrangement s'applique.
2) Les infractions pénales décrites au paragraphe 1 du présent article sont considérées comme incluses en tant qu'infractions pouvant donner lieu à extradition dans tout traité d'extradition existant entre ou parmi les Parties. Les Parties s'engagent à inclure de telles infractions comme infractions pouvant donner lieu à extradition dans tout traité d'extradition pouvant être conclu entre ou parmi elles.

3) Lorsqu'une Partie conditionne l'extradition à l'existence d'un traité et reçoit une demande d'extradition d'une autre Partie avec laquelle elle n'a pas conclu de traité d'extradition, elle peut considérer la présente Convention comme fondement juridique pour l'extradition au regard de toute infraction pénale mentionnée au paragraphe 1 du présent article.
4) Les Parties qui ne conditionnent pas l'extradition à l'existence d'un traité reconnaissent les infractions pénales mentionnées au paragraphe 1 du présent article comme des infractions pouvant donner lieu entre elles à l'extradition.
5) L'extradition est soumise aux conditions prévues par le droit interne de la Partie requise ou par les traités d'extradition en vigueur, y compris les motifs pour lesquels la Partie requise peut refuser l'extradition.
6) Si l'extradition pour une infraction pénale mentionnée au paragraphe 1 du présent article est refusée uniquement sur la base de la nationalité de la personne recherchée ou parce que la Partie requise s'estime compétente pour cette infraction, la Partie requise soumet l'affaire, à la demande de la Partie requérante, à ses autorités compétentes aux fins de poursuites, et rendra compte, en temps utile, de l'issue de l'affaire à la Partie requérante.
Les autorités en question prendront leur décision et mèneront l'enquête et la procédure de la même manière que pour toute autre infraction de nature comparable, conformément à la législation de cette Partie.
7) a) Chaque Partie communique au Secrétaire Général du Conseil de l'Europe, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, le nom et l'adresse de chaque autorité responsable de l'envoi ou de la réception d'une demande d'extradition ou d'arrestation provisoire, en l'absence de traité.
b) Le Secrétaire Général du Conseil de l'Europe établit et tient à jour un registre des autorités ainsi désignées par les Parties. Chaque Partie doit veiller en permanence à l'exactitude des données figurant dans le registre.

Titre 3 – Principes généraux relatifs à l'entraide

Article 25 – Principes généraux relatifs à l'entraide

1) Les Parties s'accordent l'entraide la plus large possible aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et à des données informatiques, ou afin de recueillir les preuves sous forme électronique d'une infraction pénale.
2) Chaque Partie adopte également les mesures législatives et autres qui se révèlent nécessaires pour s'acquitter des obligations énoncées aux articles 27 à 35.
3) Chaque Partie peut, en cas d'urgence, formuler une demande d'entraide ou les communications s'y rapportant par des moyens rapides de communication, tels que la télécopie ou le courrier électronique, pour autant que ces moyens offrent des conditions suffisantes de sécurité et d'authentification (y compris, si nécessaire, le cryptage), avec confirmation officielle ultérieure si l'Etat requis l'exige. L'Etat requis accepte la demande et y répond par n'importe lequel de ces moyens rapides de communication.
4) Sauf disposition contraire expressément prévue dans les articles du présent chapitre, l'entraide est soumise aux conditions fixées par le droit interne de la Partie requise ou par les traités d'entraide applicables, y compris les motifs sur la base desquels la Partie requise peut refuser la coopération. La Partie requise ne doit pas exercer son droit de refuser l'entraide concernant les infractions visées aux articles 2 à 11 au seul motif que la demande porte sur une infraction qu'elle considère comme de nature fiscale.
5) Lorsque, conformément aux dispositions du présent chapitre, la Partie requise est autorisée à subordonner l'entraide à l'existence d'une double incrimination, cette condition sera considérée comme satisfaite si le comportement constituant l'infraction, pour laquelle l'entraide est requise, est qualifié d'infraction pénale par son droit interne, que le droit interne classe ou non l'infraction dans la même catégorie d'infractions ou qu'il la désigne ou non par la même terminologie que le droit de la Partie requérante.

Article 26 – Information spontanée

1) Une Partie peut, dans les limites de son droit interne et en l'absence de demande préalable, communiquer à une autre Partie des informations obtenues dans le cadre de ses propres enquêtes lorsqu'elle estime que cela pourrait aider la Partie destinataire à engager ou à mener à bien des enquêtes ou des procédures au sujet d'infractions pénales établies conformément à la présente Convention, ou lorsque ces informations pourraient aboutir à une demande de coopération formulée par cette Partie au titre du présent chapitre.
2) Avant de communiquer de telles informations, la Partie qui les fournit peut demander qu'elles restent confidentielles ou qu'elles ne soient utilisées qu'à certaines conditions. Si la Partie destinataire ne peut faire droit à cette demande, elle doit en informer l'autre Partie, qui devra alors déterminer si les informations en question devraient néanmoins être fournies. Si la Partie destinataire accepte les informations aux conditions prescrites, elle sera liée par ces dernières.

Titre 4 – Procédures relatives aux demandes d'entraide en l'absence d'accords internationaux applicables

Article 27 – Procédures relatives aux demandes d'entraide en l'absence d'accords internationaux applicables

1) En l'absence de traité d'entraide ou d'arrangement reposant sur des législations uniformes ou réciproques en vigueur entre la Partie requérante et la Partie requise, les dispositions des paragraphes 2 à 9 du présent article s'appliquent. Elles ne s'appliquent pas lorsqu'un traité, un arrangement ou une législation de ce type existent, à moins que les Parties concernées ne décident d'appliquer à la place tout ou partie du reste de cet article.
2) a Chaque Partie désigne une ou plusieurs autorités centrales chargées d'envoyer les demandes d'entraide ou d'y répondre, de les exécuter ou de les transmettre aux autorités compétentes pour leur exécution;
b) Les autorités centrales communiquent directement les unes avec les autres;
c) Chaque Partie, au moment de la signature ou du dépôt de ses instruments de ratification, d'acceptation, d'approbation ou d'adhésion, communique au Secrétaire Général du Conseil de l'Europe les noms et adresses des autorités désignées en application du présent paragraphe;
d) Le Secrétaire Général du Conseil de l'Europe établit et tient à jour un registre des autorités centrales désignées par les Parties. Chaque Partie veille en permanence à l'exactitude des données figurant dans le registre.
3) Les demandes d'entraide sous le présent article sont exécutées conformément à la procédure spécifiée par la Partie requérante, sauf lorsqu'elle est incompatible avec la législation de la Partie requise.
4) Outre les conditions ou les motifs de refus prévus à l'article 25, paragraphe 4, l'entraide peut être refusée par la Partie requise:
a) si la demande porte sur une infraction que la Partie requise considère comme étant de nature politique ou liée à une infraction de nature politique; ou

b) si la Partie requise estime que le fait d'accéder à la demande risquerait de porter atteinte à sa souveraineté, à sa sécurité, à son ordre public ou à d'autres intérêts essentiels.
5) La Partie requise peut surseoir à l'exécution de la demande si cela risquerait de porter préjudice à des enquêtes ou procédures conduites par ses autorités.
6) Avant de refuser ou de différer sa coopération, la Partie requise examine, après avoir le cas échéant consulté la Partie requérante, s'il peut être fait droit à la demande partiellement, ou sous réserve des conditions qu'elle juge nécessaires.
7) La Partie requise informe rapidement la Partie requérante de la suite qu'elle entend donner à la demande d'entraide. Elle doit motiver son éventuel refus d'y faire droit ou l'éventuel ajournement de la demande. La Partie requise informe également la Partie requérante de tout motif rendant l'exécution de l'entraide impossible ou étant susceptible de la retarder de manière significative.
8) La Partie requérante peut demander que la Partie requise garde confidentiels le fait et l'objet de toute demande formulée au titre du présent chapitre, sauf dans la mesure nécessaire à l'exécution de ladite demande. Si la Partie requise ne peut faire droit à cette demande de confidentialité, elle doit en informer rapidement la Partie requérante, qui devra alors déterminer si la demande doit néanmoins être exécutée.
9) a) En cas d'urgence, les autorités judiciaires de la Partie requérante peuvent adresser directement à leurs homologues de la Partie requise les demandes d'entraide ou les communications s'y rapportant. Dans un tel cas, copie est adressée simultanément aux autorités centrales de la Partie requise par le biais de l'autorité centrale de la Partie requérante.
b) Toute demande ou communication formulée au titre du présent paragraphe peut l'être par l'intermédiaire de l'Organisation internationale de police criminelle (Interpol).
c) Lorsqu'une demande a été formulée en application de l'alinéa a. du présent article et lorsque l'autorité n'est pas compétente pour la traiter, elle la transmet à l'autorité nationale compétente et en informe directement la Partie requérante.
d) Les demandes ou communications effectuées en application du présent paragraphe qui ne supposent pas de mesure de coercition peuvent être directement transmises par les autorités compétentes de la Partie requérante aux autorités compétentes de la Partie requise.
e) Chaque Partie peut informer le Secrétaire Général du Conseil de l'Europe, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, que, pour des raisons d'efficacité, les demandes faites sous ce paragraphe devront être adressées à son autorité centrale.

Article 28 – Confidentialité et restriction d'utilisation

1) En l'absence de traité d'entraide ou d'arrangement reposant sur des législations uniformes ou réciproques en vigueur entre la Partie requérante et la Partie requise, les dispositions du présent article s'appliquent. Elles ne s'appliquent pas lorsqu'un traité, un arrangement ou une législation de ce type existent, à moins que les Parties concernées ne décident d'appliquer à la place tout ou partie du présent article.
2) La Partie requise peut subordonner la communication d'informations ou de matériels en réponse à une demande:
a) à la condition que ceux-ci restent confidentiels lorsque la demande d'entraide ne pourrait être respectée en l'absence de cette condition; ou
b) à la condition qu'ils ne soient pas utilisés aux fins d'enquêtes ou de procédures autres que celles indiquées dans la demande.
3) Si la Partie requérante ne peut satisfaire à l'une des conditions énoncées au paragraphe 2, elle en informe rapidement la Partie requise, qui détermine alors si l'information doit néanmoins être fournie. Si la Partie requérante accepte cette condition, elle sera liée par celle-ci.
4) Toute Partie qui fournit des informations ou du matériel soumis à l'une des conditions énoncées au paragraphe 2 peut exiger de l'autre Partie qu'elle lui communique des précisions, en relation avec cette condition, quant à l'usage fait de ces informations ou de ce matériel.

Section 2 – Dispositions spécifiques

Titre 1 – Entraide en matière de mesures provisoires

Article 29 – Conservation rapide de données informatiques stockées

1) Une Partie peut demander à une autre Partie d'ordonner ou d'imposer d'une autre façon la conservation rapide de données stockées au moyen d'un système informatique se trouvant sur le territoire de cette autre Partie, et au sujet desquelles la Partie requérante a l'intention de soumettre une demande d'entraide en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation desdites données.
2) Une demande de conservation faite en application du paragraphe 1 doit préciser:
a) l'autorité qui demande la conservation;
b) l'infraction faisant l'objet de l'enquête ou de procédures pénales et un bref exposé des faits qui s'y rattachent;
c) les données informatiques stockées à conserver et la nature de leur lien avec l'infraction;
d) toutes les informations disponibles permettant d'identifier le gardien des données informatiques stockées ou l'emplacement du système informatique;
e) la nécessité de la mesure de conservation; et
f) le fait que la Partie entend soumettre une demande d'entraide en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation des données informatiques stockées.
3) Après avoir reçu la demande d'une autre Partie, la Partie requise doit prendre toutes les mesures appropriées afin de procéder sans délai à la conservation des données spécifiées, conformément à son droit interne. Pour pouvoir répondre à une telle demande, la double incrimination n'est pas requise comme condition préalable à la conservation.
4) Une Partie qui exige la double incrimination comme condition pour répondre à une demande d'entraide visant la perquisition ou l'accès similaire, la saisie ou l'obtention par un moyen similaire ou la divulgation des données stockées peut, pour des infractions autres que celles établies conformément aux articles 2 à 11 de la présente Convention, se réserver le droit de refuser la demande de conservation au titre du présent article dans le cas où elle a des raisons de penser que, au moment de la divulgation, la condition de double incrimination ne pourra pas être remplie.
5) En outre, une demande de conservation peut être refusée uniquement:
a) si la demande porte sur une infraction que la Partie requise considère comme étant de nature politique ou liée à une infraction de nature politique; ou
b) si la Partie requise estime que le fait d'accéder à la demande risquerait de porter atteinte à sa souveraineté, à sa sécurité, à l'ordre public ou à d'autres intérêts essentiels.

6) Lorsque la Partie requise estime que la conservation simple ne suffira pas à garantir la disponibilité future des données, ou compromettra la confidentialité de l'enquête de la Partie requérante, ou nuira d'une autre façon à celle-ci, elle en informe rapidement la Partie requérante, qui décide alors s'il convient néanmoins d'exécuter la demande.
7) Toute conservation effectuée en réponse à une demande visée au paragraphe 1 sera valable pour une période d'au moins soixante jours afin de permettre à la Partie requérante de soumettre une demande en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation des données. Après la réception d'une telle demande, les données doivent continuer à être conservées en attendant l'adoption d'une décision concernant la demande.

Article 30 – Divulgation rapide de données conservées

1) Lorsque, en exécutant une demande de conservation de données relatives au trafic concernant une communication spécifique formulée en application de l'article 29, la Partie requise découvre qu'un fournisseur de services dans un autre Etat a participé à la transmission de cette communication, la Partie requise divulgue rapidement à la Partie requérante une quantité suffisante de données concernant le trafic, aux fins d'identifier ce fournisseur de services et la voie par laquelle la communication a été transmise.
2) La divulgation de données relatives au trafic en application du paragraphe 1 peut être refusée seulement:
a) si la demande porte sur une infraction que la Partie requise considère comme étant de nature politique ou liée à une infraction de nature politique; ou
b) si elle considère que le fait d'accéder à la demande risquerait de porter atteinte à sa souveraineté, à sa sécurité, à son ordre public ou à d'autres intérêts essentiels.

Titre 2 – Entraide concernant les pouvoirs d'investigation

Article 31 – Entraide concernant l'accès aux données stockées

1) Une Partie peut demander à une autre Partie de perquisitionner ou d'accéder de façon similaire, de saisir ou d'obtenir de façon similaire, de divulguer des données stockées au moyen d'un système informatique se trouvant sur le territoire de cette autre Partie, y compris les données conservées conformément à l'article 29.
2) La Partie requise satisfait à la demande en appliquant les instruments internationaux, les arrangements et les législations mentionnés à l'article 23, et en se conformant aux dispositions pertinentes du présent chapitre.
3) La demande doit être satisfaite aussi rapidement que possible dans les cas suivants:
a) il y a des raisons de penser que les données pertinentes sont particulièrement sensibles aux risques de perte ou de modification; ou
b) les instruments, arrangements et législations visés au paragraphe 2 prévoient une coopération rapide.

Article 32 – Accès transfrontière à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public

Une Partie peut, sans l'autorisation d'une autre Partie :
a) accéder à des données informatiques stockées accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données; ou
b) accéder à, ou recevoir au moyen d'un système informatique situé sur son territoire, des données informatiques stockées situées dans un autre Etat, si la Partie obtient le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique.

Article 33 – Entraide dans la collecte en temps réel de données relatives au trafic

1) Les Parties s'accordent l'entraide dans la collecte en temps réel de données relatives au trafic, associées à des communications spécifiées sur leur territoire, transmises au moyen d'un système informatique. Sous réserve des dispositions du paragraphe 2, cette entraide est régie par les conditions et les procédures prévues en droit interne.
2) Chaque Partie accorde cette entraide au moins à l'égard des infractions pénales pour lesquelles la collecte en temps réel de données concernant le trafic serait disponible dans une affaire analogue au niveau interne.

Article 34 – Entraide en matière d'interception de données relatives au contenu

Les Parties s'accordent l'entraide, dans la mesure permise par leurs traités et lois internes applicables, pour la collecte ou l'enregistrement en temps réel de données relatives au contenu de communications spécifiques transmises au moyen d'un système informatique.

Titre 3 – Réseau 24/7

Article 35 – Réseau 24/7

1) Chaque Partie désigne un point de contact joignable vingt-quatre heures sur vingt quatre, sept jours sur sept, afin d'assurer une assistance immédiate pour des investigations concernant les infractions pénales liées à des systèmes et à des données informatiques, ou pour recueillir les preuves sous forme électronique d'une infraction pénale. Cette assistance englobera la facilitation, ou, si le droit et la pratique internes le permettent, l'application directe des mesures suivantes:
a) apport de conseils techniques;
b) conservation des données, conformément aux articles 29 et 30;
c) recueil de preuves, apport d'informations à caractère juridique, et localisation des suspects.
2) a) Le point de contact d'une Partie aura les moyens de correspondre avec le point de contact d'une autre Partie selon une procédure accélérée.
b) Si le point de contact désigné par une Partie ne dépend pas de l'autorité ou des autorités de cette Partie responsables de l'entraide internationale ou de l'extradition, le point de contact veillera à pouvoir agir en coordination avec cette ou ces autorités, selon une procédure accélérée.
3) Chaque Partie fera en sorte de disposer d'un personnel formé et équipé en vue de faciliter le fonctionnement du réseau.

Chapitre IV – Clauses finales

Article 36 – Signature et entrée en vigueur

1) La présente Convention est ouverte à la signature des Etats membres du Conseil de l'Europe et des Etats non membres qui ont participé à son élaboration.
2) La présente Convention est soumise à ratification, acceptation ou approbation. Les instruments de ratification, d'acceptation ou d'approbation sont déposés près le Secrétaire Général du Conseil de l'Europe.
3) La présente Convention entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date à laquelle cinq Etats, incluant au moins trois Etats membres du Conseil de l'Europe, auront exprimé leur consentement à être liés par la Convention, conformément aux dispositions des paragraphes 1 et 2.
4) Pour tout Etat signataire qui exprimera ultérieurement son consentement à être lié par la Convention, celle-ci entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de l'expression de son consentement à être lié par la Convention, conformément aux dispositions des paragraphes 1 et 2.

Article 37 – Adhésion à la Convention

1) Après l'entrée en vigueur de la présente Convention, le Comité des Ministres du Conseil de l'Europe peut, après avoir consulté les Etats contractants à la Convention et en avoir obtenu l'assentiment unanime, inviter tout Etat non membre du Conseil, n'ayant pas participé à son élaboration, à adhérer à la présente Convention. La décision est prise à la majorité prévue à l'article 20.d du Statut du Conseil de l'Europe et à l'unanimité des représentants des Etats contractants ayant le droit de siéger au Comité des Ministres.
2) Pour tout Etat adhérent à la Convention, conformément au paragraphe 1 ci-dessus, la Convention entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de dépôt de l'instrument d'adhésion près le Secrétaire Général du Conseil de l'Europe.

Article 38 – Application territoriale

1) Tout Etat peut, au moment de la signature ou au moment du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, désigner le ou les territoires auxquels s'appliquera la présente Convention.
2) Tout Etat peut, à tout autre moment par la suite, par déclaration adressée au Secrétaire Général du Conseil de l'Europe, étendre l'application de la présente Convention à tout autre territoire désigné dans la déclaration. La Convention entrera en vigueur à l'égard de ce territoire le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de réception de la déclaration par le Secrétaire Général.
3) Toute déclaration faite en application des deux paragraphes précédents peut être retirée, en ce qui concerne tout territoire désigné dans cette déclaration, par notification adressée au Secrétaire Général du Conseil de l'Europe. Le retrait prendra effet le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de réception de ladite notification par le Secrétaire Général.

Article 39 – Effets de la Convention

1) L'objet de la présente Convention est de compléter les traités ou les accords multilatéraux ou bilatéraux applicables existant entre les Parties, y compris les dispositions:
– de la Convention européenne d'extradition, ouverte à la signature le 13 décembre 1957, à Paris (STE n° 24);
– de la Convention européenne d'entraide judiciaire en matière pénale, ouverte à la signature le 20 avril 1959, à Strasbourg (STE n° 30);
– du Protocole additionnel à la Convention européenne d'entraide judiciaire en matière pénale, ouvert à la signature le 17 mars 1978, à Strasbourg (STE n° 99).
2) Si deux ou plusieurs Parties ont déjà conclu un accord ou un traité relatif aux matières traitées par la présente Convention, ou si elles ont autrement établi leurs relations sur ces sujets, ou si elles le feront à l'avenir, elles ont aussi la faculté d'appliquer ledit accord ou traité ou d'établir leurs relations en conséquence, au lieu de la présente Convention.
Toutefois, lorsque les Parties établiront leurs relations relatives aux matières faisant l'objet de la présente Convention d'une manière différente de celle y prévue, elles le feront d'une manière qui ne soit pas incompatible avec les objectifs et les principes de la Convention.
3) Rien dans la présente Convention n'affecte d'autres droits, restrictions, obligations et responsabilités d'une Partie.

Article 40 – Déclarations

Par déclaration écrite adressée au Secrétaire Général du Conseil de l'Europe, tout Etat peut, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, déclarer qu'il se prévaut de la faculté d'exiger, le cas échéant, un ou plusieurs éléments supplémentaires tels que prévus aux articles 2, 3, 6, paragraphe 1.b, 7, 9, paragraphe 3, et 27, paragraphe 9.e.

Article 41 – Clause fédérale

1) Un Etat fédéral peut se réserver le droit d'honorer les obligations contenues dans le chapitre II de la présente Convention dans la mesure où celles-ci sont compatibles avec les principes fondamentaux qui gouvernent les relations entre son gouvernement central et les Etats constituants ou autres entités territoriales analogues, à condition qu'il soit en mesure de coopérer sur la base du chapitre III.
2) Lorsqu'il fait une réserve prévue au paragraphe 1, un Etat fédéral ne saurait faire usage des termes d'une telle réserve pour exclure ou diminuer de manière substantielle ses obligations en vertu du chapitre II. En tout état de cause, il se dote de moyens étendus et effectifs permettant la mise en œuvre des mesures prévues par ledit chapitre.
3) En ce qui concerne les dispositions de cette Convention dont l'application relève de la compétence législative de chacun des Etats constituants ou autres entités territoriales analogues, qui ne sont pas, en vertu du système constitutionnel de la fédération, tenus de prendre des mesures législatives, le gouvernement fédéral porte, avec son avis favorable, lesdites dispositions à la connaissance des autorités compétentes des Etats constituants, en les encourageant à adopter les mesures appropriées pour les mettre en œuvre.

Article 42 – Réserves

Par notification écrite adressée au Secrétaire Général du Conseil de l'Europe, tout Etat peut, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, déclarer qu'il se prévaut de la ou les réserves prévues à l'article 4, paragraphe 2, à l'article 6, paragraphe 3, à l'article 9, paragraphe 4, à l'article 10, paragraphe 3, à l'article 11,

paragraphe 3, à l'article 14, paragraphe 3, à l'article 22, paragraphe 2, à l'article 29, paragraphe 4, et à l'article 41, paragraphe 1. Aucune autre réserve ne peut être faite.

Article 43 – Statut et retrait des réserves

1) Une Partie qui a fait une réserve conformément à l'article 42 peut la retirer en totalité ou en partie par notification adressée au Secrétaire Général du Conseil de l'Europe. Ce retrait prend effet à la date de réception de ladite notification par le Secrétaire Général. Si la notification indique que le retrait d'une réserve doit prendre effet à une date précise, et si cette date est postérieure à celle à laquelle le Secrétaire Général reçoit la notification, le retrait prend effet à cette date ultérieure.
2) Une Partie qui a fait une réserve comme celles mentionnées à l'article 42 retire cette réserve, en totalité ou en partie, dès que les circonstances le permettent.
3) Le Secrétaire Général du Conseil de l'Europe peut périodiquement demander aux Parties ayant fait une ou plusieurs réserves comme celles mentionnées à l'article 42 des informations sur les perspectives de leur retrait.

Article 44 – Amendements

1) Des amendements à la présente Convention peuvent être proposés par chaque Partie, et sont communiqués par le Secrétaire Général du Conseil de l'Europe aux Etats membres du Conseil de l'Europe, aux Etats non membres ayant pris part à l'élaboration de la présente Convention, ainsi qu'à tout Etat y ayant adhéré ou ayant été invité à y adhérer, conformément aux dispositions de l'article 37.
2) Tout amendement proposé par une Partie est communiqué au Comité européen pour les problèmes criminels (CDPC), qui soumet au Comité des Ministres son avis sur ledit amendement.
3) Le Comité des Ministres examine l'amendement proposé et l'avis soumis par le CDPC et, après consultation avec les Etats non membres parties à la présente Convention, peut adopter l'amendement.
4) Le texte de tout amendement adopté par le Comité des Ministres conformément au paragraphe 3 du présent article est communiqué aux Parties pour acceptation.
5) Tout amendement adopté conformément au paragraphe 3 du présent article entre en vigueur le trentième jour après que toutes les Parties ont informé le Secrétaire Général de leur acceptation.

Article 45 – Règlement des différends

1) Le Comité européen pour les problèmes criminels du Conseil de l'Europe (CDPC) est tenu informé de l'interprétation et de l'application de la présente Convention.
2) En cas de différend entre les Parties sur l'interprétation ou l'application de la présente Convention, les Parties s'efforceront de parvenir à un règlement du différend par la négociation ou par tout autre moyen pacifique de leur choix, y compris la soumission du différend au CDPC, à un tribunal arbitral qui prendra des décisions qui lieront les Parties au différend, ou à la Cour internationale de justice, selon un accord entre les Parties concernées.

Article 46 – Concertation des Parties

1) Les Parties se concertent périodiquement, au besoin, afin de faciliter:
a) l'usage et la mise en œuvre effectifs de la présente Convention, y compris l'identification de tout problème en la matière, ainsi que les effets de toute déclaration ou réserve faite conformément à la présente Convention;
b) l'échange d'informations sur les nouveautés juridiques, politiques ou techniques importantes observées dans le domaine de la criminalité informatique et la collecte de preuves sous forme électronique;
d) l'examen de l'éventualité de compléter ou d'amender la Convention.
2) Le Comité européen pour les problèmes criminels (CDPC) est tenu périodiquement au courant du résultat des concertations mentionnées au paragraphe 1.
3) Le CDPC facilite, au besoin, les concertations mentionnées au paragraphe 1 et adopte les mesures nécessaires pour aider les Parties dans leurs efforts visant à compléter ou amender la Convention. Au plus tard à l'issue d'un délai de trois ans à compter de l'entrée en vigueur de la présente Convention, le CDPC procédera, en coopération avec les Parties, à un réexamen de l'ensemble des dispositions de la Convention et proposera, le cas échéant, les amendements appropriés.
4) Sauf lorsque le Conseil de l'Europe les prend en charge, les frais occasionnés par l'application des dispositions du paragraphe 1 sont supportés par les Parties, de la manière qu'elles déterminent.
5) Les Parties sont assistées par le Secrétariat du Conseil de l'Europe dans l'exercice de leurs fonctions découlant du présent article.

Article 47 – Dénonciation

1) Toute Partie peut, à tout moment, dénoncer la présente Convention par notification au Secrétaire Général du Conseil de l'Europe.
2) La dénonciation prendra effet le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de réception de la notification par le Secrétaire Général.

Article 48 – Notification

Le Secrétaire Général du Conseil de l'Europe notifie aux Etats membres du Conseil de l'Europe, aux Etats non membres ayant pris part à l'élaboration de la présente Convention, ainsi qu'à tout Etat y ayant adhéré ou ayant été invité à y adhérer :
a) toute signature;
b) le dépôt de tout instrument de ratification, d'acceptation, d'approbation ou d'adhésion;
c) toute date d'entrée en vigueur de la présente Convention, conformément à ses articles 36 et 37;
d) toute déclaration faite en application de l'article 40 ou toute réserve faite en application de l'article 42;
e) tout autre acte, notification ou communication ayant trait à la présente Convention.
En foi de quoi, les soussignés, dûment autorisés à cet effet, ont signé la présente Convention.

Fait à Budapest, le 23 novembre 2001, en français et en anglais, les deux textes faisant également foi, en un seul exemplaire qui sera déposé dans les archives du Conseil de l'Europe. Le Secrétaire Général du Conseil de l'Europe en communiquera copie

certifiée conforme à chacun des Etats membres du Conseil de l'Europe, aux Etats non membres qui ont participé à l'élaboration de la Convention et à tout Etat invité à y adhérer.

ملحق رقم : 11

22 أفريل 2002 : إتفاقية أورومتوسطية ناشئة لشراكة بين الوحدة الأوروبية و الدول الأعضاء فيها، من جهة، و الجمهورية الجزائرية الديموقراطية الشعبية، من جهة أخرى.

22 avril 2002 : Accord euro-méditerranéen établissant une association entre la Communauté européenne et ses Etats membres, d'une part, et la République Algérienne Démocratique et populaire, d'autre part.

(Ensemble six annexes, sept protocoles, un acte final, cinq déclarations communes et neuf déclarations unilatérales)

Le Royaume de Belgique,
Le Royaume de Danemark,
La République fédérale d'Allemagne,
La République hellénique,
Le Royaume d'Espagne,
La République française,
L'Irlande,
La République italienne,
Le Grand-Duché de Luxembourg,
Le Royaume des Pays-Bas,
La République d'Autriche,
La République portugaise,
La République de Finlande,
Le Royaume de Suède,
Le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord,
Parties contractantes au traité instituant la Communauté européenne, ci-après dénommées les « Etats membres », et
La Communauté européenne, ci-après dénommée « Communauté »,
D'une part, et
La République algérienne démocratique et populaire, ci-après dénommée « Algérie »,
D'autre part,

Considérant la proximité et l'interdépendance existant entre la Communauté, ses Etats membres et l'Algérie, fondées sur des liens historiques et des valeurs communes ;

Considérant que la Communauté, les Etats membres et l'Algérie souhaitent renforcer ces liens et instaurer durablement des relations fondées sur la réciprocité, la solidarité, le partenariat et le co-développement ;

Considérant l'importance que les parties attachent au respect des principes de la Charte des Nations Unies et, en particulier, au respect des droits de l'Homme et des libertés politiques et économiques qui constituent le fondement même de l'association ;

Conscients, d'une part, de l'importance de relations se situant dans un cadre global euro-méditerranéen et, d'autre part, de l'objectif d'intégration entre les pays du Maghreb ;

Désireux de réaliser pleinement les objectifs de leur association par la mise en oeuvre des dispositions pertinentes de cet accord, au bénéfice d'un rapprochement du niveau de développement économique et social de la Communauté et de l'Algérie ;

Conscients de l'importance du présent Accord, reposant sur la réciprocité des intérêts, les concessions mutuelles, la coopération et sur le dialogue ;

Désireux d'établir et d'approfondir la concertation politique sur les questions bilatérales et internationales d'intérêt commun ;

Conscients que le terrorisme et la criminalité organisée internationale constituent une menace pour la réalisation des objectifs du partenariat et la stabilité dans la région ;

Tenant compte de la volonté de la Communauté d'apporter à l'Algérie un soutien significatif à ses efforts de réforme et d'ajustement au plan économique, ainsi que de développement social ;

Considérant l'option prise respectivement par la Communauté et l'Algérie en faveur du libre-échange dans le respect des droits et des obligations découlant de l'Accord général sur les tarifs douaniers et le commerce (GATT), tel qu'il résulte du cycle d'Uruguay ;

Désireux d'instaurer une coopération, soutenue par un dialogue régulier, dans les domaines économique, scientifique, technologique, social, culturel, audiovisuel et de l'environnement afin de parvenir à une meilleure compréhension réciproque ;

Confirmant que les dispositions du présent accord qui relèvent de la troisième partie, titre IV, du traité instituant la Communauté européenne lient le Royaume-Uni et l'Irlande en tant que parties contractantes distinctes et non en qualité d'Etats membres de la Communauté jusqu'à ce que le Royaume-Uni ou l'Irlande (selon le cas) notifie à l'Algérie qu'il est désormais lié en tant que membre de la Communauté, conformément au protocole sur la position du Royaume-Uni et de l'Irlande annexée au traité sur l'Union européenne et au traité instituant la Communauté européenne. Les mêmes dispositions s'appliquent au Danemark, conformément au protocole sur la position du Danemark ;

Convaincus que le présent Accord constitue un cadre propice à l'épanouissement d'un partenariat qui se base sur l'initiative privée, et qu'il crée un climat favorable à l'essor de leurs relations économiques, commerciales et en matière d'investissement, facteur indispensable au soutien de la restructuration économique et de la modernisation technologique,

Sont convenus des dispositions qui suivent :

Article 1er

1. Il est établi une association entre la Communauté et ses Etats membres, d'une part, et l'Algérie, d'autre part.

2. Le présent accord a pour objectifs de :

- fournir un cadre approprié au dialogue politique entre les parties afin de permettre le renforcement de leurs relations et de leur coopération dans tous les domaines qu'elles estimeront pertinents ;
- développer les échanges, assurer l'essor de relations économiques et sociales équilibrées entre les parties, et fixer les conditions de la libéralisation progressive des échanges de biens, de services et de capitaux ;
- favoriser les échanges humains, notamment dans le cadre des procédures administratives ;
- encourager l'intégration maghrébine en favorisant les échanges et la coopération au sein de l'ensemble maghrébin et entre celui-ci et la Communauté et ses Etats membres ;
- promouvoir la coopération dans les domaines économique, social, culturel et financier.

Article 2

Le respect des principes démocratiques et des droits fondamentaux de l'homme, tels qu'énoncés dans la Déclaration universelle des droits de l'homme, inspire les politiques internes et internationales des parties et constitue un élément essentiel du présent accord.

TITRE VIII
COOPÉRATION DANS LE DOMAINE
DE LA JUSTICE ET DES AFFAIRES INTÉRIEURES

Article 82
Renforcement des institutions et de l'Etat de droit

Dans leur coopération dans le domaine de la justice et des affaires intérieures, les parties attacheront une importance particulière au renforcement des institutions dans les domaines de l'application du droit et le fonctionnement de la justice. Cela inclut la consolidation de l'Etat de droit.

Dans ce cadre, les parties veilleront, également, au respect des droits des nationaux des deux parties sans aucune discrimination sur le territoire de l'autre partie.

Les dispositions du présent article ne visent pas les différences de traitement fondées sur la nationalité.

Article 84
Coopération dans le domaine de la prévention et contrôle de l'immigration illégale

1. Les parties réaffirment l'importance qu'elles attachent à développer une coopération mutuelle et bénéfique portant sur l'échange d'informations sur les flux d'immigration illégale et décident de coopérer afin de prévenir et de contrôler l'immigration illégale.

A cette fin :

- l'Algérie, d'une part, et chaque Etat membre de la Communauté, d'autre part, acceptent de réadmettre leurs ressortissants présents illégalement sur le territoire de l'autre partie, après accomplissement des procédures d'identification nécessaires ;
- l'Algérie et les Etats membres de la Communauté fourniront à leurs ressortissants les documents d'identité nécessaires à cette fin.

2. Les parties, soucieuses de faciliter la circulation et le séjour de leurs ressortissants en situation régulière, conviennent de négocier à la demande d'une partie, en vue de conclure des accords bilatéraux de lutte contre l'immigration illégale ainsi que des accords de réadmission. Ces derniers accords couvriront, si cela est jugé nécessaire par l'une des parties, la réadmission de ressortissants d'autres pays en provenance directe du territoire de l'une des parties. Les modalités pratiques de mise en oeuvre de ces accords seront définies, le cas échéant, par les parties dans le cadre de ces accords mêmes ou de protocoles de mise en œuvre de ces accords.

3. Le Conseil d'association examine les autres efforts conjoints susceptibles d'être déployés en vue de prévenir et de contrôler l'immigration illégale, y compris la détection de faux documents.

Article 85
Coopération en matière juridique et judiciaire

1. Les parties conviennent que la coopération dans les domaines juridique et judiciaire est essentielle et représente un complément nécessaire aux autres coopérations prévues dans le présent accord.

2. Cette coopération peut inclure, le cas échéant, la négociation d'accords dans ces domaines.

3. La coopération judiciaire civile portera notamment sur :

- le renforcement de l'assistance mutuelle pour la coopération dans le traitement des différends ou d'affaires à caractère civil, commercial ou familial ;
- l'échange d'expérience en matière de gestion et d'amélioration de l'administration de la justice civile.

4. La coopération judiciaire pénale portera sur :

- le renforcement des dispositifs existants en matière d'assistance mutuelle ou d'extradition ;
- le développement des échanges, notamment, en matière de pratique de la coopération judiciaire pénale, de protection des droits et libertés individuelles, de lutte contre le crime organisé et d'amélioration de l'efficacité de la justice pénale.

5. Cette coopération inclura notamment la mise en place de cycles de formation spécialisée.

Article 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 domaines du trafic de personnes ; de l'exploitation à des fins sexuelles ; du trafic illicite de produits prohibés, contrefaits ou piratés et de transactions illégales concernant notamment les déchets industriels ou du matériel radioactif ; 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 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.

Article 87
Lutte contre le blanchiment de l'argent

1. Les parties conviennent de la nécessité d'œuvrer et de coopérer afin d'empêcher l'utilisation de leurs systèmes financiers au blanchiment de capitaux provenant d'activités criminelles en général et du trafic illicite de la drogue en particulier.

2. La coopération dans ce domaine comporte notamment une assistance administrative et technique en vue d'adopter et de mettre en œuvre des normes appropriées de lutte contre le blanchiment de l'argent, comparables à celles adoptées en la matière par la Communauté et les instances internationales actives dans ce domaine, et en particulier le groupe d'action financière internationale (GAFI).

3. La coopération visera :

a) La formation d'agents des services chargés de la prévention, de la détection et de la lutte contre le blanchiment de l'argent ainsi que des agents du corps judiciaire ;

b) Un soutien approprié à la création d'institutions spécialisées en la matière et au renforcement de celles déjà existantes.

Article 88
Lutte contre le racisme et la xénophobie

Les parties conviennent de prendre les mesures appropriées en vue de prévenir et de combattre toutes les formes et manifestations de discrimination fondée sur la race, l'origine ethnique et la religion, notamment dans les domaines de l'éducation, de l'emploi, de la formation et du logement. A cette fin, des actions d'information et de sensibilisation seront développées.

Dans ce cadre, les parties veillent notamment à ce que des procédures judiciaires et/ou administratives soient accessibles à toutes les personnes qui s'estiment lésées par les discriminations mentionnées ci-dessus.

Les dispositions du présent article ne visent pas les différences de traitement fondées sur la nationalité.

Article 89
Lutte contre la drogue et la toxicomanie

1. La coopération vise à :

a) Améliorer l'efficacité des politiques et mesures d'application pour prévenir et combattre la culture, la production, l'offre, la consommation et le trafic illicites de stupéfiants et de substances psychotropes ;

b) Eliminer la consommation illicite de ces produits.

2. Les parties définissent ensemble, conformément à leur législation respective, les stratégies et les méthodes de coopération appropriées pour atteindre ces objectifs. Leurs actions, lorsqu'elles ne sont pas conjointes, font l'objet de consultations et d'une coordination étroite.

Peuvent participer aux actions les institutions publiques et privées compétentes, les organisations internationales en collaboration avec le Gouvernement de l'Algérie et les instances concernées de la Communauté et de ses Etats membres.

3. La coopération est réalisée en particulier à travers les domaines suivants :

a) La création ou l'extension d'institutions socio-sanitaires et de centres d'information pour le traitement et la réinsertion des toxicomanes ;

b) La mise en œuvre de projets de prévention, d'information, de formation et de recherche épidémiologique ;

c) L'établissement de normes afférentes à la prévention du détournement des précurseurs et des autres substances essentielles utilisées pour la fabrication illicite de stupéfiants et de substances psychotropes, qui soient équivalentes à celles adoptées par la Communauté et les instances internationales concernées ;

d) Le soutien à la création de services spécialisés dans la lutte contre le trafic illicite de drogues.

4. Les deux parties favoriseront la coopération régionale et sous-régionale.

Article 90
Lutte contre le terrorisme

Les parties, dans le respect des conventions internationales dont elles sont parties et de leurs législations et réglementations respectives, conviennent de coopérer en vue de prévenir et réprimer les actes de terrorisme :

- dans le cadre de la mise en œuvre intégrale de la résolution 1373 du Conseil de sécurité et des autres résolutions pertinentes ;
- par un échange d'informations sur les groupes terroristes et leurs réseaux de soutien conformément au droit international et national ;
- par un échange d'expériences sur les moyens et méthodes pour lutter contre le terrorisme, ainsi que dans les domaines techniques et de la formation.

Article 91
Lutte contre la corruption

I. Les parties conviennent de coopérer, en se basant sur les instruments juridiques internationaux existants en la matière, pour lutter contre les actes de corruption dans les transactions commerciales internationales :

- en prenant les mesures efficaces et concrètes contre toutes les formes de corruption, pots de vin et pratiques illicites de toute nature dans les transactions commerciales internationales commis par des particuliers ou des personnes morales ;
- en se prêtant assistance mutuelle dans les enquêtes pénales relatives à des actes de corruption.

2. La coopération visera également l'assistance technique dans le domaine de la formation des agents et magistrats chargés de la prévention et la lutte contre la corruption et le soutien aux initiatives visant à l'organisation de la lutte contre cette forme de criminalité.

يمكن الإطلاع على هذه الإتفاقية بكاملها في صفحة الأنترنت التالية :
http://www.deldza.ec.europa.eu/fr/ue_algerie/Accord%20d'association.pdf

ملحق رقم : 12

مرسوم رئاسي رقم 07-375 مؤرخ في 21 ذي القعدة عام 1428 الموافق أول ديسمبر 2007، يتضمن التصديق على الإتفاقية بين حكومة الجمهورية الجزائرية الديموقراطية الشعبية و حكومة الجمهورية الفرنسية المتعلق بالتعاون في مجال الأمن و مكافحة الإجرام المنظم، الموقع بالجزائر في 25 أكتوبر سنة 2003

الجريدة الرسمية الصادرة في 9 ديسمبر 2007 / العـــدد 77

Décret présidentiel n° 07-375 du 21 Dhou El Kaada 1428 correspondant au 1er décembre 2007 portant ratification de l.accord entre le Gouvernement de la république algérienne démocratique et populaire et le Gouvernement de la République française relatif à la coopération en matière de sécurité et de lutte contre la criminalité organisée, signé à Alger le 25 octobre 2003.

Journal officiel du 9 décembre 2007 / n° 77

الجرائد الرسمية للجمهورية الجزائرية يمكن الإطلاع عليها و إستنساخها بالغة العربية أو الفرنسية في شكل مستندات من نوع *(P.D.F)* في موقع الأنترنت التالي :

http://www.joradp.dz/HAR/Index.htm

المادّة 9

يدخل هذا الاتفاق حيّز التّنفيذ في تاريخ استلام آخر التبليغين اللذين يخطر بموجبهما الطرفان بعضهما البعض، رسميا، بإتمام الإجراءات الوطنية. ويسري هذا الاتفاق لمدة غير محدودة.

يستطيع كل من الطرفين نقض هذا الاتفاق عبر القناة الدّبلوماسية بإخطار كتابي مسبق مدته ستة أشهر.

يمكن إضافة تعديلات لهذا الاتفاق بموافقة الطرفين، وتدخل هذه التعديلات حيّز التّنفيذ عن طريق القناة الدّبلوماسية.

المادّة 10

يلتزم الطرفان بالاتصال المباشر أو عن طريق القناة الدّبلوماسية لتنفيذ هذا الاتفاق.

وإثباتا لذلك، قام الموقعان أدناه، المفوضان أصولا من طرف حكومتيهما بتوقيع هذا الاتفاق.

حرّر بالجزائر في 22 نوفمبر سنة 1999 في نسختين أصليتين، بالعربيّة والفرنسية والإيطالية، ولكل النصوص نفس الحجّية القانونية. وفي حالة الاختلاف في تفسير أو تطبيق هذا الاتفاق، يرجّح النص الفرنسي.

عن حكومة الجمهورية الجزائرية الديمقراطية الشعبية

وزير الداخلية والجماعات المحلية والبيئة

عبد المالك سلال

عن حكومة الجمهورية الإيطالية

وزيرة الداخلية

روزة يرنولينو روسو

مرسوم رئاسيّ رقم 07 – 375 مؤرّخ في 21 ذي القعدة عام 1428 الموافق أوّل ديسمبر سنة 2007، يتضمّن التصديق على الاتفاق بين حكومة الجمهوريّة الجزائريّة الدّيمقراطيّة الشّعبيّة وحكومة الجمهوريّة الفرنسية المتعلّق بالتعاون في مجال الأمن ومكافحة الإجرام المنظم، الموقّع بالجزائر في 25 أكتوبر سنة 2003.

إنّ رئيس الجمهوريّة،

– بناء على تقرير وزير الشؤون الخارجيّة،

– وبناء على الدّستور، لا سيّما المادّة 77 – 9 منه،

– وبعد الاطّلاع على الاتفاق بين حكومة الجمهوريّة الجزائريّة الدّيمقراطيّة الشّعبيّة وحكومة الجمهوريّة الفرنسية المتعلّق بالتعاون في مجال الأمن ومكافحة الإجرام المنظم، الموقّع بالجزائر في 25 أكتوبر سنة 2003.

يرسم ما يأتي :

المادّة الأولى : يصدّق على الاتفاق بين حكومة الجمهوريّة الجزائريّة الدّيمقراطيّة الشّعبيّة وحكومة الجمهوريّة الفرنسية المتعلّق بالتعاون في مجال الأمن ومكافحة الإجرام المنظم، الموقّع بالجزائر في 25 أكتوبر سنة 2003، وينشر في الجريدة الرّسميّة للجمهوريّة الجزائريّة الدّيمقراطيّة الشّعبيّة.

المادّة 2 : ينشر هذا المرسوم في الجريدة الرّسميّة للجمهوريّة الجزائريّة الدّيمقراطيّة الشّعبيّة.

حرّر بالجزائر في 21 ذي القعدة عام 1428 الموافق أوّل ديسمبر سنة 2007.

عبد العزيز بوتفليقة

اتفاق بين

حكومة الجمهوريّة الجزائريّة الدّيمقراطيّة الشّعبيّة وحكومة الجمهورية الفرنسية

متعلق بالتعاون في مجال الأمن ومكافحة الإجرام المنظم

إن حكومة الجمهوريّة الجزائريّة الدّيمقراطيّة الشّعبيّة وحكومة الجمهوريّة الفرنسية المشار إليهما فيما بعد بالطرفين،

رغبة منهما في تعزيز أواصر التعاون في إطار اتفاقية التعاون الثقافي، العلمي والتقني، بين حكومة الجمهوريّة الجزائريّة الدّيمقراطيّة الشّعبيّة وحكومة الجمهوريّة الفرنسية ، الموقّعة بباريس بتاريخ 11 مارس سنة 1988،

إذ يعربان عن انشغالهما أمام التهديد الذي يشكّله الإجرام المنظم بكل أشكاله والإرهاب،

ورغبة منهما في تعزيز تعاونهما في مجال الأمن ومكافحة الإجرام المنظم خدمة لمصلحة البلدين،

اتفقتا على ما يأتي :

المادّة الأولى

يقيم الطرفان تعاونا عملياتيا وتقنيا في مجال الأمن الداخلي ويتبادلان المساعدة، بالأخص في المجالات الآتية :

1 – مكافحة الإجرام الدولي المنظم،

2 – مكافحة الاتجار غير المشروع بالمخدرات والمؤثرات العقلية وسلائفها الكيماوية،

3 – مكافحة الإرهاب،

4 – مكافحة الجرائم ذات الطابع الاقتصادي والمالي لا سيّما تبييض الأموال،

5 – مكافحة الاتجار بالبشر،

6 – مكافحة الاتجار بالأملاك الثقافية والتحف الفنية المسروقة،

7 – مكافحة التزوير والتزييف،

8 – مكافحة الهجرة السرية والتدليس في الوثائق المتعلّقة بها،

9 – أمن وسائل النّقل الجوية والبحرية،

10 – مكافحة الاحتيالات المرتبطة بتكنولوجيات الإعلام والاتصال الجديدة،

11 – النظام والأمن العامان،

12 – تكوين المستخدمين،

13 – الشرطة الجوارية،

14 – الشرطة التقنية والعلمية،

15 – شرطة الاستعلامات،

16 – تقنيات المتفجّرات،

17 – الاتصالات السلكية واللاسلكية والإعلام الآلي،

18 – مكافحة الإجرام عن طريق الإعلام الآلي.

يمكن هذا التعاون أن يشمل مجالات أخرى، متعلّقة بالأمن الداخلي عن طريق ترتيبات تتم بين الوزراء المعينين المسؤولين عن تنفيذ هذا الاتفاق.

المادّة 2

1 – مجمل النشاطات المنصوص عليها في هذا الاتفاق الخاص بالتعاون في مجال الأمن الداخلي، يقوم بها كل طرف مع الاحترام الصارم لتشريعه الوطني والالتزامات الدولية التي وقّعت عليها.

2 – يمكن أيا من الطرفين، إذا ما قدّم له طلب معلومات في إطار هذا الاتفاق، أن يرفضه إذا ما اعتبر أن قبوله بمقتضى تشريعه الوطني قد يمس بالحقوق الأساسية للشخص.

3 – يمكن أيا من الطرفين، إذا ما قدّم له طلب تعاون، سواء كان تقنيا أو عمليا تيا في إطار هذا الاتفاق، أن يرفضه إذا ما اعتبر أن قبوله قد يمس بالسيادة والأمن والنظام العامّ وقواعد تنظيم وتسيير السلطة القضائية أو مصالح أساسية أخرى لدولته.

4 – عندما يرفض أحد الطرفين، تطبيقا للفقرتين 2 و3 من هذه المادّة، طلب تعاون، يعلم الطرف الآخر بذلك.

المادّة 3

يتعاون الطرفان في مجال الوقاية والبحث عن الأفعال المعاقب عليها التي يشملها الإجرام المنظم بمختلف أشكاله لهذه الأغراض :

1 – يتبادل الطرفان المعلومات المتعلّقة بالأشخاص الطبيعيين والمعنويين والجماعات التي يشتبه فيها المشاركة في مختلف أشكال الإجرام الدولي وبالعلاقات بين هؤلاء الأشخاص بهيكلة وسير وطرق عمل المنظمات الإجرامية وبظروف ارتكاب الجريمة في هذا السياق، وكذا بالأحكام القانونية التي تمت مخالفتها وبالإجراءات المتخذة، إذا كان هذا ضروريا للوقاية من مثل هذه الجرائم.

2 – يتخذ كل طرف، بطلب من الآخر، إجراءات شرطية، إذا كانت تبدو ضرورية لتنفيذ هذا الاتفاق.

3 – يكون تعاون الطرفين في شكل إجراءات شرطية منسقة وتعاون متبادل فيما يخص الموظفين والعتاد على أساس ترتيبات تكميلية موقّعة من طرف السلطات المختصة.

4 – يتبادل الطرفان المعلومات المتعلّقة بالطرق والأشكال الجديدة للإجرام الدولي. في هذا الإطار، يمكن كل طرف وضع عينات أو أشياء أو معلومات ذات الصلة تحت تصرّف الطرف الآخر، وهذا بناء على طلب الطرف الرّاغب في ذلك.

5 – يتبادل الطرفان نتائج الأبحاث التي قاما بها في مجال التحقيق الجنائي وعلم الإجرام مع الاستعلام المتبادل حول الطرق المنتهجة في التحقيق وكذا وسائل مكافحة الإجرام الدولي.

6 – يتبادل الطرفان المختصين بهدف اكتساب المعارف المهنية ذات المستوى الرفيع واكتشاف الوسائل والطرق والتقنيات الحديثة الخاصة بمكافحة الإجرام الدولي.

المادّة 4

قصد منع زراعة المخدرات واقتلاعها وإنتاجها واستيرادها وتصديرها وعبورها وتسويقها غير المشروعين والمؤثرات العقلية وسلائفها، يتخذ الطرفان إجراءات منسقة ويقومان بتبادل :

1 – المعلومات المتعلّقة بالأشخاص المشاركين في الإنتاج والاتجار غير المشروعين بالمخدرات

والمؤثرات العقلية وسلائفها والطرق المنتهجة ومخابئهم ووسائل نقلهم وأماكن قدومهم وعبورهم واقتناء وتوجيه المخدرات والمؤثرات العقلية وسلائفها وكذلك كل التفاصيل المتعلّقة بهذه الجرائم التي قد تساهم في الوقاية منها ومنعها والمساعدة على اكتشاف الأفعال المنصوص عليها في الاتفاقية الوحيدة للأمم المتحدة حول المخدرات لـ 30 مارس سنة 1961 والمعدّلة ببروتوكول 25 مارس سنة 1972 والاتفاقية المتعلّقة بالمؤثرات العقلية لـ 21 فبراير سنة 1971 وكذا اتفاقية 19 ديسمبر سنة 1988 المتعلّقة بمكافحة الاتجار غير المشروع بالمخدرات والمؤثرات العقلية.

2 – المعلومات العملياتية حول الطرق المستعملة في الاتجار الدولي غير المشروع بالمخدرات والمؤثرات العقلية وكذا تبييض الأموال المتأتية من هذه العملية.

3 – نتائج أبحاث علم التحقيق الجنائي وعلم الإجرام التي تم القيام بها في مجالات الاتجار غير المشروع بالمخدرات والمؤثرات العقلية والتعسف في استعمالها.

4 – عينات المخدرات والمؤثرات العقلية والسلائف التي يتم استعمالها وكذا المعلومات التقنية حول العينات التي أخذت.

5 – نتائج التجارب الخاصّة بالرقابة والاتجار القانوني بالمخدرات والمؤثرات العقلية وسلائفها.

المادّة 5

في إطار مكافحة الإرهاب، يشرع الطرفان في تبادل المعلومات المفيدة المتعلّقة بـ :

1 – الأعمال الإرهابية المخطط لها أو المرتكبة وطرق التنفيذ وكذا الوسائل التقنية المستعملة لتنفيذ مثل هذه الأعمال.

2 – الجماعات الإرهابية وأفرادها الذين يعتزمون القيام بأعمال إرهابية أو يقومون أو قاموا بتنفيذها على إقليم أحد الطرفين وتمس بمصالح الطرف الآخر.

3 – يدرج الطرفان تعاونهما في إطار الالتزامات المنصوص عليها في القرار رقم 1373 لمجلس الأمن للأمم المتحدة والالتزامات المتعاقد عليها في المنتديات الأورو متوسطية.

المادّة 6

يتمثل الموضوع الرئيسي للتعاون التقني في كل من المجالات المذكورة في المادّة الأولى من هذا الاتفاق في :

1 – التكوين العامّ والمتخصص.

2 – تبادل المعلومات والخبرات المهنية.

3 – الاستشارة التقنية.

4 – تبادل الوثائق المتخصصة.

5 – وعند الحاجة، الاستقبال المتبادل للموظفين والخبراء.

المادّة 7

قصد تحقيق الأهداف المنصوص عليها في هذا الاتفاق وتنفيذ التعاون كما هو مذكور، تم إنشاء اللجنة المشتركة للتعاون التقني في مجال الأمن ومكافحة الإجرام المنظم. بالنسبة لمسائل التكوين العامّ والمتخصص، فإن الطرفين يستغلان اللجنة المشتركة للمشاريع الفرنسية – الجزائريّة للمصادقة على البرمجة.

تجتمع اللجنة سنويا أو بطلب من أحد الطرفين بالتناوب بالجزائر وبفرنسا.

تعد اللّجنة المحاور ذات الأولوية لنشاطات التعاون التقني للسنة القادمة، وتبرز هذه البرمجة مساهمة كل طرف في حدود إمكانياته الماليّة.

عند الحاجة، تحدّد الترتيبات التقنية بين الإدارات المعنية، كيفيات التنفيذ الملموس للنشاطات التي سيتم قبولها.

المادّة 8

الوزراء المعنيون مسؤولون عن التنفيذ الحسن لهذا الاتفاق.

وعليه، فإنهم يعينون الهيئات المكلّفة بتنفيذ مختلف مجالات التعاون المشار إليها في هذا الاتفاق، ويتم إطلاع الطرف الآخر على هذا التعيين عن طريق القناة الدّبلوماسية.

المادّة 9

قصد ضمان حمايتها، فإن المعطيات الاسمية التي يتم موافاة الطرف الآخر بها في إطار التعاون المقام بناء على هذا الاتفاق، تخضع للشروط الآتية :

1 – لا يمكن الطرف المستقبل للمعطيات الاسمية استعمالها إلا للأغراض وبالشروط المتفق عليها مع الطرف المرسل بما فيها الآجال التي يجب فيها إتلاف هذه المعطيات.

2 – يعلم الطرف المستقبل للمعطيات الاسمية الطرف المرسل، بطلب منه، بالمجالات التي استعملت فيها والنتائج المتحصّل عليها.

3 – لا ترسل المعطيات الاسمية إلاّ للسلطات المختصّة للنشاط الذي تعد هذه المعطيات ضرورية له كما أن إرسال هذه المعلومات لسلطات أخرى لا يمكن أن يتم إلاّ بموافقة كتابية للطرف المرسل.

4 – يضمن الطرف المرسل دقة المعطيات الموجّهة بعد تأكّده من ضرورتها ومطابقتها للهدف المرجو. وإذا ثبت أنه تم إرسال معلومات غير صحيحة أو لا يمكن إرسالها، يقوم الطرف المرسل بإعلام الطرف المستقبل فورا بذلك لتصحيحها أو إتلاف المعطيات التي لا يمكن إرسالها.

5 – يجب إتلاف المعطيات الاسمية بمجرد أن يتبيّن أنها لم تعد صالحة للاستعمال من قبل الطرف المستقبل، يعلم الطرف المستقبل بدون تأخير الطرف المرسل بإتلاف المعطيات المرسلة مع توضيح أسباب هذا الإتلاف.

6 – يحوز كل طرف على سجل للمعطيات المرسلة وإتلافها.

7 – يضمن الطرفان حماية المعطيات الاسمية المرسلة إليهما من الاطلاع عليها بدون رخصة أو تعديلها أو نشرها.

8 – في حالة إلغاء هذا الاتفاق أو عدم تمديده، يجب إتلاف كل المعطيات الاسمية بدون تأخير.

المادّة 10

1 – يضمن كل طرف المعالجة السرية للمعلومات المصنّفة سرية من قبل الطرف الآخر.

2 – لا ترسل العينات والأشياء والمعلومات المتبادلة في إطار هذا الاتفاق إلى دولة ثالثة دون موافقة الطرف المرسل.

المادّة 11

يسوى أي اختلاف متعلّق بتفسير أو تطبيق هذا الاتفاق عن طريق مشاورات بين الطرفين.

المادّة 12

يبلغ كل طرف الطرف الآخر بإتمام الإجراءات الداخلية المطلوبة فيما يخصه، لسريان مفعول هذا الاتفاق الذي يدخل حيّز التّنفيذ في اليوم الأوّل من الشهر الثاني الموالي لتاريخ استلام آخر تبليغ.

يبرم هذا الاتفاق لمدة ثلاث (3) سنوات ويمكن تجديده بالتمديد الضمني لفترات جديدة تمتد على ثلاث (3) سنوات.

يمكن كل طرف إلغاءه في أي وقت، بتبليغ كتابي يوجّه للطرف الآخر مع إشعار مسبق مدّته ثلاثة (3) أشهر. هذا الإلغاء لا يمس في أي حال من الأحوال حقوق والتزامات الطرفين المتعلّقة بالأعمال التي شرع فيها في إطار هذا الاتفاق.

يمكن تبني تعديلات تدخل على هذا الاتفاق في نفس أشكال هذا النص.

إثباتا لذلك، وقّع ممثلا الطرفين، المفوضان رسميا لهذا الغرض، على هذا الاتفاق، ووضعا ختميهما.

حرّر بالجزائر، في يوم السبت 25 أكتوبر سنة 2003، في نسختين باللّغة الفرنسية واللّغة العربيّة، ولكل النصّين نفس الحجّية القانونية.

عن حكومة الجمهورية الجزائرية الديمقراطية الشعبية

نور الدين يزيد زرهوني

وزير الدولة، وزير الداخلية والجماعات المحلية

عن حكومة الجمهورية الفرنسية

نيكولا ساركوزي

وزير الداخلية والأمن الداخلي والحريات المحلية

مرسوم رئاسيّ رقم 07 – 376 مؤرّخ في 21 ذي القعدة عام 1428 الموافق أوّل ديسمبر سنة 2007، يتضمّن التصديق على اتفاق التعاون السياحي بين حكومة الجمهوريّة الجزائريّة الدّيمقراطيّة الشّعبيّة وحكومة دولة الإمارات العربيّة المتحدة، الموقّع بأبو ظبي في 27 جمادى الأولى عام 1428 الموافق 13 يونيو سنة 2007.

إنّ رئيس الجمهوريّة،

– بناء على تقرير وزير الشؤون الخارجيّة،

– وبناء على الدّستور، لا سيّما المادّة 77 – 9 منه،

– وبعد الاطّلاع على اتفاق التعاون السياحي بين حكومة الجمهوريّة الجزائريّة الدّيمقراطيّة الشّعبيّة وحكومة دولة الإمارات العربيّة المتحدة، الموقّع بأبو ظبي في 27 جمادى الأولى عام 1428 الموافق 13 يونيو سنة 2007،

يرسم ما يأتي :

المادّة الأولى : يصدّق على اتفاق التعاون السياحي بين حكومة الجمهوريّة الجزائريّة الدّيمقراطيّة الشّعبيّة وحكومة دولة الإمارات العربيّة المتحدة،

Décret présidentiel n° 07-375 du 21 Dhou El Kaada 1428 correspondant au 1er décembre 2007 portant ratification de l'accord entre le Gouvernement de la République algérienne démocratique et populaire et le Gouvernement de la République française relatif à la coopération en matière de sécurité et de lutte contre la criminalité organisée, signé à Alger le 25 octobre 2003.

— — — —

Le Président de la République,

Sur le rapport du ministre des affaires étrangères,

Vu la Constitution, notamment son article 77-9° ;

Considérant l'accord entre le Gouvernement de la République algérienne démocratique et populaire et le Gouvernement de la République française relatif à la coopération en matière de sécurité et de lutte contre la criminalité organisée, signé à Alger le 25 octobre 2003 ;

Décrète :

Article 1er. — Est ratifié et sera publié au *Journal officiel* de la République algérienne démocratique et populaire l'accord entre le Gouvernement de la République algérienne démocratique et populaire et le Gouvernement de la République française relatif à la coopération en matière de sécurité et de lutte contre la criminalité organisée, signé à Alger le 25 octobre 2003.

Art. 2. — Le présent décret sera publié au *Journal officiel* de la République algérienne démocratique et populaire.

Fait à Alger, le 21 Dhou El Kaada 1428 correspondant au 1er décembre 2007.

Abdelaziz BOUTEFLIKA.

— — — — — — — —

Accord entre le Gouvernement de la République algérienne démocratique et populaire et le Gouvernement de la République française relatif à la coopération en matière de sécurité et de lutte contre la criminalité organisée.

— — — —

Le Gouvernement de la République algérienne démocratique et populaire ; et

Le Gouvernement de la République française ;

Ci-après dénommés les parties ;

Désireux de resserrer leurs liens de coopération dans le cadre de la convention de coopération culturelle, scientifique et technique entre le Gouvernement de la République algérienne démocratique et populaire et le Gouvernement de la République française, signée le 11 mars 1988 ;

Préoccupés par la menace que constituent la criminalité organisée sous toutes ses formes et le terrorisme ;

Souhaitant renforcer leur coopération en matière de sécurité et de lutte contre la criminalité organisée dans l'intérêt des deux pays ;

Sont convenus de ce que suit :

Article 1er

Les parties mènent une coopération opérationnelle et technique en matière de sécurité intérieure et s'accordent mutuellement assistance, notamment, dans les domaines suivants :

1. la lutte contre la criminalité organisée internationale ;

2. la lutte contre le trafic illicite des stupéfiants, des susbstances psychotropes et de leurs précurseurs chimiques ;

3. la lutte contre le terrorisme ;

4. la lutte contre les infractions à caractère économique et financier, notamment le blanchiment de fonds ;

5. la lutte contre la traite des êtres humains ;

6. la lutte contre le trafic des biens culturels et des objets d'art volés ;

7. la lutte contre les faux et les contrefaçons ;

8. la lutte contre l'immigration irrégulière et la fraude documentaire s'y rapportant ;

9. La sûreté des moyens de transport aériens et maritimes ;

10. la lutte contre les fraudes liées aux nouvelles technologies de l'information et de la communication ;

11. l'ordre et la sécurité publics ;

12. la formation des personnels ;

13. la police de proximité ;

14. la police technique et scientifique ;

15. la police du renseignement ;

16. la pyrotechnie ;

17. les télécommunications et l'informatique ;

18. la lutte contre la cybercriminalité.

Cette coopération peut être étendue à d'autres domaines relatifs à la sécurité intérieure par voie d'arrangements entre les ministres désignés responsables de l'exécution du présent accord.

Article 2

1. L'ensemble des activités prévues par le présent accord au titre de la coopération en matière de sécurité intérieure est mené par chacune des parties dans le strict respect de sa législation nationale et des engagements internationaux qu'elle a souscrits.

2. Saisie d'une demande de communication d'informations formulée dans le cadre du présent accord, chacune des parties peut la rejeter si elle estime qu'en vertu de sa législation nationale son acceptation porterait atteinte aux droits fondamentaux de la personne.

3. Saisie d'une demande de coopération tant technique qu'opérationnelle formulée dans le cadre du présent accord, chaque partie peut la rejeter si elle estime que son acceptation porterait atteinte à la souveraineté, à la sécurité, à l'ordre public, aux règles d'organisation et de fonctionnement de l'autorité judiciaire ou à d'autres intérêts essentiels de son Etat.

4. Lorsque, en application des paragraphes 2 et 3 du présent article, l'une des parties rejette une demande de coopération, elle en informe l'autre partie.

Article 3

Les parties coopèrent à la prévention et à la recherche des faits punissables que revêtent les différentes formes de la criminalité internationale. A ces fins :

1. les parties se communiquent les informations relatives aux personnes morales, physiques et aux groupes soupçonnés de prendre part aux différentes formes de la criminalité internationale, aux relations entre ces personnes , à la structure, au fonctionnement et aux méthodes des organisations criminelles, aux circonstances des crimes commis dans ce contexte, ainsi qu'aux dispositions légales enfreintes et aux mesures prises, dans la mesure où cela est nécessaire à la prévention de telles infractions ;

2. chaque partie prend, à la demande de l'autre, des mesures policières si elles apparaissent nécessaires pour la mise en œuvre du présent accord ;

3. les parties coopèrent sous forme de mesures policières coordonnées et d'assistance réciproque en personnel et en matériel sur la base d'arrangements complémentaires signés par les autorités compétentes ;

4. les parties se communiquent les informations relatives aux méthodes et aux nouvelles formes de la criminalité internationale. Dans ce cadre, chaque partie peut mettre à la disposition de l'autre, à sa demande, des échantillons ou des objets et les informations relatives à ceux-ci ;

5. les parties échangent les résultats de recherches qu'elles mènent en criminalistique et en criminologie et s'informent mutuellement de leurs méthodes d'enquête et moyens de lutte contre la criminalité internationale ;

6. les parties échangent des spécialistes dans le but d'acquérir des connaissances professionnelles de haut niveau et de découvrir les moyens, méthodes et techniques modernes de lutte contre la criminalité internationale.

Article 4

Pour empêcher la culture, l'extraction, la production, l'importation, l'exportation, le transit et la commercialisation illicites de stupéfiants, de substances psychotropes et de leurs précurseurs, les parties prennent des mesures coordonnées et procèdent à des échanges :

1. d'informations relatives aux personnes participant à la production et au trafic illicites de stupéfiants et de substances psychotropes, aux méthodes utilisées par celles-ci, à leurs caches et à leurs moyens de transport, aux lieux de provenance, de transit, d'acquisition et de destination des stupéfiants et des substances psychotropes et de leurs précurseurs ainsi que de tout détail particulier relatif à ces infractions, susceptibles de contribuer à les prévenir, les empêcher et d'aider à détecter les faits visés par la convention unique des Nations unies sur les stupéfiants du 30 mars 1961 modifiée par le protocole du 25 mars 1972, la convention sur les substances psychotropes du 21 février 1971 et la convention du 19 décembre 1988 contre le trafic illicite de stupéfiants et de substances psychotropes ;

2. d'informations opérationnelles sur les méthodes courantes du commerce international illicite des stupéfiants et des substances psychotropes et sur le blanchiment de fonds en résultant ;

3. de résultats de recherches en criminalistique et en criminologie menées dans les domaines du trafic illicite des stupéfiants, des susbstances psychotropes et de leur abus ;

4. d'échantillons de stupéfiants, de substances psychotropes et de précurseurs pouvant faire l'objet d'abus ou d'informations techniques sur les prélèvements effectués ;

5. de résultats d'expériences relatives au contrôle et au commerce légal de stupéfiants, de substances psychotropes et de leurs précurseurs.

Article 5

Dans le cadre de la lutte contre le terrorisme, les parties procèdent à des échanges d'informations pertinentes relatives :

1. aux actes de terrorisme projetés ou commis, aux modes d'exécution et aux moyens techniques utilisés pour l'exécution de tels actes ;

2. aux groupes de terroristes et aux membres de ces groupes qui prévoient, commettent ou ont commis des actes terroristes sur le territoire de l'une des parties et portent atteinte aux intérêts de l'autre ;

3. les deux parties inscrivent leur coopération dans le cadre des engagements induits par la résolution 1373 du Conseil de sécurité des Nations unies et des engagements contractés dans les fora euro-méditerranéens.

Article 6

Dans chacun des domaines énumérés à l'article 1er du présent accord, la coopération technique a pour objet principal :

1. la formation générale et spécialisée ;

2. les échanges d'informations et d'expériences professionnelles ;

3. le conseil technique ;

4. l'échange de documentation spécialisée ;

5. et, en tant que de besoin, l'accueil réciproque de fonctionnaires et d'experts.

Article 7

En vue d'atteindre les objectifs prévus dans le présent accord et de mettre en œuvre la coopération ainsi décrite, il est créé un "comité mixte de coopération technique en matière de sécurité et de lutte contre la criminalité organisée". Pour les questions de formation générale et spécialisée, les parties mettront à profit le comité mixte des projets franco-algériens pour valider la programmation.

Le comité se réunit annuellement ou à la demande de l'une ou de l'autre partie, alternativement en Algérie et en France.

Le comité établit la programmation des axes prioritaires des actions de coopération technique pour l'année à venir. Cette programmation fait ressortir la contribution de chaque partie dans la limite de ses disponibilités budgétaires.

En tant que de besoin, des arrangements techniques entre administrations concernées précisent les modalités de mise en œuvre concrète des actions qui auront été retenues.

Article 8

Les ministres concernés sont responsables de la bonne exécution du présent accord.

A cet effet, ils désignent les organismes chargés de la mise en œuvre des différents domaines de coopération mentionnés dans le présent accord. Cette désignation est portée à la connaissance de l'autre partie par voie diplomatique.

Article 9

En vue d'assurer leur protection, les données nominatives communiquées à l'autre partie dans le cadre de la coopération instituée par le présent accord sont soumises aux conditions suivantes :

1. la partie destinataire de données nominatives ne peut les utiliser qu'aux fins et conditions convenues avec la partie émettrice, y compris les délais au terme desquels ces données doivent être détruites ;

2. la partie destinataire de données nominatives informe la partie émettrice, à sa demande, de l'usage qui en est fait et des résultats obtenus ;

3. les données nominatives sont transmises aux seules autorités compétentes pour l'activité à laquelle ces données leur sont nécessaires ; la transmission de ces informations à d'autres autorités n'est possible qu'après consentement écrit de la partie émettrice ;

4. la partie émettrice garantit l'exactitude des données communiquées après s'être assurée de la nécessité et de l'adéquation de cette communication à l'objectif recherché. S'il est établi que des données inexactes ou non communicables ont été transmises, la partie émettrice en informe sans délai la partie destinataire qui corrige les données inexactes ou détruit les données non communicables ;

5. les données nominatives doivent être détruites dès qu'elles n'ont plus d'usage pour la partie destinataire. La partie destinataire informe sans délai la partie émettrice de la destruction des données communiquées en lui précisant les motifs de cette destruction ;

6. chaque partie tient un registre des données communiquées et de leur destruction ;

7. les parties garantissent la protection des données nominatives qui leur sont communiquées contre tout accès non autorisé, toute modification et toute publication ;

8. en cas de dénonciation du présent accord ou de sa non-reconduction, toutes les données nominatives doivent être détruites sans délai.

Article 10

1. Chaque partie garantit le traitement confidentiel des informations qualifiées comme telles par l'autre partie.

2. Les échantillons, objets et informations communiqués dans la cadre du présent accord ne peuvent être transmis à un Etat tiers sans l'accord de la partie qui les a fournis.

Article 11

Tout différend relatif à l'interprétation ou à l'application du présent accord est réglé par voie de consultations entre les parties.

Article 12

Chaque partie notifie à l'autre l'accomplissement des procédures internes requises, en ce qui la concerne, pour l'entrée en vigueur du présent accord qui prend effet le premier jour du deuxième mois suivant la date de réception de la dernière de ces notifications.

Le présent accord est conclu pour une durée de trois (3) ans. Il est renouvelable par tacite reconduction pour de nouvelles périodes de trois (3) ans.

Chaque partie peut le dénoncer, à tout moment, par notification écrite adressée à l'autre avec un préavis de trois (3) mois. Cette dénonciation ne remet pas en cause les droits et obligations des parties liés aux actions engagées dans le cadre du présent accord.

Des amendements à cet accord peuvent être adoptés dans les mêmes formes que le présent texte.

En foi de quoi, les représentants des deux parties, dûment autorisés à cet effet, ont signé le présent accord et y ont apposé leur sceau.

Fait à Alger, le samedi 25 octobre 2003, en deux (2) exemplaires, chacun en langues française et arabe, les deux textes faisant également foi.

Pour le Gouvernement de la République algérienne démocratique et populaire	Pour le Gouvernement de la République française
Nouredine ZERHOUNI dit Yazid	Nicolas SARKOZY
Ministre d'Etat, ministre de l'intérieur et des collectivités locales	Ministre de l'intérieur, de la sécurité intérieure et des libertés locales

ملحق رقم : 13

برنامج "مبعوث خاص" في قناة التلفزية الفرنسية

الثانية ليوم : الخميس 7 ماي 2010 تحت عنوان :

"المجرمين المعلوماتيين"، إعداد كال من : آن ريشارد

، جيروم بافلوفسكي و ستيفان روسي.

Programme "Envoyé Special" sur la chaine France 2

Du jeudi 7 Mai 2010

Titre du reportage : "Les Cybercriminels"

De Anne Richard, Jérôme Pavlovsky et Stéphane Ross

محمول على قرص مضغوط DVD-Rom

ملحق رقم : 14

الإعـــلان العالمـــي لحقـــوق الإنســـان

إعتمد بموجب قرار الجمعية العامة 217 ألف (د– 3) المؤرخ في 10 كانون الأول/ديسمبر 1948 في 10 كانون الأول/ديسمبر 1948، اعتمدت الجمعية العامة للأمم المتحدة الإعلان العالمي لحقوق الإنسان وأصدرته، ويرد النص الكامل للإعلان في الصفحات التالية. و بعد هذا الحدث التاريخي، طلبت الجمعية العامة من البلدان الأعضاء كافة أن تدعو لنص الإعلان و"أن تعمل على نشره وتوزيعه وقراءته وشرحه، ولاسيما في المدارس والمعاهد التعليمية الأخرى، دون أي تمييز بسبب المركز السياسي للبلدان أو الأقاليم".

الديباجـــــة :

لما كان الاعتراف بالكرامة المتأصلة في جميع أعضاء الأسرة البشرية وبحقوقهم المتساوية الثابتة هو أساس الحرية والعدل والسلام في العالم.

ولما كان تناسي حقوق الإنسان وازدراؤها قد أفضيا إلى أعمال همجية آذت الضمير الإنساني، وكان غاية ما يرنو إليه عامة البشر انبثاق عالم يتمتع فيه الفرد بحرية القول والعقيدة ويتحرر من الفزع والفاقة.

و لما كان من الضروري أن يتولى القانون حماية حقوق الإنسان لكي لا يضطر المرء آخر الأمر إلى التمرد على الاستبداد والظلم.

و لما كانت شعوب الأمم المتحدة قد أكدت في الميثاق من جديد إيمانها بحقوق الإنسان الأساسية وبكرامة الفرد وقدره وبما للرجال والنساء من حقوق متساوية وحزمت أمرها على أن تدفع بالرقي الاجتماعي قدماً وأن ترفع مستوى الحياة في جو من الحرية أفسح.

ولما كانت الدول الأعضاء قد تعهدت بالتعاون مع الأمم المتحدة على ضمان اطراد مراعاة حقوق الإنسان و الحريات الأساسية واحترامها.

ولما كان للإدراك العام لهذه الحقوق والحريات الأهمية الكبرى للوفاء التام بهذا التعهد.

فإن الجمعية العامة تنادي بهذا الإعلان العالمي لحقوق الإنسان على أنه المستوى المشترك الذي ينبغي أن تستهدفه كافة الشعوب والأمم حتى يسعى كل فرد وهيئة في المجتمع، واضعين على الدوام هذا الإعلان نصب أعينهم، إلى توطيد احترام هذه الحقوق والحريات عن طريق التعليم والتربية واتخاذ إجراءات مطردة، قومية وعالمية، لضمان الاعتراف بها ومراعاتها بصورة عالمية فعالة بين الدول الأعضاء ذاتها وشعوب البقاع الخاضعة لسلطانها.

المـــــادة 1 :

يولد جميع الناس أحراراً متساوين في الكرامة والحقوق، وقد وهبوا عقلاً وضميراً وعليهم أن يعامل بعضهم بعضاً بروح الإخاء.

المـــــادة 2 :

لكل إنسان حق التمتع بكافة الحقوق والحريات الواردة في هذا الإعلان، دون أي تمييز، كالتمييز بسبب العنصر أو اللون أو الجنس أو اللغة أو الدين أو الرأي السياسي أو أي رأي آخر، أو الأصل الوطني أو الاجتماعي أو الثروة أو الميلاد أو أي وضع

آخر، دون أية تفرقة بين الرجال والنساء. وفضلا عما تقدم فلن يكون هناك أي تمييز أساسه الوضع السياسي أو القانوني أو الدولي لبلد أو البقعة التي ينتمي إليها الفرد سواء كان هذا البلد أو تلك البقعة مستقلا أو تحت الوصاية أو غير متمتع بالحكم الذاتي أو كانت سيادته خاضعة لأي قيد من القيود.

المـــــادة 3 :

لكل فرد الحق في الحياة والحرية وسلامة شخصه.

المـــــادة 4 :

لا يجوز استرقاق أو استعباد أي شخص، ويحظر الاسترقاق وتجارة الرقيق بكافة أوضاعهما.

المـــــادة 5 :

لا يعرض أي إنسان للتعذيب ولا للعقوبات أو المعاملات القاسية أو الوحشية أو الحاطة بالكرامة.

المـــــادة 6 :

لكل إنسان أينما وجد الحق في أن يعترف بشخصيته القانونية.

المـــــادة 7 :

كل الناس سواسية أمام القانون ولهم الحق في التمتع بحماية متكافئة عنه دون أية تفرقة، كما أن لهم جميعا الحق في حماية متساوية ضد أي تميز يخل بهذا الإعلان وضد أي تحريض على تمييز كهذا.

المـــــادة 8 :

لكل شخص الحق في أن يلجأ إلى المحاكم الوطنية لإنصافه عن أعمال فيها اعتداء على الحقوق الأساسية التي يمنحها له القانون.

المـــــادة 9 :

لا يجوز القبض على أي إنسان أو حجزه أو نفيه تعسفاً.

المـــــادة 10 :

لكل إنسان الحق، على قدم المساواة التامة مع الآخرين، في أن تنظر قضيته أمام محكمة مستقلة نزيهة نظراً عادلاً علنياً للفصل في حقوقه والتزاماته وأية تهمة جنائية توجه إليه.

المـــــادة 11 :

1- كل شخص متهم بجريمة يعتبر بريئاً إلى أن تثبت إدانته قانوناً بمحاكمة علنية تؤمن له فيها الضمانات الضرورية للدفاع عنه.

2- لا يدان أي شخص من جراء أداة عمل أو الامتناع عن أداة عمل إلا إذا كان ذلك يعتبر جرماً وفقاً للقانون الوطني أو الدولي وقت الارتكاب، كذلك لا توقع عليه عقوبة أشد من تلك التي كان يجوز توقيعها وقت ارتكاب الجريمة.

المـــــادة 12 :

لا يعرض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته أو لحملات على شرفه وسمعته، ولكل شخص الحق في حماية القانون من مثل هذا التدخل أو تلك الحملات.

المـــــادة 13 :

1- لكل فرد حرية التنقل واختيار محل إقامته داخل حدود كل دولة.

2- يحق لكل فرد أن يغادر أية بلاد بما في ذلك بلده كما يحق له العودة إليه.

المـــــادة 14 :

1- لكل فرد الحق في أن يلجأ إلى بلاد أخرى أو يحاول الالتجاء إليها هرباً من الاضطهاد.

2- لا ينتفع بهذا الحق من قدم للمحاكمة في جرائم غير سياسية أو لأعمال تناقض أغراض الأمم المتحدة ومبادئها.

المـــــادة 15 :

1- لكل فرد حق التمتع بجنسية ما.

2- لا يجوز حرمان شخص من جنسيته تعسفاً أو إنكار حقه في تغييرها.

المـــــادة 16 :

1- للرجل و المرأة متى بلغا سن الزواج حق التزوج وتأسيس أسرة دون أي قيد بسبب الجنس أو الدين، و لهما حقوق متساوية عند الزواج وأثناء قيامه وعند انحلاله.

2- لا يبرم عقد الزواج إلا برضى الطرفين الراغبين في الزواج رضى كاملاً لا إكراه فيه.

3- الأسرة هي الوحدة الطبيعية الأساسية للمجتمع ولها حق التمتع بحماية المجتمع والدولة.

المـــــادة 17 :

1- لكل شخص حق التملك بمفرده أو بالاشتراك مع غيره.

2- لا يجوز تجريد أحد من ملكه تعسفاً.

المـــــادة 18 :

لكل شخص الحق في حرية التفكير والضمير والدين، ويشمل هذا الحق حرية تغيير ديانته أو عقيدته، وحرية الإعراب عنهما بالتعليم والممارسة وإقامة الشعائر ومراعاتها سواء أكان ذلك سراً أم مع الجماعة.

المـــــادة 19 :

لكل شخص الحق في حرية الرأي والتعبير، ويشمل هذا الحق حرية اعتناق الآراء دون أي تدخل، واستقاء الأنباء والأفكار وتلقيها وإذاعتها بأية وسيلة كانت دون تقيد بالحدود الجغرافية.

المـــــادة 20 :

1- لكل شخص الحق في حرية الاشتراك في الجمعيات والجماعات السلمية.

2- لا يجوز إرغام أحد على الانضمام إلى جمعية ما.

المـــــادة 21 :

1- لكل فرد الحق في الاشتراك في إدارة الشؤون العامة لبلاده إما مباشرة وإما بواسطة ممثلين يختارون اختياراً حراً.

2- لكل شخص نفس الحق الذي لغيره في تقلد الوظائف العامة في البلاد.

3- إن إرادة الشعب هي مصدر سلطة الحكومة، ويعبر عن هذه الإرادة بانتخابات نزيهة دورية تجري على أساس الاقتراع السري وعلى قدم المساواة بين الجميع أو حسب أي إجراء مماثل يضمن حرية التصويت.

المـــــادة 22 :

لكل شخص بصفته عضواً في المجتمع الحق في الضمانة الاجتماعية وفي أن تحقق بوساطة المجهود القومي والتعاون الدولي وبما يتفق ونظم كل دولة ومواردها الحقوق الاقتصادية والاجتماعية والتربوية التي لا غنى عنها لكرامته وللنمو الحر لشخصيته.

المـــــادة 23 :

1- لكل شخص الحق في العمل، وله حرية اختياره بشروط عادلة مرضية كما أن له حق الحماية من البطالة.

2- لكل فرد دون أي تمييز الحق في أجر متساو للعمل.

3- لكل فرد يقوم بعمل الحق في أجر عادل مرض يكفل له ولأسرته عيشة لائقة بكرامة الإنسان تضاف إليه، عند اللزوم، وسائل أخرى للحماية الاجتماعية.

4- لكل شخص الحق في أن ينشئ وينضم إلى نقابات حماية لمصلحته.

المـــــادة 24 :

لكل شخص الحق في الراحة، وفي أوقات الفراغ، ولاسيما في تحديد معقول لساعات العمل وفي عطلات دورية بأجر.

المـــــادة 25 :

1- لكل شخص الحق في مستوى من المعيشة كاف للمحافظة على الصحة والرفاهية له ولأسرته، ويتضمن ذلك التغذية والملبس والمسكن والعناية الطبية وكذلك الخدمات الاجتماعية اللازمة، وله الحق في تأمين معيشته في حالات البطالة والمرض والعجز والترمل والشيخوخة وغير ذلك من فقدان وسائل العيش نتيجة لظروف خارجة عن إرادته.

2- للأمومة والطفولة الحق في مساعدة ورعاية خاصتين، وينعم كل الأطفال بنفس الحماية الاجتماعية سواء أكانت ولادتهم ناتجة عن رباط شرعي أو بطريقة غير شرعية.

المـــــادة 26 :

1- لكل شخص الحق في التعلم، ويجب أن يكون التعليم في مراحله الأولى والأساسية على الأقل بالمجان، وأن يكون التعليم الأولي إلزامياً وينبغي أن يعمم التعليم الفني والمهني، وأن ييسر القبول للتعليم العالي على قدم المساواة التامة للجميع وعلى أساس الكفاءة.

2- يجب أن تهدف التربية إلى إنماء شخصية الإنسان إنماء كاملاً، وإلى تعزيز احترام الإنسان والحريات الأساسية وتنمية التفاهم والتسامح والصداقة بين جميع الشعوب والجماعات العنصرية أو الدينية، وإلى زيادة مجهود الأمم المتحدة لحفظ السلام.

3- للآباء الحق الأول في اختيار نوع تربية أولادهم.

المـــــادة 27 :

1- لكل فرد الحق في أن يشترك اشتراكاً حراً في حياة المجتمع الثقافي وفي الاستمتاع بالفنون والمساهمة في التقدم العلمي والاستفادة من نتائجه.

2- لكل فرد الحق في حماية المصالح الأدبية والمادية المترتبة على إنتاجه العلمي أو الأدبي أو الفني.

المـــــادة 28 :

لكل فرد الحق في التمتع بنظام اجتماعي دولي تتحقق بمقتضاه الحقوق والحريات المنصوص عليها في هذا الإعلان تحققاً تاما.

المـــــادة 29 :

1- على كل فرد واجبات نحو المجتمع الذي يتاح فيه وحده لشخصيته أن تنمو نمواً حراً كاملاً.

2- يخضع الفرد في ممارسة حقوقه وحرياته لتلك القيود التي يقررها القانون فقط، لضمان الاعتراف بحقوق الغير وحرياته واحترامها ولتحقيق المقتضيات العادلة للنظام العام والمصلحة العامة والأخلاق في مجتمع ديمقراطي.

3- لا يصح بحال من الأحوال أن تمارس هذه الحقوق ممارسة تتناقض مع أغراض الأمم المتحدة ومبادئها.

المـــــادة 30 :

ليس في هذا الإعلان نص يجوز تأويله على أنه يخول لدولة أو جماعة أو فرد أي حق في القيام بنشاط أو تأدية عمل يهدف إلى هدم الحقوق والحريات الواردة فيه.

ملحق رقم : 15

القانون لـــ 29 جويلية 1881 – حول حرية الصحافة
الفصل الرابع : " الجنايات و الجنح المرتكبة بواسطة الصحافة أو بأي وسيلة أخرى للنشر "
و الفصل الخامس : " عن المتابعات و القمع "

مدعمة بآخر التعديلات في 7 أوت 2009
سارية المفعول بتاريخ 18 أكتوبر 2009

Loi du 29 juillet 1881 - Sur la liberté de la presse
Chapitre IV : " Des crimes et délits commis par la voie de la presse ou par tout autre moyen de publication " & chapitre V : " Des poursuites et de la répression "

Consolidée avec les dernières modifications au : 07 août 2009
Version en vigueur au 18 octobre 2009

CHAPITRE IV :
« DES CRIMES ET DELITS COMMIS PAR LA VOIE DE LA PRESSE OU PAR TOUT AUTRE MOYEN DE PUBLICATION »

Paragraphe 1er : Provocation aux crimes et délits.

Article 23
Modifié par Loi n°2004-575 du 21 juin 2004 - art. 2 JORF 22 juin 2004
Seront punis comme complices d'une action qualifiée crime ou délit ceux qui, soit par des discours, cris ou menaces proférés dans des lieux ou réunions publics, soit par des écrits, imprimés, dessins, gravures, peintures, emblèmes, images ou tout autre support de l'écrit, de la parole ou de l'image vendus ou distribués, mis en vente ou exposés dans des lieux ou réunions publics, soit par des placards ou des affiches exposés au regard du public, soit par tout moyen de communication au public par voie électronique, auront directement provoqué l'auteur ou les auteurs à commettre ladite action, si la provocation a été suivie d'effet.
Cette disposition sera également applicable lorsque la provocation n'aura été suivie que d'une tentative de crime prévue par l'article 2 du code pénal.

Article 24
Modifié par Loi n°2004-1486 du 30 décembre 2004 - art. 20 JORF 31 décembre 2004
Modifié par Loi n°2004-1486 du 30 décembre 2004 - art. 22 JORF 31 décembre 2004
Seront punis de cinq ans d'emprisonnement et de 45 000 euros d'amende ceux qui, par l'un des moyens énoncés à l'article précédent, auront directement provoqué, dans le cas où cette provocation n'aurait pas été suivie d'effet, à commettre l'une des infractions suivantes :
1° Les atteintes volontaires à la vie, les atteintes volontaires à l'intégrité de la personne et les agressions sexuelles, définies par le livre II du code pénal ;
2° Les vols, les extorsions et les destructions, dégradations et détériorations volontaires dangereuses pour les personnes, définis par le livre III du code pénal.
Ceux qui, par les mêmes moyens, auront directement provoqué à l'un des crimes et délits portant atteinte aux intérêts fondamentaux de la nation prévus par le titre Ier du livre IV du code pénal, seront punis des mêmes peines.
Seront punis de la même peine ceux qui, par l'un des moyens énoncés en l'article 23, auront fait l'apologie des crimes visés au premier alinéa, des crimes de guerre, des crimes contre l'humanité ou des crimes et délits de collaboration avec l'ennemi.
Seront punis des peines prévues par l'alinéa 1er ceux qui, par les mêmes moyens, auront provoqué directement aux actes de terrorisme prévus par le titre II du livre IV du code pénal, ou qui en auront fait l'apologie.
Tous cris ou chants séditieux proférés dans les lieux ou réunions publics seront punis de l'amende prévue pour les contraventions de la 5° classe.
Ceux qui, par l'un des moyens énoncés à l'article 23, auront provoqué à la discrimination, à la haine ou à la violence à l'égard d'une personne ou d'un groupe de personnes à raison de leur origine ou de leur appartenance ou de leur non-appartenance à une ethnie, une nation, une race ou une religion déterminée, seront punis d'un an d'emprisonnement et de 45 000 euros d'amende ou de l'une de ces deux peines seulement.
Seront punis des peines prévues à l'alinéa précédent ceux qui, par ces mêmes moyens, auront provoqué à la haine ou à la violence à l'égard d'une personne ou d'un groupe de personnes à raison de leur sexe, de leur orientation sexuelle ou de leur handicap ou auront provoqué, à l'égard des mêmes personnes, aux discriminations prévues par les articles 225-2 et 432-7 du code pénal.
En cas de condamnation pour l'un des faits prévus par les deux alinéas précédents, le tribunal pourra en outre ordonner :
1° Sauf lorsque la responsabilité de l'auteur de l'infraction est retenue sur le fondement de l'article 42 et du premier alinéa de l'article 43 de la présente loi ou des trois premiers alinéas de l'article 93-3 de la loi n° 82-652 du 29 juillet 1982 sur la

communication audiovisuelle, la privation des droits énumérés aux 2° et 3° de l'article 131-26 du code pénal pour une durée de cinq ans au plus ;
2° L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35 du code pénal.

Article 24 bis
Modifié par Loi n°92-1336 du 16 décembre 1992 - art. 247 JORF 23 décembre 1992 en vigueur le 1er mars 1994
Seront punis des peines prévues par le sixième alinéa de l'article 24 ceux qui auront contesté, par un des moyens énoncés à l'article 23, l'existence d'un ou plusieurs crimes contre l'humanité tels qu'ils sont définis par l'article 6 du statut du tribunal militaire international annexé à l'accord de Londres du 8 août 1945 et qui ont été commis soit par les membres d'une organisation déclarée criminelle en application de l'article 9 dudit statut, soit par une personne reconnue coupable de tels crimes par une juridiction française ou internationale.
Le tribunal pourra en outre ordonner :
1° L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35 du code pénal.

Paragraphe 2 : Délits contre la chose publique.

Article 26
Modifié par Ordonnance n°2000-916 du 19 septembre 2000 - art. 3 (V) JORF 22 septembre 2000 en vigueur le 1er janvier 2002
L'offense au Président de la République par l'un des moyens énoncés dans l'article 23 est punie d'une amende de 45 000 euros.
Les peines prévues à l'alinéa précédent sont applicables à l'offense à la personne qui exerce tout ou partie des prérogatives du Président de la République.

Article 27
Modifié par Ordonnance n°2000-916 du 19 septembre 2000 - art. 3 (V) JORF 22 septembre 2000 en vigueur le 1er janvier 2002
La publication, la diffusion ou la reproduction, par quelque moyen que ce soit, de nouvelles fausses, de pièces fabriquées, falsifiées ou mensongèrement attribuées à des tiers lorsque, faite de mauvaise foi, elle aura troublé la paix publique, ou aura été susceptible de la troubler, sera punie d'une amende de 45 000 euros.
Les mêmes faits seront punis 135 000 euros d'amende, lorsque la publication, la diffusion ou la reproduction faite de mauvaise foi sera de nature à ébranler la discipline ou le moral des armées ou à entraver l'effort de guerre de la Nation.

Paragraphe 3 : Délits contre les personnes.

Article 29
Créé par Loi 1881-07-29 Bulletin Lois n° 637 p. 125
Toute allégation ou imputation d'un fait qui porte atteinte à l'honneur ou à la considération de la personne ou du corps auquel le fait est imputé est une diffamation. La publication directe ou par voie de reproduction de cette allégation ou de cette imputation est punissable, même si elle est faite sous forme dubitative ou si elle vise une personne ou un corps non expressément nommés, mais dont l'identification est rendue possible par les termes des discours, cris, menaces, écrits ou imprimés, placards ou affiches incriminés.
Toute expression outrageante, termes de mépris ou invective qui ne renferme l'imputation d'aucun fait est une injure.

Article 30
Modifié par Ordonnance n°2000-916 du 19 septembre 2000 - art. 3 (V) JORF 22 septembre 2000 en vigueur le 1er janvier 2002
La diffamation commise par l'un des moyens énoncés en l'article 23 envers les cours, les tribunaux, les armées de terre, de mer ou de l'air, les corps constitués et les administrations publiques, sera punie d'une amende de 45 000 euros.

Article 31
Créé par Loi 1881-07-29 Bulletin Lois n° 637 p. 125
Sera punie de la même peine, la diffamation commise par les mêmes moyens, à raison de leurs fonctions ou de leur qualité, envers un ou plusieurs membres du ministère, un ou plusieurs membres de l'une ou de l'autre Chambre, un fonctionnaire public, un dépositaire ou agent de l'autorité publique, un ministre de l'un des cultes salariés par l'Etat, un citoyen chargé d'un service ou d'un mandat public temporaire ou permanent, un juré ou un témoin, à raison de sa déposition.
La diffamation contre les mêmes personnes concernant la vie privée relève de l'article 32 ci-après.

Article 32
Modifié par Loi n°2004-1486 du 30 décembre 2004 - art. 21 JORF 31 décembre 2004
Modifié par Loi n°2004-1486 du 30 décembre 2004 - art. 22 JORF 31 décembre 2004
La diffamation commise envers les particuliers par l'un des moyens énoncés en l'article 23 sera punie d'une amende de 12000 euros.
La diffamation commise par les mêmes moyens envers une personne ou un groupe de personnes à raison de leur origine ou de leur appartenance ou de leur non-appartenance à une ethnie, une nation, une race ou une religion déterminée sera punie d'un an d'emprisonnement et de 45000 euros d'amende ou de l'une de ces deux peines seulement.
Sera punie des peines prévues à l'alinéa précédent la diffamation commise par les mêmes moyens envers une personne ou un groupe de personnes à raison de leur sexe, de leur orientation sexuelle ou de leur handicap.
En cas de condamnation pour l'un des faits prévus par les deux alinéas précédents, le tribunal pourra en outre ordonner :
1° L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35 du code pénal.

Article 33

Modifié par Loi n°2004-1486 du 30 décembre 2004 - art. 21 JORF 31 décembre 2004
Modifié par Loi n°2004-1486 du 30 décembre 2004 - art. 22 JORF 31 décembre 2004

L'injure commise par les mêmes moyens envers les corps ou les personnes désignés par les articles 30 et 31 de la présente loi sera punie d'une amende de 12 000 euros.
L'injure commise de la même manière envers les particuliers, lorsqu'elle n'aura pas été précédée de provocations, sera punie d'une amende de 12 000 euros.
Sera punie de six mois d'emprisonnement et de 22 500 euros d'amende l'injure commise, dans les conditions prévues à l'alinéa précédent, envers une personne ou un groupe de personnes à raison de leur origine ou de leur appartenance ou de leur non-appartenance à une ethnie, une nation, une race ou une religion déterminée.
Sera punie des peines prévues à l'alinéa précédent l'injure commise dans les mêmes conditions envers une personne ou un groupe de personnes à raison de leur sexe, de leur orientation sexuelle ou de leur handicap.
En cas de condamnation pour l'un des faits prévus par les deux alinéas précédents, le tribunal pourra en outre ordonner :
1° L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35 du code pénal.

Article 34

Créé par Loi 1881-07-29 Bulletin Lois n° 637 p. 125

Les articles 31, 32 et 33 ne seront applicables aux diffamations ou injures dirigées contre la mémoire des morts que dans le cas où les auteurs de ces diffamations ou injures auraient eu l'intention de porter atteinte à l'honneur ou à la considération des héritiers, époux ou légataires universels vivants.
Que les auteurs des diffamations ou injures aient eu ou non l'intention de porter atteinte à l'honneur ou à la considération des héritiers, époux ou légataires universels vivants, ceux-ci pourront user, dans les deux cas, du droit de réponse prévu par l'article 13.

Article 35

Modifié par Ordonnance n°2009-80 du 22 janvier 2009 - art. 19

La vérité du fait diffamatoire, mais seulement quand il est relatif aux fonctions, pourra être établie par les voies ordinaires, dans le cas d'imputations contre les corps constitués, les armées de terre, de mer ou de l'air, les administrations publiques et contre toutes les personnes énumérées dans l'article 31.
La vérité des imputations diffamatoires et injurieuses pourra être également établie contre les directeurs ou administrateurs de toute entreprise industrielle, commerciale ou financière, dont les titres financiers sont admis aux négociations sur un marché réglementé ou offerts au public sur un système multilatéral de négociation ou au crédit.
La vérité des faits diffamatoires peut toujours être prouvée, sauf :
a) Lorsque l'imputation concerne la vie privée de la personne ;
b) Lorsque l'imputation se réfère à des faits qui remontent à plus de dix années ;
c) Lorsque l'imputation se réfère à un fait constituant une infraction amnistiée ou prescrite, ou qui a donné lieu à une condamnation effacée par la réhabilitation ou la révision ;
Les deux alinéas a et b qui précèdent ne s'appliquent pas lorsque les faits sont prévus et réprimés par les articles 222-23 à 222-32et 227-22 à 227-27 du code pénal et ont été commis contre un mineur.
Dans les cas prévus aux deux paragraphes précédents, la preuve contraire est réservée. Si la preuve du fait diffamatoire est rapportée, le prévenu sera renvoyé des fins de la plainte.
Dans toute autre circonstance et envers toute autre personne non qualifiée, lorsque le fait imputé est l'objet de poursuites commencées à la requête du ministère public, ou d'une plainte de la part du prévenu, il sera, durant l'instruction qui devra avoir lieu, sursis à la poursuite et au jugement du délit de diffamation.

Article 35 bis

Toute reproduction d'une imputation qui a été jugée diffamatoire sera réputée faite de mauvaise foi, sauf preuve contraire par son auteur.

Article 35 ter

Modifié par Ordonnance n°2000-916 du 19 septembre 2000 - art. 3 (V) JORF 22 septembre 2000 en vigueur le 1er janvier 2002

I. - Lorsqu'elle est réalisée sans l'accord de l'intéressé, la diffusion, par quelque moyen que ce soit et quel qu'en soit le support, de l'image d'une personne identifiée ou identifiable mise en cause à l'occasion d'une procédure pénale mais n'ayant pas fait l'objet d'un jugement de condamnation et faisant apparaître, soit que cette personne porte des menottes ou entraves, soit qu'elle est placée en détention provisoire, est punie de 15 000 euros d'amende.
II. - Est puni de la même peine le fait :
- soit de réaliser, de publier ou de commenter un sondage d'opinion, ou toute autre consultation, portant sur la culpabilité d'une personne mise en cause à l'occasion d'une procédure pénale ou sur la peine susceptible d'être prononcée à son encontre ;
- soit de publier des indications permettant d'avoir accès à des sondages ou consultations visés à l'alinéa précédent.

Article 35 quater

Modifié par Ordonnance n°2000-916 du 19 septembre 2000 - art. 3 (V) JORF 22 septembre 2000 en vigueur le 1er janvier 2002

La diffusion, par quelque moyen que ce soit et quel qu'en soit le support, de la reproduction des circonstances d'un crime ou d'un délit, lorsque cette reproduction porte gravement atteinte à la dignité d'une victime et qu'elle est réalisée sans l'accord de cette dernière, est punie de 15 000 euros d'amende.

Paragraphe 4 : Délits contre les chefs d'Etat et agents diplomatiques étrangers.

Article 36 (abrogé)
Modifié par Ordonnance n°2000-916 du 19 septembre 2000 - art. 3 (V) JORF 22 septembre 2000 en vigueur le 1er janvier 2002
Abrogé par Loi n°2004-204 du 9 mars 2004 - art. 52 JORF 10 mars 2004

Article 37
Modifié par Ordonnance n°2000-916 du 19 septembre 2000 - art. 3 (V) JORF 22 septembre 2000 en vigueur le 1er janvier 2002
L'outrage commis publiquement envers les ambassadeurs et ministres plénipotentiaires, envoyés, chargés d'affaires ou autres agents diplomatiques accrédités près du gouvernement de la République, sera puni d'une amende de 45 000 euros.

Paragraphe 5 : Publications interdites, immunités de la défense.

Article 38
Modifié par Ordonnance n°2000-916 du 19 septembre 2000 - art. 3 (V) JORF 22 septembre 2000 en vigueur le 1er janvier 2002
Modifié par Loi n°2001-539 du 25 juin 2001 - art. 22 JORF 25 juin 2001
Il est interdit de publier les actes d'accusation et tous autres actes de procédure criminelle ou correctionnelle avant qu'ils aient été lus en audience publique et ce, sous peine d'une amende de 3 750 euros.
Sans préjudice des dispositions de l'article 15 du code pénal, il est interdit, sous la même peine, de publier aucune information relative aux travaux et délibérations du conseil supérieur de la magistrature, à l'exception des informations concernant les audiences publiques et les décisions publiques rendues en matière disciplinaire à l'encontre des magistrats. Pourront toutefois être publiées les informations communiquées par le président ou le vice-président dudit conseil.

NOTA:
L'article 15 est abrogé par la loi n° 81-908 du 9 octobre 1981.

Article 38 ter
Modifié par Ordonnance n°2000-916 du 19 septembre 2000 - art. 3 (V) JORF 22 septembre 2000 en vigueur le 1er janvier 2002
Dès l'ouverture de l'audience des juridictions administratives ou judiciaires, l'emploi de tout appareil permettant d'enregistrer, de fixer ou de transmettre la parole ou l'image est interdit. Le président fait procéder à la saisie de tout appareil et du support de la parole ou de l'image utilisés en violation de cette interdiction.
Toutefois, sur demande présentée avant l'audience, le président peut autoriser des prises de vues quand les débats ne sont pas commencés et à la condition que les parties ou leurs représentants et le ministère public y consentent.
Toute infraction aux dispositions du présent article sera punie de 4 500 euros d'amende. Le tribunal pourra en outre prononcer la confiscation du matériel ayant servi à commettre l'infraction et du support de la parole ou de l'image utilisé.
Est interdite, sous les mêmes peines, la cession ou la publication, de quelque manière et par quelque moyen que ce soit, de tout enregistrement ou document obtenu en violation des dispositions du présent article.

Article 39
Modifié par Ordonnance n°2000-916 du 19 septembre 2000 - art. 3 (V) JORF 22 septembre 2000 en vigueur le 1er janvier 2002
Il est interdit de rendre compte des procès en diffamation dans les cas prévus aux paragraphes a, b et c de l'article 35 de la présente loi. Il est pareillement interdit de rendre compte des débats et de publier des pièces de procédures concernant les questions de filiation, actions à fins de subsides, procès en divorce, séparation de corps et nullités de mariage, procès en matière d'avortement. Cette interdiction ne s'applique pas au dispositif des décisions, qui peut toujours être publié.
Les dispositions qui précèdent ne s'appliquent pas aux publications techniques à condition que soit respecté l'anonymat des parties.
Dans toutes affaires civiles, les cours et tribunaux pourront interdire le compte rendu du procès.
Il est également interdit de rendre compte des délibérations intérieures, soit des jurys, soit des cours et tribunaux.
Toute infraction à ces dispositions sera punie d'une amende de 18 000 euros.

Article 39 bis
Modifié par Ordonnance n°2000-916 du 19 septembre 2000 - art. 3 (V) JORF 22 septembre 2000 en vigueur le 1er janvier 2002
Est puni de 15 000 euros d'amende le fait de diffuser, de quelque manière que ce soit, des informations relatives à l'identité ou permettant l'identification :
- d'un mineur ayant quitté ses parents, son tuteur, la personne ou l'institution qui était chargée de sa garde ou à laquelle il était confié ;
- d'un mineur délaissé dans les conditions mentionnées aux articles 227-1 et 227-2 du code pénal ;
- d'un mineur qui s'est suicidé ;
- d'un mineur victime d'une infraction.
Les dispositions du présent article ne sont pas applicables lorsque la publication est réalisée à la demande des personnes ayant la garde du mineur ou des autorités administratives ou judiciaires.

Article 39 ter (abrogé)
Modifié par Loi n°92-1336 du 16 décembre 1992 - art. 322 (V) JORF 23 décembre 1992 en vigueur le 1er mars 1994
Abrogé par Loi n°2000-516 du 15 juin 2000 - art. 99 (V) JORF 16 juin 2000

Article 39 quater

Modifié par Ordonnance n°2000-916 du 19 septembre 2000 - art. 3 (V) JORF 22 septembre 2000 en vigueur le 1er janvier 2002

Il est interdit, moins de trente ans après la mort de l'adopté, de publier par le livre, la presse, la radiodiffusion, le cinématographe ou de quelque manière que ce soit, une information relative à la filiation d'origine d'une personne ayant fait l'objet d'une adoption plénière.

Les infractions à la disposition qui précède sont punies de 6 000 euros d'amende ; en cas de récidive un emprisonnement de deux ans pourra être prononcé.

Article 39 quinquies

Modifié par Ordonnance n°2000-916 du 19 septembre 2000 - art. 3 (V) JORF 22 septembre 2000 en vigueur le 1er janvier 2002

Le fait de diffuser, par quelque moyen que ce soit et quel qu'en soit le support, des renseignements concernant l'identité d'une victime d'une agression ou d'une atteinte sexuelles ou l'image de cette victime lorsqu'elle est identifiable est puni de 15 000 euros d'amende.

Les dispositions du présent article ne sont pas applicables lorsque la victime a donné son accord écrit.

Article 39 sexies

Modifié par LOI n°2009-971 du 3 août 2009 - art. 21

Le fait de révéler, par quelque moyen d'expression que ce soit, l'identité des fonctionnaires de la police nationale, de militaires, de personnels civils du ministère de la défense ou d'agents des douanes appartenant à des services ou unités désignés par arrêté du ministre intéressé et dont les missions exigent, pour des raisons de sécurité, le respect de l'anonymat, est puni d'une amende de 15 000 euros.

Article 40

Modifié par Ordonnance n°2000-916 du 19 septembre 2000 - art. 3 (V) JORF 22 septembre 2000 en vigueur le 1er janvier 2002

Il est interdit d'ouvrir ou d'annoncer publiquement des souscriptions ayant pour objet d'indemniser des amendes, frais et dommages-intérêts prononcés par des condamnations judiciaires, en matière criminelle et correctionnelle, sous peine de six mois d'emprisonnement et de 45 000 euros d'amende, ou de l'une de ces deux peines seulement.

Article 41

Modifié par LOI n°2008-1187 du 14 novembre 2008 - art. 1

Ne donneront ouverture à aucune action les discours tenus dans le sein de l'Assemblée nationale ou du Sénat ainsi que les rapports ou toute autre pièce imprimée par ordre de l'une de ces deux assemblées.

Ne donnera lieu à aucune action le compte rendu des séances publiques des assemblées visées à l'alinéa ci-dessus fait de bonne foi dans les journaux.

Ne donneront lieu à aucune action en diffamation, injure ou outrage ni les propos tenus ou les écrits produits devant une commission d'enquête créée, en leur sein, par l'Assemblée nationale ou le Sénat, par la personne tenue d'y déposer, sauf s'ils sont étrangers à l'objet de l'enquête, ni le compte rendu fidèle des réunions publiques de cette commission fait de bonne foi.

Ne donneront lieu à aucune action en diffamation, injure ou outrage, ni le compte rendu fidèle fait de bonne foi des débats judiciaires, ni les discours prononcés ou les écrits produits devant les tribunaux.

Pourront néanmoins les juges, saisis de la cause et statuant sur le fond, prononcer la suppression des discours injurieux, outrageants ou diffamatoires, et condamner qui il appartiendra à des dommages-intérêts.

Pourront toutefois les faits diffamatoires étrangers à la cause donner ouverture, soit à l'action publique, soit à l'action civile des parties, lorsque ces actions leur auront été réservées par les tribunaux, et, dans tous les cas, à l'action civile des tiers.

Article 41-1

Créé par Loi 85-1317 1985-12-13 art. 18 II JORF 24 décembre 1985

Pour l'application des dispositions des paragraphes 4 et 5 du présent chapitre, la communication audiovisuelle est regardée comme un mode de publication.

CHAPITRE V : DES POURSUITES ET DE LA REPRESSION

Paragraphe 1er : Des personnes responsables de crimes et délits commis par la voie de la presse.

Article 42

Créé par Loi 1881-07-29 Bulletin Lois n° 637 p. 125

Modifié par Ordonnance 1944-08-26 ART. 15 JORF 30 août 1944

Modifié par Loi n°52-336 du 25 mars 1952 - art. 4 JORF 26 mars 1952

Seront passibles, comme auteurs principaux des peines qui constituent la répression des crimes et délits commis par la voie de la presse, dans l'ordre ci-après, savoir :

1° Les directeurs de publications ou éditeurs, quelles que soient leurs professions ou leurs dénominations, et, dans les cas prévus au deuxième alinéa de l'article 6, de les codirecteurs de la publication ;

2° A leur défaut, les auteurs ;

3° A défaut des auteurs, les imprimeurs ;

4° A défaut des imprimeurs, les vendeurs, les distributeurs et afficheurs.

Dans les cas prévus au deuxième alinéa de l'article 6, la responsabilité subsidiaire des personnes visées aux paragraphes 2°, 3° et 4° du présent article joue comme s'il n'y avait pas de directeur de la publication, lorsque, contrairement aux dispositions de la présente loi, un codirecteur de la publication n'a pas été désigné.

Article 43

Créé par Loi 1881-07-29 Bulletin LOIS N° 637 p. 125
Modifié par Ordonnance 1944-08-26 art. 15 JORF 30 août 1944
Modifié par Loi n°52-336 du 25 mars 1952 - art. 5 JORF 26 mars 1952
Lorsque les directeurs ou codirecteurs de la publication ou les éditeurs seront en cause, les auteurs seront poursuivis comme complices.
Pourront l'être, au même titre et dans tous les cas, les personnes auxquelles l'article 121-7 du code pénal pourrait s'appliquer. Ledit article ne pourra s'appliquer aux imprimeurs pour faits d'impression, sauf dans le cas et les conditions prévus par l'article431-6 du code pénal sur les attroupements ou, à défaut de codirecteur de la publication, dans le cas prévu au deuxième alinéa de l'article 6.
Toutefois, les imprimeurs pourront être poursuivis comme complices si l'irresponsabilité pénale du directeur ou du codirecteur de la publication était prononcée par les tribunaux. En ce cas, les poursuites sont engagées dans les trois mois du délit ou, au plus tard, dans les trois mois de la constatation judiciaire de l'irresponsabilité du directeur ou du codirecteur de la publication.

Article 43-1

Créé par Loi n°2004-204 du 9 mars 2004 - art. 55 JORF 10 mars 2004
Les dispositions de l'article 121-2 du code pénal ne sont pas applicables aux infractions pour lesquelles les dispositions des articles 42 ou 43 de la présente loi sont applicables.

Article 44

Créé par Loi 1881-07-29 Bulletin Lois n° 637 p. 125
Modifié par Loi n°52-336 du 25 mars 1952 - art. 6 JORF 26 mars 1952
Les propriétaires des journaux ou écrits périodiques sont responsables des condamnations pécuniaires prononcées au profit des tiers contre les personnes désignées dans les deux articles précédents, conformément aux dispositions des articles 1382, 1383, 1384 du code civil.
Dans les cas prévus au deuxième alinéa de l'article 6, le recouvrement des amendes et dommages-intérêts pourra être poursuivi sur l'actif de l'entreprise.

Article 45

Créé par Loi 1881-07-29 Bulletin Lois n° 637 p. 125
Les infractions aux lois sur la presse sont déférées aux tribunaux correctionnels sauf :
a) Dans les cas prévus par l'article 23 en cas de crime ;
b) Lorsqu'il s'agit de simples contraventions.

Article 46

Créé par Loi 1881-07-29 Bulletin Lois n° 637 p. 125
L'action civile résultant des délits de diffamation prévus et punis par les articles 30 et 31 ne pourra, sauf dans les cas de décès de l'auteur du fait incriminé ou d'amnistie, être poursuivie séparément de l'action publique.

Paragraphe 2 : De la procédure.

Article 47

La poursuite des délits et contraventions de police commis par la voie de la presse ou par tout autre moyen de publication aura lieu d'office et à la requête du ministère public sous les modifications ci-après.

Article 48

Modifié par Loi n°2007-297 du 5 mars 2007 - art. 34 JORF 7 mars 2007
1° Dans le cas d'injure ou de diffamation envers les cours, tribunaux et autres corps indiqués en l'article 30, la poursuite n'aura lieu que sur une délibération prise par eux en assemblée générale et requérant les poursuites, ou, si le corps n'a pas d'assemblée générale, sur la plainte du chef du corps ou du ministre duquel ce corps relève ;
1° bis Dans les cas d'injure et de diffamation envers un membre du Gouvernement, la poursuite aura lieu sur sa demande adressée au ministre de la justice ;
2° Dans le cas d'injure ou de diffamation envers un ou plusieurs membres de l'une ou de l'autre Chambre, la poursuite n'aura lieu que sur la plainte de la personne ou des personnes intéressées ;
3° Dans le cas d'injure ou de diffamation envers les fonctionnaires publics, les dépositaires ou agents de l'autorité publique autres que les ministres et envers les citoyens chargés d'un service ou d'un mandat public, la poursuite aura lieu, soit sur leur plainte, soit d'office sur la plainte du ministre dont ils relèvent ;
4° Dans le cas de diffamation envers un juré ou un témoin, délit prévu par l'article 31, la poursuite n'aura lieu que sur la plainte du juré ou du témoin qui se prétendra diffamé ;
5° Dans le cas d'offense envers les chefs d'Etat ou d'outrage envers les agents diplomatiques étrangers, la poursuite aura lieu sur leur demande adressée au ministre des affaires étrangères et par celui-ci au ministre de la justice ;
6° Dans le cas de diffamation envers les particuliers prévu par l'article 32 et dans le cas d'injure prévu par l'article 33, paragraphe 2, la poursuite n'aura lieu que sur la plainte de la personne diffamée ou injuriée. Toutefois, la poursuite, pourra être exercée d'office par le ministère public lorsque la diffamation ou l'injure aura été commise envers une personne ou un groupe de personnes à raison de leur origine ou de leur appartenance ou de leur non-appartenance à une ethnie, une nation, une race ou une religion déterminée. La poursuite pourra également être exercée d'office par le ministère public lorsque la

diffamation ou l'injure aura été commise envers un groupe de personnes à raison de leur sexe, de leur orientation sexuelle ou de leur handicap ; il en sera de même lorsque ces diffamations ou injures auront été commises envers des personnes considérées individuellement, à la condition que celles-ci aient donné leur accord ;
7° Dans le cas de diffusion de l'image d'une personne menottée ou entravée prévue par l'article 35 ter, la poursuite n'aura lieu que sur la plainte de la personne intéressée ;
8° Dans le cas d'atteinte à la dignité de la victime prévue par l'article 35 quater, la poursuite n'aura lieu que sur la plainte de la victime.
En outre, dans les cas prévus par les 2°, 3°, 4°, 5°, 6°, 7° et 8° ci-dessus, ainsi que dans les cas prévus aux articles 13 et 39 quinquies de la présent loi, la poursuite pourra être exercée à la requête de la partie lésée.

Article 48-1
Modifié par Loi n°2007-297 du 5 mars 2007 - art. 34 JORF 7 mars 2007
Toute association régulièrement déclarée depuis au moins cinq ans à la date des faits, se proposant, par ses statuts, de défendre la mémoire des esclaves et l'honneur de leurs descendants, de combattre le racisme ou d'assister les victimes de discrimination fondée sur leur origine nationale, ethnique, raciale ou religieuse, peut exercer les droits reconnus à la partie civile en ce qui concerne les infractions prévues par les articles 24 (dernier alinéa), 32 (alinéa 2) et 33 (alinéa 3), de la présente loi, ainsi que les délits de provocation prévus par le 1° de l'article 24, lorsque la provocation concerne des crimes ou délits commis avec la circonstance aggravante prévue par l'article 132-76 du code pénal.
Toutefois, quand l'infraction aura été commise envers des personnes considérées individuellement, l'association ne sera recevable dans son action que si elle justifie avoir reçu l'accord de ces personnes.

Article 48-2
Créé par Loi n°90-615 du 13 juillet 1990 - art. 13 JORF 14 juillet 1990
Toute association régulièrement déclarée depuis au moins cinq ans à la date des faits, qui se propose, par ses statuts, de défendre les intérêts moraux et l'honneur de la Résistance ou des déportés peut exercer les droits reconnus à la partie civile en ce qui concerne l'apologie des crimes de guerre, des crimes contre l'humanité ou des crimes ou délits de collaboration avec l'ennemi et en ce qui concerne l'infraction prévue par l'article 24 bis.

Article 48-3
Modifié par Loi n°2006-449 du 18 avril 2006 - art. 27 JORF 19 avril 2006
Toute association régulièrement déclarée depuis au moins cinq ans à la date des faits et inscrite auprès de l'Office national des anciens combattants et victimes de guerre dans des conditions fixées par décret en Conseil d'Etat, qui se propose par ses statuts de défendre les intérêts moraux et l'honneur des anciens combattants et victimes de guerre et des morts pour la France, peut exercer les droits reconnus à la partie civile en ce qui concerne les délits de diffamation ou d'injures qui ont causé un préjudice direct ou indirect à la mission qu'elle remplit.
En cas de diffamation ou d'injure contre les armées prévues par l'article 30 et le premier alinéa de l'article 33, les dispositions du 1° de l'article 48 ne sont pas applicables.
En cas de diffamation ou d'injure commises envers des personnes considérées individuellement, l'association ne sera recevable dans son action que si elle justifie avoir reçu l'accord de ces personnes ou de leurs ayants droit.

Article 48-4
Modifié par Loi n°2007-297 du 5 mars 2007 - art. 34 JORF 7 mars 2007
Toute association, régulièrement déclarée depuis au moins cinq ans à la date des faits, se proposant, par ses statuts, de combattre les violences ou les discriminations fondées sur l'orientation sexuelle ou d'assister les victimes de ces discriminations peut exercer les droits reconnus à la partie civile en ce qui concerne les délits prévus par le neuvième alinéa de l'article 24, le troisième alinéa de l'article 32 et le quatrième alinéa de l'article 33, ainsi que les délits de provocation prévus par le 1° de l'article 24, lorsque la provocation concerne des crimes ou délits commis avec la circonstance aggravante prévue par l'article 132-77 du code pénal.
Toutefois, quand l'infraction aura été commise envers des personnes considérées individuellement, l'association ne sera recevable dans son action que si elle justifie avoir reçu l'accord de ces personnes.

Article 48-5
Modifié par Loi n°2007-297 du 5 mars 2007 - art. 34 JORF 7 mars 2007
Toute association, régulièrement déclarée depuis au moins cinq ans à la date des faits, se proposant, par ses statuts, de combattre les violences ou les discriminations fondées sur le sexe ou d'assister les victimes de ces discriminations peut exercer les droits reconnus à la partie civile en ce qui concerne les délits prévus par le neuvième alinéa de l'article 24, le troisième alinéa de l'article 32 et le quatrième alinéa de l'article 33, ainsi que les délits de provocation prévus par le 1° de l'article 24, lorsque la provocation concerne des crimes ou délits d'agressions sexuelles ou commis avec la circonstance aggravante prévue par l'article 132-80 du code pénal.
Toutefois, quand l'infraction aura été commise envers des personnes considérées individuellement, l'association ne sera recevable dans son action que si elle justifie avoir reçu l'accord de ces personnes.

Article 48-6
Modifié par Loi n°2007-297 du 5 mars 2007 - art. 34 JORF 7 mars 2007
Toute association, régulièrement déclarée depuis au moins cinq ans à la date des faits, se proposant, par ses statuts, de combattre les violences ou les discriminations fondées sur le handicap ou d'assister les victimes de ces discriminations peut exercer les droits reconnus à la partie civile en ce qui concerne les délits prévus au neuvième alinéa de l'article 24, au troisième alinéa de l'article 32 et au quatrième alinéa de l'article 33, ainsi que les délits de provocation prévus par le 1° de l'article 24, lorsque la provocation concerne des crimes ou délits aggravés en raison du handicap de la victime.
Toutefois, quand l'infraction aura été commise envers des personnes considérées individuellement, l'association ne sera recevable dans son action que si elle justifie avoir reçu l'accord de ces personnes.

Article 49
Dans tous les cas de poursuites correctionnelles ou de simple police, le désistement du plaignant ou de la partie poursuivante arrêtera la poursuite commencée.

Article 50
Si le ministère public requiert une information, il sera tenu, dans son réquisitoire, d'articuler et de qualifier les provocations, outrages, diffamations et injures à raison desquels la poursuite est intentée, avec indication des textes dont l'application est demandée, à peine de nullité du réquisitoire de ladite poursuite.

Article 50-1
Créé par Loi n°2007-297 du 5 mars 2007 - art. 39 JORF 7 mars 2007
Lorsque les faits visés par les articles 24 et 24 bis résultent de messages ou informations mis à disposition du public par un service de communication au public en ligne et qu'ils constituent un trouble manifestement illicite, l'arrêt de ce service peut être prononcé par le juge des référés, à la demande du ministère public et de toute personne physique ou morale ayant intérêt à agir.

Article 51
Immédiatement après le réquisitoire, le juge d'instruction pourra, mais seulement en cas d'omission du dépôt prescrit par les articles 3 et 10 ci-dessus, ordonner la saisie de quatre exemplaires de l'écrit, du journal ou du dessin incriminé.
Toutefois, dans les cas prévus aux articles 24 (par. 1er et 3), 25, 36, et 37 de la présente loi, la saisie des écrits ou imprimés, des placards ou affiches, aura lieu conformément aux règles édictées par le code de procédure pénale.

Article 52
Modifié par Loi 93-1013 1993-08-24 art. 46 JORF 25 août 1993 en vigueur le 2 septembre 1993
Si la personne mise en examen est domiciliée en France, elle ne pourra être préventivement arrêtée, sauf dans les cas prévus aux articles 23, 24 (par. 1er et 3), 25, 27, 36 et 37 ci-dessus.

Article 53
La citation précisera et qualifiera le fait incriminé, elle indiquera le texte de loi applicable à la poursuite.
Si la citation est à la requête du plaignant, elle contiendra élection de domicile dans la ville où siège la juridiction saisie et sera notifiée tant au prévenu qu'au ministère public.
Toutes ces formalités seront observées à peine de nullité de la poursuite.

Article 54
Le délai entre la citation et la comparution sera de vingt jours outre un jour par cinq myriamètres de distance.
Toutefois, en cas de diffamation ou d'injure pendant la période électorale contre un candidat à une fonction électorale, ce délai sera réduit à vingt-quatre heures, outre le délai de distance, et les dispositions des articles 55 et 56 ne seront pas applicables.

Article 55
Quand le prévenu voudra être admis à prouver la vérité des faits diffamatoires, conformément aux dispositions de l'article 35 de la présente loi, il devra, dans le délai de dix jours après la signification de la citation, faire signifier au ministère public ou au plaignant au domicile par lui élu, suivant qu'il est assigné à la requête de l'un ou de l'autre :
1° Les faits articulés et qualifiés dans la citation, desquels il entend prouver la vérité ;
2° La copie des pièces ;
3° Les noms, professions et demeures des témoins par lesquels il entend faire la preuve.
Cette signification contiendra élection de domicile près le tribunal correctionnel, le tout à peine d'être déchu du droit de faire la preuve.

Article 56
Dans les cinq jours suivants, en tous cas moins de trois jours francs avant l'audience, le plaignant ou le ministère public, suivant le cas, sera tenu de faire signifier au prévenu, au domicile par lui élu, les copies des pièces et les noms, professions et demeures des témoins par lesquels il entend faire la preuve du contraire sous peine d'être déchu de son droit.

Article 57
Le tribunal correctionnel et le tribunal de police seront tenus de statuer au fond dans le délai maximum d'un mois à compter de la date de la première audience.
Dans le cas prévu à l'alinéa 2 de l'article 54, la cause ne pourra être remise au-delà du jour fixé pour le scrutin.

Article 58
Modifié par Loi 81-759 1981-08-06 art. 3 JORF 7 août 1981
Le droit de se pourvoir en cassation appartiendra au prévenu et à la partie civile quant aux dispositions relatives à ses intérêts civils. Le prévenu sera dispensé de se mettre en état.
La partie civile pourra user du bénéfice de l'article 585 du Code de procédure pénale sans le ministère d'un avocat à la Cour de cassation.

Article 59
Le pourvoi devra être formé, dans les trois jours au greffe de la cour ou du tribunal qui aura rendu la décision. Dans les vingt-quatre heures qui suivront, les pièces seront envoyées à la Cour de cassation, qui jugera d'urgence dans les dix jours à partir de leur réception.

L'appel contre les jugements ou le pourvoi contre les arrêts des cours d'appel qui auront statué sur les incidents et exceptions autres que les exceptions d'incompétence ne sera formé, à peine de nullité, qu'après le jugement ou l'arrêt définitif et en même temps que l'appel ou le pourvoi contre ledit jugement ou arrêt.
Toutes les exceptions d'incompétence devront être proposées avant toute ouverture du débat sur le fond : faute de ce, elles seront jointes au fond et il sera statué sur le tout par le même jugement.

Article 60
Sous réserve des dispositions des articles 50, 51, et 52 ci-dessus, la poursuite des crimes [*commis par la voie de la presse*] aura lieu conformément au droit commun.

Paragraphe 3 : Peines complémentaires, récidive, circonstances atténuantes, prescription.

Article 61
S'il y a condamnation, l'arrêt pourra, dans les cas prévus aux articles 24 (par. 1er et 3), 25, 36 et 37, prononcer la confiscation des écrits ou imprimés, placards ou affiches saisis et, dans tous les cas, ordonner la saisie et la suppression ou la destruction de tous les exemplaires qui seraient mis en vente, distribués ou exposés aux regard du public. Toutefois, la suppression ou la destruction pourra ne s'appliquer qu'à certaines parties des exemplaires saisis.

Article 62
En cas de condamnation prononcée en application des articles 23, 24 (alinéas 1er et 2), 25 et 27, la suspension du journal ou du périodique pourra être prononcée par la même décision de justice pour une durée qui n'excédera pas trois mois. Cette suspension sera sans effet sur les contrats de travail qui liaient l'exploitant lequel reste tenu de toutes les obligations contractuelles ou légales en résultant.

Article 63
Modifié par Loi n°2004-1486 du 30 décembre 2004 - art. 22 JORF 31 décembre 2004
L'aggravation des peines résultant de la récidive ne sera applicable qu'aux infractions prévues par les articles 24 (alinéas 5, 6, 8 et 9), 32 (alinéas 2 et 3) et 33 (alinéas 3 et 4) de la présente loi.
En cas de conviction de plusieurs crimes ou délits prévus par la présente loi, les peines ne se cumuleront pas, et la plus forte sera seule prononcée.

Article 64
Modifié par Loi n°2000-516 du 15 juin 2000 - art. 95 JORF 16 juin 2000
Lorsque ont été ordonnées en référé des mesures limitant par quelque moyen que ce soit la diffusion de l'information, le premier président de la cour d'appel statuant en référé peut, en cas d'appel, arrêter l'exécution provisoire de la décision si celle-ci risque d'entraîner des conséquences manifestement excessives.

Article 65
Modifié par Loi n°93-2 du 4 janvier 1993 - art. 52 JORF 5 janvier 1993
L'action publique et l'action civile résultant des crimes, délits et contraventions prévus par la présente loi se prescriront après trois mois révolus, à compter du jour où ils auront été commis ou du jour du dernier acte d'instruction ou de poursuite s'il en a été fait.
Toutefois, avant l'engagement des poursuites, seules les réquisitions aux fins d'enquête seront interruptives de prescription. Ces réquisitions devront, à peine de nullité, articuler et qualifier les provocations, outrages, diffamations et injures à raison desquels l'enquête est ordonnée.
Les prescriptions commencées à l'époque de la publication de la présente loi, et pour lesquelles il faudrait encore, suivant les lois existantes, plus de trois mois à compter de la même époque, seront, par ce laps de trois mois, définitivement accomplies.

Article 65-1
Créé par Loi n°93-2 du 4 janvier 1993 - art. 53 JORF 5 janvier 1993
Les actions fondées sur une atteinte au respect de la présomption d'innocence commise par l'un des moyens visés à l'article 23 se prescriront après trois mois révolus à compter du jour de l'acte de publicité.

Article 65-2
Créé par Loi n°93-2 du 4 janvier 1993 - art. 52 JORF 5 janvier 1993
En cas d'imputation portant sur un fait susceptible de revêtir une qualification pénale, le délai de prescription prévu par l'article 65 est réouvert ou court à nouveau, au profit de la personne visée, à compter du jour où est devenue définitive une décision pénale intervenue sur ces faits et ne la mettant pas en cause.

Article 65-3
Créé par Loi n°2004-204 du 9 mars 2004 - art. 45 JORF 10 mars 2004
Pour les délits prévus par le huitième alinéa de l'article 24, l'article 24 bis, le deuxième alinéa de l'article 32 et le troisième alinéa de l'article 33, le délai de prescription prévu par l'article 65 est porté à un an.

Article 68
Créé par Loi 1881-07-29 Bulletin Lois n° 637 p. 125
Sont abrogés les édits, lois, décrets, ordonnances, arrêtés, règlements, déclarations généralement quelconques, relatifs à l'imprimerie, à la librairie, à la presse périodique ou non périodique, au colportage, à l'affichage, à la vente sur la voie publique et aux crimes et délits prévus par les lois sur la presse et les autres moyens de publication, sans que puissent revivre les dispositions abrogées par les lois antérieures.

Est également abrogé le second paragraphe de l'article 31 de la loi du 10 août 1871 sur les conseils généraux, relatif à l'appréciation de leurs discussions par les journaux.

Article 69

Modifié par Ordonnance n°96-267 du 28 mars 1996 - art. 10 (V)

La présente loi est applicable dans les territoires d'outre-mer et dans la collectivité territoriale de Mayotte.

أنظر صفحة الأنترنت في العنوان التالي :

http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006070722&dateTexte=20091018

ملحق رقم : 16

القانون رقم 98-468 لـــ 17 جوان 1998 المتعلق بالوقاية و قمع الجرائم الجنسية و كذا حماية القصر

متمم و منقح في 26 جويلية 2009

Loi n° 98-468 du 17 juin 1998 relative à la prévention et à la répression des infractions sexuelles ainsi qu'a la protection des mineurs
Version consolidée au 26 juillet 2009

Titre II :
Dispositions ayant pour objet de prévenir et de réprimer les infractions sexuelles, les atteintes à la dignité de la personne humaine et de protéger les mineurs victimes

Chapitre Ier : Dispositions modifiant le code pénal

Article 10
A modifié les dispositions suivantes :
Crée Code pénal - art. 132-16-1 (V)

Article 11
A modifié les dispositions suivantes :
Modifie Code pénal - art. 222-33 (M)

Article 12
A modifié les dispositions suivantes :
Modifie Code pénal - art. 222-45 (M)

Article 13
A modifié les dispositions suivantes :
Modifie Code pénal - art. 222-24 (M)
Modifie Code pénal - art. 222-28 (M)
Modifie Code pénal - art. 225-7 (M)
Modifie Code pénal - art. 227-22 (M)
Modifie Code pénal - art. 227-26 (M)

Article 14
A modifié les dispositions suivantes :
Crée Code pénal - art. 225-16-1 (M)
Crée Code pénal - art. 225-16-2 (M)
Crée Code pénal - art. 225-16-3 (V)

Article 15
A modifié les dispositions suivantes :
Modifie Code pénal - art. 226-14 (M)
Modifie Code pénal - art. 434-3 (M)

Article 16
A modifié les dispositions suivantes :
Modifie Code pénal - art. 222-12 (M)
Modifie Code pénal - art. 222-13 (M)
Modifie Code pénal - art. 227-18 (M)
Modifie Code pénal - art. 227-18-1 (M)
Modifie Code pénal - art. 227-19 (M)
Modifie Code pénal - art. 227-21 (M)
Modifie Code pénal - art. 227-22 (M)

Article 17
A modifié les dispositions suivantes :
Modifie Code pénal - art. 227-23 (M)

Article 18
A modifié les dispositions suivantes :

Modifie Code pénal - art. 227-25 (M)

Article 19
A modifié les dispositions suivantes :
Modifie Code pénal - art. 222-22 (M)
Modifie Code pénal - art. 227-26 (M)
Crée Code pénal - art. 227-27-1 (V)

Article 20
A modifié les dispositions suivantes :
Crée Code pénal - art. 227-28-1 (M)

Article 21
A modifié les dispositions suivantes :
Modifie Code pénal - art. 227-29 (M)

Article 22
A modifié les dispositions suivantes :
Crée Code pénal - art. 450-4 (V)

Chapitre II : Dispositions modifiant le code de procédure pénale et concernant la protection des victimes

Article 23
A modifié les dispositions suivantes :
Modifie CODE DE PROCEDURE PENALE - art. 2-2 (M)

Article 24
A modifié les dispositions suivantes :
Modifie CODE DE PROCEDURE PENALE - art. 2-3 (M)

Article 25
A modifié les dispositions suivantes :
Modifie CODE DE PROCEDURE PENALE - art. 7 (M)

Article 26
A modifié les dispositions suivantes :
Modifie CODE DE PROCEDURE PENALE - art. 8 (M)

Article 27
A modifié les dispositions suivantes :
Modifie CODE DE PROCEDURE PENALE - art. 40 (M)

Article 28
A modifié les dispositions suivantes :
Crée CODE DE PROCEDURE PENALE - art. 706-47 (T)
Crée CODE DE PROCEDURE PENALE - art. 706-48 (V)
Crée CODE DE PROCEDURE PENALE - art. 706-49 (V)
Crée CODE DE PROCEDURE PENALE - art. 706-50 (V)
Crée CODE DE PROCEDURE PENALE - art. 706-51 (V)
Crée CODE DE PROCEDURE PENALE - art. 706-52 (M)
Crée CODE DE PROCEDURE PENALE - art. 706-53 (V)
Crée CODE DE PROCEDURE PENALE - art. 706-54 (M)

Article 29
A modifié les dispositions suivantes :
Modifie CODE DE PROCEDURE PENALE - art. 722 (M)

Article 30
A modifié les dispositions suivantes :
Modifie CODE DE PROCEDURE PENALE - art. 722 (M)

Article 31
A modifié les dispositions suivantes :
Modifie Code de la sécurité sociale. - art. L322-3 (M)

Chapitre III : Dispositions relatives à l'interdiction de mise à disposition de certains documents aux mineurs

Article 32
Modifié par Loi n°2007-297 du 5 mars 2007 - art. 35 JORF 7 mars 2007 en vigueur le 7 septembre 2007

Lorsqu'un document fixé par un procédé déchiffrable par voie électronique en mode analogique ou en mode numérique présente un danger pour la jeunesse en raison de son caractère pornographique, le support et chaque unité de son conditionnement doivent comporter de façon visible, lisible et inaltérable la mention "mise à disposition des mineurs interdite (article 227-24 du code pénal)". Cette mention emporte interdiction de proposer, donner, louer ou vendre le produit en cause aux mineurs.
Lorsqu'un document fixé par un procédé identique peut présenter un risque pour la jeunesse en raison de la place faite au crime, à la violence, à l'incitation à l'usage, à la détention ou au trafic de stupéfiants, à l'incitation à la consommation excessive d'alcool ainsi qu'à la discrimination ou à la haine contre une personne déterminée ou un groupe de personnes, le support et chaque unité de son conditionnement doivent faire l'objet d'une signalétique spécifique au regard de ce risque. Cette signalétique, dont les caractéristiques sont fixées par l'autorité administrative, est destinée à en limiter la mise à disposition à certaines catégories de mineurs, en fonction de leur âge.
La mise en oeuvre de l'obligation fixée aux deux alinéas précédents incombe à l'éditeur ou, à défaut, au distributeur chargé de la diffusion en France du document.

Article 33

Modifié par Loi n°2007-297 du 5 mars 2007 - art. 35 JORF 7 mars 2007

L'autorité administrative peut en outre interdire :
1° De proposer, de donner, de louer ou de vendre à des mineurs les documents mentionnés à l'article 32 ;
2° D'exposer les documents mentionnés à l'article 32 à la vue du public en quelque lieu que ce soit. Toutefois, l'exposition demeure possible dans les lieux dont l'accès est interdit aux mineurs ;
3° De faire, en faveur de ces documents, de la publicité par quelque moyen que ce soit. Toutefois, la publicité demeure possible dans les lieux dont l'accès est interdit aux mineurs.

Article 34

Modifié par Loi n°2007-297 du 5 mars 2007 - art. 35 JORF 7 mars 2007

Le fait de ne pas se conformer aux obligations et interdictions fixées au premier alinéa de l'article 32 et à l'article 33 est puni d'un an d'emprisonnement et d'une amende de 15 000 Euros.
Le fait, par des changements de titres ou de supports, par des artifices de présentation ou de publicité ou par tout autre moyen, d'éluder ou de tenter d'éluder l'application du premier alinéa de l'article 32 et de l'article 33 est puni de deux ans d'emprisonnement et d'une amende de 30 000 Euros.
Les personnes physiques coupables des infractions prévues aux deux premiers alinéas encourent également la peine complémentaire de confiscation de la chose qui a servi à commettre l'infraction ou était destinée à la commettre ou de la chose qui en est le produit.
Les personnes morales déclarées pénalement responsables des infractions prévues aux deux premiers alinéas encourent les peines suivantes :
- l'amende, dans les conditions fixées par l'article 131-38 du code pénal ;
- la confiscation prévue par le 8° de l'article 131-39 du même code.

Article 35

Modifié par Ordonnance n°2009-901 du 24 juillet 2009 - art. 2 (V)

Les dispositions du présent chapitre ne s'appliquent pas aux documents qui constituent la reproduction intégrale d'une oeuvre cinématographique ayant obtenu le visa prévu à l'article L. 211-1 du code du cinéma et de l'image animée.
Toutefois, les documents reproduisant des oeuvres cinématographiques auxquelles s'appliquent les articles 11 et 12 de la loi de finances pour 1976 (n° 75-1278 du 30 décembre 1975) sont soumis de plein droit à l'interdiction prévue au premier alinéa de l'article 32 de la présente loi.

Article 36 (abrogé)

Modifié par Ordonnance n°2000-916 du 19 septembre 2000 - art. 3 (V) JORF 22 septembre 2000 en vigueur le 1er janvier 2002
Abrogé par Loi n°2007-297 du 5 mars 2007 - art. 35 JORF 7 mars 2007

Article 37 (abrogé)

Modifié par Ordonnance n°2000-916 du 19 septembre 2000 - art. 3 (V) JORF 22 septembre 2000 en vigueur le 1er janvier 2002
Abrogé par Loi n°2007-297 du 5 mars 2007 - art. 35 JORF 7 mars 2007

Article 38 (abrogé)

Abrogé par Loi n°2007-297 du 5 mars 2007 - art. 35 JORF 7 mars 2007

Article 39 (abrogé)

Abrogé par Loi n°2007-297 du 5 mars 2007 - art. 35 JORF 7 mars 2007

Titre III :

Dispositions diverses et de coordination.

Article 40

A modifié les dispositions suivantes :
Crée CODE DE PROCEDURE PENALE - art. 873-1 (M)

Article 41

A modifié les dispositions suivantes :
Modifie CODE DE PROCEDURE PENALE - art. 736 (V)
Modifie CODE DE PROCEDURE PENALE - art. 746 (V)

Modifie CODE DE PROCEDURE PENALE - art. 775 (M)
Modifie CODE DE PROCEDURE PENALE - art. 777 (V)
Modifie Code pénal - art. 133-16 (AbD)

Article 42
A modifié les dispositions suivantes :
Crée CODE DE PROCEDURE PENALE - art. 902 (M)

Article 43
A modifié les dispositions suivantes :
Modifie Code civil - art. 2270-1 (V)

Article 44
A modifié les dispositions suivantes :
Modifie Loi n°1881-07-29 du 29 juillet 1881 - art. 35 (V)

Article 45
A modifié les dispositions suivantes :
Modifie Ordonnance n°45-174 du 2 février 1945 - art. 20-4 (V)

Article 46
A modifié les dispositions suivantes :
Modifie Code des douanes - art. 38 (M)

Article 47 (abrogé) En savoir plus sur cet article...
Abrogé par Ordonnance 2000-549 2000-06-15 art. 7 JORF 22 juin 2000

Article 48
Les nouvelles dispositions de l'article 706-52 du code de procédure pénale entreront en vigueur au plus tard le 1er juin 1999.

Article 49
L'article 87-1 du code de procédure pénale est abrogé.

Article 50
Les dispositions des articles 7 et 8 du code de procédure pénale, dans leur rédaction résultant des articles 25 et 26 de la présente loi, sont applicables aux infractions non encore prescrites lors de l'entrée en vigueur de la présente loi.

Article 51 (abrogé)
Abrogé par Ordonnance 2000-548 2000-06-15 art. 4 JORF 22 juin 2000

Jacques Chirac
Par le Président de la République :
Le Premier ministre,
Lionel Jospin
La ministre de l'emploi et de la solidarité,
Martine Aubry
Le garde des sceaux, ministre de la justice,
Élisabeth Guigou
Le ministre de l'intérieur,
Jean-Pierre Chevènement
La ministre de la culture et de la communication,
Catherine Trautmann
Le secrétaire d'Etat à la santé,
Bernard Kouchner
Le secrétaire d'Etat à l'outre-mer,
Jean-Jack Queyranne

أنظر صفحة الأنترنت التالية :

http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000556901

ملحق رقم : 17

Cyber guérilla - Hackers, pirates et guerres secrétes
difusé le 10 mars à 20h35 sur la chaine France 5

حرب العصابات المعلوماتية – هاكرز، قراصنة و حروب سرية
تم إيداعه في 10 مارس 2009 على الساعة 20سا و 35د في قناة فرنسة 5

محمول على قرص مضغوط *DVD-Rom*

http://www.france5.fr/et-vous/France-5-et-vous/Les-programmes/Archives/LE-MAG-N-11-2009/articles/p-1966-Cyber-guerilla-Hackers-pirates-et-guerres-secretes.htm

قـــائـــمـــة الـــمـــراجـــع

أولا : المراجع باللغة العربيـــــة

1- النصوص القانونيـــة

- النصوص القانونية و المراسيم الوطنية (الجزائريـــة)

- القانون رقم 04-15 المؤرخ في 27 رمضان 1425 الموافق 10 نوفمبر سنة 2004 الذي أدخل إلى قانون العقوبات قسم سابع مكرر تحت عنوان : "المساس بأنظمة المعالجة الآلية للمعطيات " (المواد من 394 مكرر إلى 394 مكرر 7 ق.ع.جزائري).
- القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق لـــ 5 أوت 2009 المتضمن : "القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها " و الذي دخل حيز النفاذ بموجب الجريدة الرسمية/العدد 47 الصادرة بتاريخ 16 أوت 2009.
- المرسوم الرئاسي رقم 07-375 المؤرخ في 21 ذي القعدة عام 1428 الموافق لـــ 1 ديسمبر 2007 المنشور في الجريدة الرسمية المؤرخة في 9 ديسمبر 2007 / العدد 77، المتعلق بالمصادقة على (إتفاقية دولية ثنائية) بين الجمهورية الجزائرية و بين الحكومة الفرنسية و المتعلقة بـــ : "التعاون في مجال الأمن و مكافحة الإجرام المنظم" الموقع عليها بالجزائر في 25 أكتوبر 2003.

2- الكتـــــب

أ- الكتب العلمية العامـــــة

- أحسن بوسقيعة، " **الوجيز في القانون الجزائي العام** "، (الطبعة الأولى، طبعة 2002)، الديوان الوطني للأشغال التربوية، (الجزائر)
- أحسن بوسقيعة، "**الوجيز في القانون الجنائي الخاص** "، **الجزء الثاني : جرائم الموظفين، جرائم الأعمال، جرائم التزوير**، دار هومه، طبعة 2004، (الجزائر)
- أحسن بوسقيعة، "**الوجيز في القانون الجزائي الخاص** " **(الجزء الأول) الجرائم ضد الأشخاص و الجرائم ضد الأموال** ، دار هومه، (طبعة منقحة و متممة في ضوء قانون 2006/12/20) الطبعة الثامنة 2008، (الجزائر)
- محمد حزيط، "**مذكرات في قانون الإجراءات الجزائية الجزائري**"، دار هومه، الطبعة الثالثة 2008، (الجزائر).

ب- الكتب العلمية المتخصصـــــة

- جميل عبد الباقي الصغير، "**القانون الجنائي و التكنولوجيا الحديثة (الكتاب الأول : الجرائم الناشئة عن إستخدام الحاسب الآلي)** " (الطبعة الأولى)، دار النهضة العربية، ، طبعة 1992، القاهرة (مصر)
- محمد أمين الرومي، "**جرائم الكمبيوتر و الأنترنت** "، دار المطبوعات الجامعية، طبعة 2004، الإسكندرية (مصر)
- محمد سامي الشوا، "**ثورة المعلومات و إنعكاساتها على قانون العقوبات**"، دار النهضة العربية، سنة 1993، القاهرة (مصر)
- هدى حامد قشقوش، "**جرائم الحاسب الإلكتروني في التشريع المقارن** "، (الطبعة الأولى)، دار النهضة العربية، 1992، القاهرة (مصر)
- هشام محمد فريد رستم، "**قانون العقوبات و مخاطر تقنية المعلومات** "، مكتبة الآلات الحديثة، 1994، باسيوط (مصر)

3- المقالات العلميـــــة

- طاشور عبد الحفيظ، "**شبكة الأنترنت، الرهانات التكنولوجية و الإشكالات القانونية**"، أعمال المؤتمر التاسع للإتحاد العربي للمكتبات و المعلومات، دمشق أيام 21 إلى 26 أكتوبر 1998، تونس، المنظمة العربية للتربية و الثقافة و العلوم و الإتحاد العربي للمكتبات و المعلومات 1999، من الصفحة 251 إلى 258.

4- المذكرات و الرسائل الجامعيـــــة

- المومني أنيس، ماجستير شعبة : القانون الجنائي، "**قانون العقوبات في مواجهة مخاطر الأنترنت** " تحت إشراف الأستاذ الدكتور بوكحيل لخضر ، جامعة باجي مختار (عنابة) – كلية حقوق، سنة 2004.

5- مواقع الأنترنت باللغة العربيـــــة

- **المركز الوطني للتوثيق : قاعدة المعطيات حول التنمية الاقتصادية والاجتماعية – المركز المتعدد الوسائط : www.doc.abhatoo.net.ma/**

يتضمن :

- المستند **(WORD)** (يونس عرب، تحت عنوان : **جرائم الكمبيوتر والانترنت المعنى والخصائص والصور و إستراتيجية المواجهة القانونية**، أكتوبر 2006، **المركز الوطني للتوثيق: قاعدة المعطيات حول التنمية الاقتصادية والاجتماعية – المركز المتعدد الوسائط)** المستنسخ **Téléchargé** من صفحة الأنترنت التالية :

www.doc.abhatoo.net.ma/IMG/doc/dro5.doc (de la page 1 à 6 du document)

- المستند **(WORD)**، (إعداد : يونس عربي، تحت عنوان : **جرائم الكمبيوتر والانترنت – إيجاز في المفهوم و النطاق و الخصائص و الصور و القواعد و القواعد الإجرائية للملاحقة و الإثبات)** المستنسخ **Téléchargé** من صفحة الأنترنت التالية :

www.doc.abhatoo.net.ma/IMG/doc/dro35.doc (page 3 du document)

- **موقع الأنترنت للجريدة الرسمية للجمهورية الجزائرية في العنوان التالي :**

http://www.joradp.dz/

ثانيا – المراجع الأجنبيـــــة

1– النصوص القانونيـــة

أ– النصوص القانونية و المراسيم الأجنبية (الفرنسيـــة)

- القانون رقم 88–19 لـــ 5 جانفي 1988 الصادر بالجريدة الرسمية لـــ 6 جانفي 1988 المتعلق بالغش المعلوماتي، الفصل الثالث من قانون العقوبات الفرنسي تحت عنوان : ببعض الجرائم في مجال المعلوماتية (المواد من 462–2 إلى 462–9 ق.ع.فرنسي).
- القانون رقم 88–19 لـــ 5 جانفي 1988 المتعلق بـــ : "الجرائم ضد أنظمة المعالجة الآلية للمعطيات" المعدل و الذي أدخل في قانون العقوبات في 1 جانفي 1994 ، المواد من 323–1 إلى 323–7 ق.ع.فرنسي.
- القانون رقم 2004–575 لـــ 21 جوان 2004 تحت عنوان : "الثقة في الإقتصاد المعلوماتي "، الفصل الثاني تحت عنوان : "المكافحة ضد الإجرام المعلوماتي " من الباب الثالث تحت عنوان : "الأمن في الإقتصاد المعلوماتي" (المواد من 41 إلى 46).
- القانون رقم 88–19 لـــ 5 جانفي 1988 المتعلق بـــ : "الجرائم ضد أنظمة المعالجة الآلية للمعطيات" المعدل بموجب القانون رقم 2004–575 لـــ 21 جوان 2004 تحت عنوان : "الثقة في

الإقتصاد المعلوماتي"، (المواد من 323-1 إلى 323-7 ق.ع.فرنسي، مع إضافة المادة 323-3-1 ق.ع.فرنسي).

- القانون رقم 78-17 المؤرخ في 6 جانفي 1978 و المتعلق بالمعلوماتية، المعطيات و الحريات المعدل بموجب القانون رقم 2009-526 المؤرخ في 12 ماي 2009 (الجريدة الرسمية لـــ 13 ماي 2009).
- القانون المؤرخ في 29 جويلية 1881 حول : "حرية الصحافة"، الفصل الرابع : "الجنايات و الجنح المرتكبة بواسطة الصحافة أو أي وسيلة أخرى للنشر" و الفصل الخامس : "عن المتابعات و القمع" (مدعمة بآخر التعديلات في 7 أوت 2009 و السارية المفعول في 18 أكتوبر 2009).

ب- النصوص القانونية الدولية (إتفاقيات و معاهـــدات)

- الإعلان العالمي لحقوق الإنسان ***La déclaration universelle des droits de l'homme*** لـــ 10 ديسمبر 1948.
- إتفاقية بيداباست ***"La convention de Budapest"*** حول "الإجرام المعلوماتي " ***« La cyber criminalité »*** المصادق عليها أمام المجلس الأوربي في بداباست في 23 نوفمبر 2001.
- الإتفاقية الأورومتوسطية ***"Accord euro-méditerranéen"*** (إتفاقية دولية متعددة الأطراف ***"Convention internationale multilatérale"***) المؤرخة في 22 أفريل 2002 و التي تهدف إلى ربط الجهود بين الوحدة الأوروبية و الدول الأعضاء فيها من جهة و الحكومة الجزائرية من جهة أخرى في ميادين مختلفة، و منها ما ورد في الفصل الثامن ***(Titre VIII)*** تحت عنوان : "التعاون في مجال القضاء و الشؤون الداخلية " ***« Coopération dans le domaine de la justice et des affaires intérieurs ».***

2- الإجتهادات القضائيـــــة :

- الجهات القضائية الفرنسيـــــة :

- ***Arrêt de la cour suprême française chambre pénale du 8 janvier 1979 (Affaire LOGABAX)***
- ***Jugement du tribunal de Rennes section pénale du 8 septembre 1988***
- ***Arrêt de cour suprême Française chambre pénale du 29 avril 1986 (Affaire HERBERTEAU)***
- ***Arrêt de cour suprême Française chambre pénale du 12 janvier 1989 (Affaire BOURQUIN)***
- ***Arrêt de cour suprême Française chambre pénale du 1 mars 1989 (Affaire ANTONIOLLI)***
- ***Arret de la cour d'Aix en Provence de l'année 1993***
- ***Jugement du tribunal de grande instances de Paris section pénale du 16 septembre 1994***
- ***Arrêt de la cour de Caen section pénale du 8 septembre 1999***

- ***Cass. Crim., 23 février 2000, Bull. crim. n° 85***
- ***Jugement du tribunal de grandes instances de Paris Section pénale du 2 novembre 2000***
- ***Arrêt de la cour suprême Française chambre pénale du 23 février 2000***
- ***Ordonnance du tribunal de grandes instances de Paris du 31 juillet 2000***
- ***Jugement du tribnal de Paris du 25 février 2000***
- ***Arrêt de cour suprême Française chambre pénale du 14 novembre 2000***
- ***Arrêt de la cour de justice de Paris chambre pénale du 2 avril 2002***
- ***Arrêt de cour suprême Française chambre pénale du 22 septembre 2004***

- الجهات القضائية الألمانيـــــة :

- ***Jugement du tribunal de Neuss (Allemagne) section pénale du 19 août 2002***

3- الكتـــــب

- الكتب العلمية المتخصصـــــة

- André Lucas, Jean Devrèze, Jean Frayssinet, ***Droit de l'informatique et de l'Internet***, édition Dalloz, collection Thémis (Droit Privé), Novembre 2001(France).
- Bensoussan Alain (sous la direction de), ***Internet : aspect juridique***, édition Hermès, juin 1996, (France)
- Etienne WERY, ***« Sexe en ligne : aspects juridiques et protection des mineurs »***, édition LARCIER (Droit des technologies), 2004 (France)
- Féral-schuhl Christiane, ***Cyber Droit (le droit à l'épreuve de l'Internet)***, édition Dalloz (2e édition), septembre 2000 (France).
- Frédérique-Jérome Pansier & Emmanuel Jez, ***La Criminalité sur Internet***, édition Que sais-je ? (P.U.F) 2ème édition mise à jour, Septembre 2001 (France).
- Hollande Alain, De Bellefonds Linant Xavier, ***Pratique du droit de l'informatique***, édition Delmas (5e édition), Avril 2002, (France).
- Michel Vivant (sous la direction), Christian Le Stanc, Lucien Rapp, Michel Guibal (avec leurs collaboration), Lionel Costes (secrétaire général de la rédaction), ***Lamy - Droit de l'Informatique / Informatique, Télématique, Réseaux***, édition Lamy S.A., France, édition 1991, (France)
- Pansier Frédéric-Jérôme, Jez Emmanuel, ***Initiation à l'Internet juridique***, édition Litec (2e édition), 1er trimestre 2000, (France)
- X. Linant de Bellefonds, A. Hollande, ***Droit de l'Informatique et de la Télématique***, Encyclopédie Delmas pour la vie des affaires, édition J. Delmas et Cie, 2ème édition, 01 décembre 1997, (France).

4- المذكرات و الرسائل الجامعيـــــة

- Eric TAVENARD, mémoire de (DESS) droit du multimédia et de l'informatique, ***La pornographie sur Internet***, sous la direction du : professeur Jérôme HUET, université Paris II – Panthéon Assas, année 2002-2003 (France).
- Laureen KRAFTCHIK, mémoire de master de recherche mention : droit pénal, ***Les appropriations frauduleuses et le recel de biens incorporels,*** sous la direction du : Professeur Alain DEKEUWER, Lille 2 (Université de droit et de la santé),
  Faculté des Sciences juridiques, Politiques et Sociales, année 2004-2005 (France).
- Sophie REVOL, mémoire de (DESS) droit du multimédia et de l'informatique, ***Terroristes et Internet***, sous la direction de M. KOSTIC, université Paris II – Panthéon Assas, année 2002-2003 (France).

5- مواقع الأنترنت باللغة الفرنسيـــــة

- **http://www.net-iris.com/**

المتضمـــن :

صفحة الأنترنت (مقال من **أليكس بسكال** ***Pascal Alix*** تحت عنوان : ***L'accès ou le maintien non autorisé dans un système informatique***، **www.net-iris.fr**، 23 نوفمبر 2004) في العنوان التالي :

http://www.net-iris.com/publication/author/document.php3?document=342

- **http://solutions.journaldunet.com**

يتضمـــن :

صفحة الأنترنت (مقال تحت عنوان : ***Comprendre les virus informatiques***، 28 / 05 / 2005) في العنوان التالي : **http://solutions.journaldunet.com/dossiers/pratique/virus.shtml**

صفحة الأنترنت في العنوان التالي (مقال إعداد : تحت عنوان : ***Les virus sasser netsky décapités par l'arrestation de leur auteur***، 11 / 05 / 2004) :

http://solutions.journaldunet.com/0405/040511_sasser.shtml

- **موقع الأنترنت الجزائري الأول في مجال الحماية المعلوماتية** في العنوان التالي :

www.wikayanet.dz

يتضمـــن :

أنظر صفحة الأنترنت (مقال تحت عنوان : ***Les virus***) في العنوان التالي :

http://www.wikayanet.dz/modules.php?name=Virus

- **http://www.lex-electronica.org/**

يتضمـــن :

مستند (PDF) تحت عنوان : « ***Espionnage économique et droit : l'inutile création d'un bien informationnel*** » المستنسخ **Téléchargé** من صفحة الأنترنت التالية :

http://www.lex-electronica.org/articles/v7-1/Dupre.pdf (de la Page 4 à 8 du document)

- **http://www.njuris.com/**

يتضمـــن :

صفحة الأنترنت التالية (مقال تحت عنوان : ***2 : 700 internautes victimes d'abus de confiance français interpellés***، من ***Michel robert***، **http://www.njuris.com/**، 07 / 10 / 2005) :

http://www.njuris.com/ShowBreve.aspx?IDBreve=704

- **موقع الأنترنت : لإتحادية المعلوماتية و الأنترنت** ***Fédération informatique & liberté*** **:**

http://www.vie-privee.org/

يتضمـــن :

صفحة الأنترنت التالية (مقال إعداد : **جريدة يومية فرنسية** ***le Monde***، تحت عنوان : ***Il faut sauver la loi informatique et libertés***، 14 أوت 2004، **موقع النشر : لإتحادية المعلوماتية و الأنترنت** ***Fédération informatique & liberté*** **) :** **http://www.vie-privee.org/news302**

- **موقع الأنترنت الفرنسي الذي يظم كل الجرائد الرسمية و قوانين الجمهورية الفرنسية :**

http://www.legifrance.gouv.fr/home.jsp

6 – المؤتمرات الدوليـــــة

- المؤتمر الحادي عشر للأمم المتحدة ***(O.N.U)*** حول "الوقاية من الجريمة و العدالة الجنائية ***La prévention du crime et la justice pénale***" أيام 18 إلى 25 أفريل 2005 ببنكوك (تايلاند) من خلال :
  - وثيقة معلومات رقم 6 تحت عنوان : "الإجرام المعلوماتي ***Délinquance informatique***"
  - التقرير الصحافي حول أعمال اللجنة الثانية في الجلسة التاسعة مساءا يوم 22 أفريل 2005 من المؤتمر الحادية عشر للأمم المتحدة "للوقاية من الإجرام و العدالة الجنائية" لدراسة وسائل إستدراك عجز الأنظمة القانونية في مواجهة الإجرام المعلوماتي.

7 – الأشرطة العلمية السمعية بصرية الأجنبيـــــة (فرنسية)

- **برنامج مبعوث خاص *Envoyé Special* في قناة التلفزية *France 2* ليوم : الخميس 7 ماي 2010**
  تحت عنوان : المجرمين المعلوماتيين *Les Cybercriminels*، إعداد كال من : ان ريشارد، جيروم بافلوفسكي و ستيفان روسي ***Un reportage de Anne Richard, Jérôme Pavlovsky et Stéphane Ross***.

- **برنامج في القناة الفرنسية الخامسة :**

Cyber guérilla - Hackers, pirates et guerres secrètes difusé le 10 mars 2009 a 20h35. Une exclusivité France 5 (Réalisation : Jean-Martial LEFRANC – Production : France 5 & GEDEON Programmes) redifusé sur la chaine française : ARTE.

مقدمـــــــــة

الفصل الأول : جرائم المعلوماتية ضد الأموال ذو طبيعة إلكترونيـــــة

الفصل الثاني : جرائم المعلوماتية الماسة بالأشخاص و الحريـــــات