العنوان:	الحماية الجنائية للمعطيات في المجال المعلوماتي
المصدر:	المجلة المغربية للقانون الجنائي والعلوم الجنائية
الناشر:	مركز الدراسات والبحوث الإنسانية والاجتماعية
المؤلف الرئيسي:	عبدالمجيد، كوزى
المجلد/العدد:	ع3
محكمة:	نعم
التاريخ الميلادي:	2016
الصفحات:	109 - 124
رقم MD:	815718
نوع المحتوى:	بحوث ومقالات
اللغة:	Arabic
قواعد المعلومات:	IslamicInfo
مواضيع:	القوانين والتشريعات، النظم المعلوماتية، شبكة الانترنت، الحماية الجنائية، المعاملات الالكترونية، المغرب
رابط:	http://search.mandumah.com/Record/815718

الحماية الجنائية للمعطيات في المجال المعلوماتي

الدكتور عبد المجيد كوزي

دكتوراه في الحقوق

تمهيد :

اتسم عصر الألفية الثالثة بالتغيرات الجذرية في مختلف مناحي الحياة، وأصبحت التكنولوجيا في المجال المعلوماتي طاغية على مختلف أوجه حياتنا اليومية، واكتسح التعامل الإلكتروني جميع المجالات الاقتصادية منها والاجتماعية والثقافية، وتعددت الاستعمالات خاصة في مجال التجارة الإلكترونية التي تعتمد على أساسا على الوثائق الإلكترونية في مختلف أشكالها كوسيلة للتعامل، وأيضا تلك التي تشمل المعطيات الشخصية أو ما يعبر عنه بالخصوصية المعلوماتية.

وقد لعبت وسائل الاتصال الحديثة من خلال الشبكة العالمية للمعلومات (الانترنت)، دورا كبيرا فتح الباب لثورة معلوماتية متعددة الأبعاد والوسائط، إذ يطرح موضوع الحماية الجنائية للمعطيات الشخصية بالمغرب كما في باقي دول المعمور تحديات عديدة، تشريعية وهيكلية ومؤسساتية، ضمنها تحدي صعوبة الحماية الجنائية في المجال المعلوماتي خاصة على مستوى التوفيق والموازنة بين مسايرة التقدم التكنولوجي الجديد في ظل الزمن المعولم وحماية المعطيات ذات الطابع الشخصي.

وقد عمل المشرع الجنائي على الإحاطة بمختلف الاعتداءات التي يمكن أن تطال الوثيقة الإلكترونية من خلال الاعتداء على نظم معالجتها أو بالتلاعب ببياناتها وتغيير مضمونها وهو ما يشكل نمطا جديدا للتدليس، يعرف بالتدليس الإلكتروني، فما هي المقاربة التي أقرها المشرع الدولي والوطني لمعالجة صور الاعتداء على نظم المعالجة في المجال المعلوماتي ؟ وما هي سبل الحماية الجنائية المقرر في هذا الشأن من خلال القانون المؤطر لحماية المعطيات ذات الطابع الشخصي 08-09 ؟.

المحور الأول: صور الاعتداء على نظم المعالجة وسبل الحماية في التشريع المغربي والمقارن

حرص المشرع الجنائي بموجب القانون رقم 03-07 بشأن تتميم مجموعة القانون الجنائي فيما يتعلق بالإخلال بسير نظم المعالجة الآلية للمعطيات مضمنة في تسعة فصول (من الفصل 3-607 إلى الفصل 11-607 من مجموعة القانون الجنائي المغربي)[1]، كما تضمن القانون 08-09 مجموعة من الأحكام ذات الطابع الزجري، وهي في اعتقادنا خطوة هامة في اتجاه مواكبة المشرع المغربي للجريمة المعلوماتية، وتوفير الحماية الجنائية للوثيقة الالكترونية وللمعطيات ذات الطابع الشخصي، خاصة أن الأحكام الجنائية التقليدية تبدو قاصرة عن توفير هذه الحماية.

كما أضاف المشرع المغربي بموجب القانون 03-07، والذي جرم بموجبه أنماط الاعتداء على نظم المعالجة الآلية للبيانات الإلكترونية، تمييزا من خلال أحكام هذا الفصل بين الجرائم المتعلقة بالاعتداء على نظام المعالجة المعلوماتية وبين صور التجريم للاعتداء المسلط على البيانات الموجودة بالنظام (الفقرة الأولى) وتجليات الحماية المقررة في القانون الجنائي المغربي (الفقرة الثانية).

الفقرة الأولى: الاعتداءات على نظام المعالجة المعلوماتية

تتعدد أشكال الاعتداء على نظم المعالجة المعلوماتية وتختلف من حيث خطورتها من خلال طبيعتها التقنية والقانونية، ولعل صعوبة إيجاد تعريف موحد يزيد من صعوبتها رغم الجهود الدولية في هذا الإطار، حيث أكد بعض الفقه[2] كون هذا النوع من الجرائم الماسة بالنظم المعلوماتية يقاوم التعريف.

ويمكن التمييز بين مجرد الولوج، أو البقاء بنظام المعالجة المعلوماتية (أولا) وبين تدمير أو إفساد سير نظام المعالجة (ثانيا).

أولا: البقاء بصفة غير شرعية بنظام المعالجة المعلوماتية:

اعتبر المشرع المغربي أن مجرد الولوج، أو البقاء بنظام معالجة معلوماتية، يعد جريمة متى كان ذلك بصفة غير شرعية، ولو اختلفت الجريمتان، من حيث الأفعال المادية المكونة لكل واحدة منها، فإنها تشترك من حيث المحل الذي تتسلط عليه، وهو نظام المعالجة الآلية للبيانات.

1. أصبح هذا القانون يشكل الباب العاشر من الجزء الأول من الكتاب الثالث من القانون الجنائي المغربي تحت عنوان: المس بنظم المعالجة الآلية للمعطيات. وقد صدر بتنفيذه الظهير الشريف رقم 197-03-1 بتاريخ 16 رمضان 1424 الموافق ل11 نونبر 2003.
2. محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات مكتبة الآلات الحديثة، القاهرة 1992، ص: 25.

أما المشرع الفرنسي من جانبه حين أصدر القانون المعروف بقانون Godfrain [3] نسبة إلى مقترحه وهو النائب «Jacques Godfrain»، تخلى عن تحديد مفهوم نظام المعالجة الآلية للبيانات، على الرغم أن مجلس النواب كان قد اقترح ضمن التعديلات التي أدخلها على مشروع هذا القانون تعريفا لنظام المعالجة الآلية للبيانات، ورد فيه أن «مجموعة متكونة من وحدات المعالجة ومن الذاكرة وطرق المعالجة والبيانات، ووحدات الإدخال والإخراج والربط بشرط أن تكون محمية بواسطة آلية لضمان السلامة».

كما عرفه القرار الوزاري الفرنسي الصادر في 22 ديسمبر 1981 المتعلق بإثراء مصطلحات الإعلامية –نظام البرامج المعلوماتية –بأنه «مجموع البرامج والوسائل والقواعد وكذلك الوثائق المتعلقة بها للوصول لمعالجة مجموعة بيانات».

وقد اشتمل التعريف المقترح من مجلس النواب، شرط خضوع النظام للحماية التقنية، غير أن المشرع الفرنسي لم يشر إلى هذا المعطى عند صدور القانون، في صيغته النهائية، ولم يقصر توفر جريمة الاعتداء على نظام المعالجة الآلية على شرط الحماية التقنية لهذا النظام، وهو نفس موقف المشرع المغربي، الذي لم يورد شرط الحماية التقنية لنظام المعالجة الآلية لقيام الجريمة.

إلا أن هناك جانبا من الفقه[4]، يرى ضرورة وجود نظام أمني، لقيام الجريمة خاصة وأن توفر هذه الحماية الفنية، والدخول بالرغم من ذلك إلى نظام المعالجة الآلية، من شأنه أن يكون دليلا قاطعا، على توفر ركن العمد لدى الجاني، الذي لا يمكن أن يكون دخوله لهذا النظام صدفة بعد أن يكون قد استعمل طرق تقنية معقدة لخرق هذه الحماية.

غير أن هذا الاتجاه لم يجد له عديد الأنصار، وهو ما يتضح من عدم اشتراط شرط الحماية الفنية، في مختلف النصوص المتعلقة بتجريم الاعتداء على النظم المعلوماتية سواء في فرنسا أو في المغرب، وقد تدعم ذلك بموقف فقه القضاء الفرنسي في هذا الشأن، من خلال القرار الإستئنافي الصادر عن محكمة باريس في 5 أبريل 1994 الذي جاء به أنه «لا يشترط لقيام الجريمة وجود

3. La loi française-Godfrain- N88 du 5-1-1988 concernant la fraude informatique : La loi française est extrêmement claire mais mérite malgré tout de définir certains concepts: la loi du 5 janvier 1988, dite la loi Godfrain, à mise en place le délit d'accès frauduleux à un Système de Traitement Automatisé de Données. Cette notion a été introduite dans le code pénal français par le biais de la loi Godfrain du 5 janvier 1988.
https://sites.google.com/site/cyberhamid2/loi-godfrain-etat-de-la-jurisprudence-francaise, consulté le 10-5-2015

4. عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الالكترونية : الكتاب الثاني، الحماية الجنائية للتجارة الالكترونية، دار الفكر الجامعي الإسكندرية 2002، ص: 24.

وسائل حماية لنظام المعالجة المعلوماتية»[5]، ولا يشترط لقيام جريمة البقاء أو الولوج وقوع اختراق نظام حماية ما، يكفي أن يكون الولوج أو البقاء غير مشروع.

ويتحقق الدخول غير المشروع، متى كان ذلك مخالفا لإرادة صاحب النظام أو من له حق السيطرة عليه ومن ذلك الأنظمة المتعلقة بأسرار الدولة، أو التي تتضمن بيانات شخصية تتعلق بحرمة الحياة الخاصة ولا يجوز الإطلاع عليها[6]، وكذلك كلما كان نظام البرمجيات غير مفتوح أو موجه للعموم والإطلاع عليه مقتصر على أشخاص معينين دون غيرهم.

وقد استعمل المشرع المغربي في صلب هذا الفصل 3-607 من القانون الجنائي عبارة الدخول عوضا عن عبارة النفاذ، ليؤكد الخاصية المادية لهذه الجريمة، فعبارة النفاذ قد يكون لها مدلول معنوي، بحيث يشبه من هذه الناحية النفاذ إلى النظام بالدخول في ذاكرة الإنسان[7]، بحيث كان على المشرع المغربي استعمال عبارة النفاذ لكونها أكثر شمولية في نظرنا من الدخول، غير أن هناك من يرى أن النفاذ، له مدلول معنوي، ومدلول مادي يتمثل في أن الشخص قد يكون حاول الدخول أو دخل بالفعل إلى النظام المعلوماتي، ويمكن أن يكون ذلك من خلال عمليات مادية تنفذ على النظام المعلوماتي[8].

فالدخول يتحقق إذا كلما قام شخص بالولوج بنظام المعالجة الآلية للمعلومات باستعمال مختلف الوسائل ولم يحدد المشرع المغربي وسائل الدخول، ويمكن أن يحصل ذلك بطرق متعددة، من ذلك استعمال كلمة السر الحقيقية، متى كان الجاني غير مخول له في استخدامها أو استخدام برنامج أو شفرة خاص[9]، أو الدخول من خلال شخص غير مسموح له بالدخول، أو عن طريق تجاوز النظام الحماية التقنية.

وقد جرم المشرع المغربي مجرد الدخول إلى نظام المعالجة المعلوماتية، حتى إن لم يترتب عن ذلك أي ضرر، أو عن طريق الخطأ، لذا يطرح تساؤل هنا إذا كان مجرد قراءة شاشة الحاسوب يعد دخولا معاقب عليه قانونا؟

---

5. CA Paris, 5 Avril 1994, petite Affiche 1995, n° 80, P. 13. note Alvarez « qu'il n'est pas nécessaire pour que l'infraction existe que l'accès soit limité par un dispositif de protection ».

6. عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الالكترونية، مرجع سابق، ص: 29.

7. Gassin H « la protection pénale d'une nouvelle universalité de fait en droit français » : le système de traitement automatisé des données, Dalloz 1989, 4ème cahier, p. 17.

8. Deveze (J) Atteinte au système automatisé des données, Jurisclasseur pénal 1997 PE3/294.

9. عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الالكترونية، المرجع السابق، ص: 29.

الرأي الغالب كان بالنفي متى لم يصدر عن الشخص نشاط إيجابي للدخول للنظام، أو محاولة الدخول لنظام ممنوع عليه الاتصال به، فلا تتوافر الجريمة إذا اقتصر دور الشخص على مجرد قراءة الشاشة ولا تقوم بهذه الأفعال جريمة الدخول غير المشروع للنظام [10].

ويتحقق فعل النفاذ سواء كان ذلك للنظام كله أو لجزء منه بصريح أحكام القانون الجنائي فيكفي إذا لقيام الجريمة، الدخول إلى بعض عناصر النظام أو إلى عنصر واحد منه، وقد تتحقق الجريمة أيضا إذا كان الجاني مسموح له باستعمال جزء من النظام فقط فيتجاوزه لاستعمال جزء آخر غير مسموح له بالنفاذ إليه، وقد استعمل المشرع عبارة عن طريق الاحتيال كشرط من شروط قيام جريمة الدخول و البقاء وهو ما يجعل هذه الجرائم من الجرائم العمد، أي اتجاه نية الفاعل إلى الدخول لنظام البيانات المعلوماتية مع علمه أن هذا الفعل ممنوع عليه، بذلك متى كان الدخول حصل نتيجة خطأ أو عدم تنبه أو قلة يقظة فيمكن اعتبار الجريمة غير متوفرة لانعدام الركن المادي، على أنه إذا ترتب عن الدخول غير العمدي البقاء والاستقرار بالنظام المعلوماتي فإنه تقوم جريمة أخرى تتمثل في جريمة البقاء.

يقصد بالبقاء التواجد بالنظام المعلوماتي بصفة غير مشروعة، وتبرز أهمية تجريم فعل البقاء في صورة ما إذا كان الدخول إلى نظام المعالجة المعلوماتية بطريق الصدفة وانعدام ركن العمد، فإذا ما انتفت جريمة الدخول لعدم توفر الركن المعنوي تقوم جريمة البقاء باستقرار الجاني بنظام المعالجة الآلية للبيانات، ويطرح التساؤل إن كان المقصود بالبقاء المرحلة التي تلي مباشرة الدخول أو أن هناك مؤشرات أخرى لتوفر جريمة البقاء؟

يبدو أن اعتبار أن البقاء هو المرحلة التي تلي مباشرة الدخول، قد يكون فيه إجحاف بمن ينفذ بصفة عفوية بالنظام المعلوماتي، لذلك يستوجب البقاء بالنظام مدة تتجاوز المدة المسموح بها للخروج منه بعد أن يكون الجاني قد تفطن وتنبه لدخوله غير المشروع.

إلا أن البقاء بنظام المعالجة المعلوماتية قد لا يكون بالضرورة نتيجة دخول غير شرعي، فقد يكون شخص معين له الحق في دخول النظام، إلا أنه يتجاوز المدة المحددة له للبقاء فيه، أو يقوم بنسخ المعلومات في حين أنه مرخص له بالإطلاع عليها فقط، وتجدر الإشارة إلى أنه، إذا كان البقاء لاحقا للدخول غير المشروع للنظام المعلوماتي، وذلك باعتبار أن فعل الدخول يختلف عن البقاء، إلا أن المقصد منهما واحد وهو الولوج إلى نظام المعالجة المعلوماتية والإطلاع على محتوياته.

10. عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الالكترونية، مرجع السابق، ص: 30.

ونلاحظ أن المشرع المغربي قد جرم مجرد الدخول أو البقاء بنظام المعالجة المعلوماتية، وحدد شرط الاحتيال حتى وإن لم يترتب أي ضرر للغير، فنحن إذن أمام جرائم شكلية غير متوقفة على حصول نتيجة منها، وعدم حصول ضرر عن الدخول أو البقاء غير الشرعي، قد يفسر نوعا ما العقاب المخفف الذي أقره المشرع المغربي وذلك بالمقارنة مع ما أقره المشرع من عقاب في صورة إفساد أو تدمير سير نظام المعالجة المعلوماتية، وقد عاقب المشرع المغربي مرتكب هذا النوع من الجرائم طبقا لمقتضيات الفقرة الأولى من الفصل 3-607 بعقوبة سالبة للحرية من شهر إلى ثلاثة أشهر وبغرامة مالية من 2000 إلى 10000 درهم أو بإحدى العقوبتين.

أما جريمة البقاء في داخل النظام المعلوماتي أو في جزء منه، إذا تم عن طريق الخطأ وبدون موجب حق، فقد حددت الفقرة الثانية من نفس الفصل نفس العقوبة المقررة في الفصل السابق.

كما اقتضى الفصل 3-607 في فقرته الثالثة، مضاعفة العقوبة المقررة إذا نتج عن فعل الدخول أو البقاء حذف، أو تغيير للمعطيات المدرجة في نظام المعالجة الآلية للمعطيات أو اضطراب في سيره، ومن ثم، فإن المشرع المغربي سار على نفس منهج المشرع الفرنسي بخصوص مضاعفة عقوبة الدخول أو البقاء داخل النظام، إذا اقترن ذلك بظرف مشدد، قد يتجلى في حذف أو تغيير المعطيات الموجودة داخل أي نظام للمعالجة الآلية للمعطيات[11].

فنظام المعالجة الآلية للمعطيات، أصبح محلا لارتكاب الجرائم والتأثير، من خلال الاعتداءات عليها وإلحاق أضرار وخسائر بالغة[12]، ونسجل في هذا الصدد حجم ما تعرضت له الشركات الأمريكية من خسائر، وفق الإحصائيات الواردة في مجال سرقة المعلومات بنسبة تصل لخمسة وثمانين في المائة كما تعرضت الأجهزة المعلوماتية لمؤسسة البانتغون الأمريكي لاعتداءات على نظمها المعلوماتية، مما قد يتسبب في زعزعة الاقتصاد بأكمله في أي بلد من البلدان[13].

المشرع الفرنسي من جهته، أقر بموجب قانون «Godfrain»عقوبة بالسجن من 3 أشهر إلى 3 سنوات وبغرامة من عشرة آلاف فرنك إلى مائة ألف فرنك، أو بإحدى العقوبتين عند إعاقة أو إفساد سير نظام المعالجة الآلية للبيانات[14]، إلا أنه بعد تعديل القانون الجنائي الفرنسية في أكثر من

11. أمين أعزان، مواجهة الجريمة الإلكترونية في ضوء القانون الجنائي المغربي، مجلة الحقوق المغربية، العدد 12 السنة السادسة 2011.
12. صفاء الصابوني، جرائم المس بنظم المعالجة الآلية للمعطيات، أطروحة لنيل شهادة الدكتوراه في الحقوق، شعبى القانون الخاص، مختبر الدراسات القانونية والاجتماعية، تخصص القانون الجنائي والعلوم الجنائية، كلية العلوم القانونية والاجتماعية والاقتصادية، جامعة محمد الأول وجدة ص:16، السنة الجامعية 2013-2014.
13. Roland L.Dick : «La criminalité informatique capable selon son nouveau de déstabiliser l'économie entière d'un pays» 5ème Forum international sur la cybercriminalité, 22 Mars , 2007, Grand palais de Lille.
14. Art 462.3 : « Qui conque 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 10.000 F à 100.000 F ou de l'une de ces deux peines ».

مناسبة، آخرها التعديل بموجب القانون 575- 2004 المؤرخ في 21 يونيو 2004 أصبحت بمقتضاه العقوبة المقررة هي خمسة سنوات سجن وغرامة تقدر بـ 75.000 أورو[15].

والملاحظ أن المشرع الفرنسي، قد شدد في العقوبة المقررة بالنسبة لجرائم إفساد وإعاقة سير نظام المعالجة المعلوماتية، ويعكس ذلك إيمانه بالخطورة الكبرى التي تمثله مثل هذه الأفعال التي يمكن أن تترتب عنها أضرار مادية جسيمة، بحكم استعمال الأنظمة المعلوماتية في مختلف الأنشطة الحيوية المحتوية على بيانات ومعلومات في غاية من الأهمية، بحيث أن إفساد نظم معالجتها، قد تترتب عنها خسائر فادحة، يصعب في غالب الأحيان تداركها بسهولة.

يقتضى بذلك قيام الجريمة المذكورة أن يترتب عن السلوك الإجرامي إما إفساد أو تدمير النظام المعلوماتي، واستعمال المشرع الفرنسي للدلالة على هذه الجريمة عبارتي الإعاقة بالفصل 323 (فقرة ثانية) من القانون الجنائي الفرنسي، ورغم استعمال المشرع المغربي عبارتي الإفساد والتدمير وإقرار نفس العقوبة فإن الاختلاف قائم بينهما كالتالي:

1 - الإفساد:

يقصد بالإفساد إحداث عطب أو خلل بالشيء، بما يجعله لا يقوم بعمله بصورة طبيعية، وقد يكون ذلك بالحد من سرعة النظام المعلوماتي، وجعله بطيئا، أو يعطي نتائج غير تلك التي من الواجب الحصول عليها، والوسائل المعتمدة في ذلك متعددة، كاستخدام القنبلة المعلوماتية التي تتفرع بدورها إلى نوعين:

القنبلة المنطقية والقنبلة الموقوتة، واللذان من خلالهما يقع تسريب برنامج يحتوي على تعليمات لإفساد سير النظام في وقت وتاريخ معين أو في صورة وقوع حدث معينين.

كما يمكن أن يترتب الإفساد عن استعمال تقنية «الإغراق» «Spamming» وهو أسلوب عادة ما يرتكب عبر الشبكات المفتوحة، وذلك بأن يقع الإيهام إلكترونيا بوقوع الارتباط من قبل آلاف المستعملين، بحيث أن الموقع لا يمكنه مجاراة الكم الهائل من طلبات الارتباط فيتوقف سير النظام، وهو ما حدث مثلا لمحرك البحث Yahoo والنظام المعلوماتي لقناة إعلامية كبرى CNN اللذان عرقل سيرهما مدة يومين، كما يمكن أن يكون الإغراق بإرسال كم هائل من الرسائل الإلكترونية إلى أن يعجز النظام عن مجاراة هذا التدفق للرسائل.

15. Art 323.2 : « Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé des données et puni de cinq ans d'emprisonnement et de 75.000 Euros d'amende, code pénal partie législative, par Sébastien Fontaine sur www.authsecu.com.

2 - التدمير :

يقصد بالتدمير إعدام الشيء وجعله غير صالح للاستعمال مطلقا، ومن هذه الناحية يختلف الإفساد عن التدمير من حيث، يتيح فرصة إصلاح النظام وإرجاعه لحالته الطبيعية، إلا أن التدمير يترتب عنه انعدام صلاحية النظام وعدم إمكانية إصلاحه.

ولم يبين المشرع الطريقة التي يمكن أن يتم بها تدمير سير نظام المعالجة الآلية للبيانات، ويبدو ذلك أمر منطقيا بالنظر لتعدد الوسائل ولغلبة الصبغة التقنية عليها بحيث يعسر حصرها أو تبويبها ويمكن أن تكون وسيلة التدمير مادية وذلك بتخريب الأجهزة المادية للنظام المعلوماتي أو قطع شبكات الاتصال، أو بسكب أي مادة على الأجهزة، يترتب عنها تدمير النظام.

كما يمكن أن تكون وسيلة التدمير معنوية، عبر استعمال البرامج والفيروسات التي تؤدي إلى إعدام سير نظام المعالجة الآلية للمعلومات، ومن أمثلتها برامج الدودة التي تستهدف أكبر نطاق ممكن من النظام المعلوماتي، وتقوم بأعمال تخريب للبرامج والبيانات سواء تعلق الأمر بالإفساد أو التدمير، فيجب أن يكون ارتكاب الجريمة قد تم بطريقة العمد.

وما يلاحظ أن المشرع الفرنسي، تخلى عن الإشارة إلى ركن العمد في هذه الجريمة إثر التنقيح المدخل على المجلة الجزائية سنة 1992، حيث كان الفصل 462-4 ينص أنه "كل شخص يسبب عمدا أو بدون مراعاة لحقوق الغير إعاقة وإفساد سير عمل نظام المعالجة الآلية للمعطيات يعاقب بالسجن لمدة تتراوح بين 3 أشهر و3 سنوات وبغرامة من 1000 إلى 100.000 فرنك، أو بإحدى العقوبتين، في حين أن الفصل 323-2 الذي عوض الفصل 462-4 من القانون الجنائي الفرنسي لم يتضمن عبارة «عمدا» التي حذفت بموجب التعديل المدخل على هذا الفصل.

ويبدو أن المشرع الفرنسي قد اعتبر أن الركن العمدي مفترض في هذه الجريمة، لضرورة أنه لا يمكن ارتكابها إلا بواسطة شخص ذي معارف فنية، وله إلمام واسع بأدق تفاصيل النظام المعلوماتي، ويرى الفقيه القانوني «Deveze» أن إزالة عبارة «عمدا» منطقي باعتبار أن القانون الجنائي الفرنسي أقر أن القصد الجنائي مفترض، وحين تكون الجريمة ناتجة عن خطأ تبرز ذلك، أما بالنسبة للجرائم العمد فليس من الضروري استعمال عبارة عمدا في كل مرة»[16]، وبذلك حذف المشرع الفرنسي بموجب تعديل 1992، عبارة «بدون مراعاة لحقوق الغير» ويعد ذلك أمرا طبيعيا، باعتبار أفعال التعطيل أو الإفساد هي أفعال غير مشروعة، وهي تشكل بذلك تعديا على حقوق الغير.

16. Deveze (J), atteinte au système automatisé des donnée. Article précité.

ومتى كانت الجريمة عمدية، ترتب إفساد أو تدمير سير النظام عن خطأ أو إهمال، فلا وجود لجريمة مثال ذلك الشخص الذي يستعمل اسطوانة ممغنطة تحتوي على فيروس مدمر للنظام المعلوماتي، دون أن يكون على علم بوجود هذا الفيروس إلا أن هذا التقصير والإهمال وإن كان لا يرتب مسؤوليته الجنائية فإنه يمكن أن يرتب مسؤوليته المدنية ومطالبته بجبر الأضرار التي تسبب فيها ومن تم طلب التعويض.

ومن أمثلة القضايا التي طرحت فيها هذه الجريمة قضية شهيرة في فرنسا تمثلت وقائعها في قيام شخص متخصص في المجال، بالسيطرة على النظام المعلوماتي لشركة موجودة بمدينة باريس، وانطلاقا منه قام بتوجيه اعتداءات على مئات المواقع الحكومية بما نجم عنه الإضرار بهذه المواقع، وذكر الجاني أنه أقدم على هذه الأفعال ليكشف النقائص التي تعتري برامج الحماية للأنظمة المعلوماتية التي قام بالاعتداء عليها، وقد أدين من أجل جملة من التهم بما فيها إعاقة سير نظام المعالجة الآلية للبيانات[17].

الفقرة الثانية : تمظهرات الحماية المقررة في القانون الجنائي المغربي

لا يمكن أن تطال الاعتداءات، نظام المعالجة المعلوماتية فحسب، بل البيانات التي يحتويها، وهنا تتضح خطورة مثل هاته الأفعال، والاعتداء على البيانات والمعطيات يمكن أن يكون ناتجا عن الدخول أو البقاء بنظام المعالجة المعلوماتية (أولا) أو بصفة مستقلة عبر إدخال بيانات جديدة لنظام المعالجة يترتب عنها إفساد البيانات الموجودة (ثانيا).

أولا : الاعتداء على البيانات كنتيجة للدخول غير الشرعي

اقتضى الفصل 3-607[18] مضاعفة العقوبة المقررة في حالة تدمير، أو إفساد البيانات في هذه الصورة كظرف تشديد لجريمة الدخول، أو البقاء بصفة غير شرعية، متى ثبتت العلاقة السببية بين هذا الدخول غير الشرعي لنظام المعالجة المعلوماتية والإضرار بالبيانات الموجودة به.

نلاحظ، أن الفقرة الأولى من هذا الفصل، تجرم الدخول إلى مجموع، أو بعض نظام المعالجة الآلية للمعطيات، لكن يجب أن يتم ذلك عن طريق الاحتيال، وعليه فإن اشتراط هذا

17. Tribunal de grande instance de paris 12ème chambre jugement du 20 juin 2006.

18. الفصل 3-607 على ما يلي (يعاقب بالحبس من شهر إلى ثلاثة أشهر وبالغرامة من 2000 إلى 10000 درهم أو بإحدى هاتين العقوبتين فقط كل من دخل إلى مجموع أو بعض نظام المعالجة الآلية للمعطيات عن طريق الاحتيال).

الأخير لقيام الجريمة يعني أن الجريمة هنا عمدية، ثم إن المشرع المغربي لم يشترط في هذا النص القانوني كون النظام محميا أم لا، ولم يشترط حدوث النتيجة الإجرامية[19].

وعليه، فالمشرع يجرم كل حالة يدخل فيها شخص إلى نظام المعالجة الآلية للمعطيات وبالتالي ففعل الدخول وحده بدون حق مجرم قانوناً، وقد عاقب المشرع المغربي مقترف هذه الجريمة - حسب الفقرة الأولى من الفصل 3-607 - بالحبس من شهر إلى ثلاثة أشهر وبالغرامة من 2000 إلى 10.000 درهم، أو بإحدى هاتين العقوبتين ويتضح بذلك الأهمية المضاعفة التي يوليها المشرع للبيانات المعلوماتية.

المشرع الفرنسي من ناحيته أقر عقوبة مشددة في صورة ما إذا ترتب عن النفاذ أو البقاء غير الشرعي بنظام المعالجة المعلوماتية الإضرار بالبيانات، وقد رفع في العقاب في مناسبتين فبعد أن كان في الفصل 462-2 فقرة ثانية من القانون الجنائي الفرنسي بالسجن لمدة تتراوح بين شهرين وعامين وغرامة من 10.000 فرنك إلى 100.000 فرنك أصبح بموجب تعديل سنة 1992 بالسجن لمدة سنتين وبغرامة بـ 300.000 فرنك[20]، ثم وقع الرفع في العقوبة بعد التعديل المدخل على القانون الجنائي الفرنسي بموجب القانون عدد 575.204 المؤرخ في 21 يونيو 2004، وأصبحت عقوبة السجن لمدة ثلاث سنوات والغرامة بمبلغ 45.000 أورو[21].

ما يلاحظ أن المشرع الفرنسي استعمل عبارات الحذف والتغيير، في حين أن المشرع المغربي استعمل عبارات الإفساد والتدمير، وعبارة الإفساد التي استعملها المشرع المغربي، لها مدلول أوسع من التغيير، باعتبار أن الإفساد يعني إحداث عطب بالشيء أي إدخال اضطراب عليه يجعله غير قادر على أداء وظيفته بصورة طبيعية، أما عبارة التدمير فتعني الحذف والمسح للبيانات.

وفي الحالة التي يكون الإفساد أو تدمير البيانات ناتجا عن الدخول غير الشرعي لنظام المعالجة لا يشترط الركن العمدي لقيام الجرم وتسليط العقاب، بل أضاف المشرع المغربي من خلال الفصل 4- 607 إقرار عقوبات أشد، وذلك بالحبس من ستة أشهر إلى سنتين وبالغرامة من 10.000 إلى 100.000 درهم لكل من ارتكب الأفعال المشار إليها في الفصل السابق في حق مجموع

19. أمين أعزان، مواجهة الجريمة الإلكترونية في ضوء القانون الجنائي المغربي مجلة الحقوق المغربية، العدد 12 السنة السادسة 2011

20. « Lorsqu'il en résulte soit la suppression où la modification des données contenues dans le système, soit une altération du fonctionnement de ce système la peine est de deux ans d'emprisonnement et de 300.000 Francs d'amende », Article 323-1 alinéa2, du code pénal français.

21. Lorsque il en résulte 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 45.000 euros d'amende, code pénale partie législative lié à la sécurité informatique par Sébastien Fontaine sur www.authsecu.com

أو بعض نظام للمعالجة الآلية للمعطيات يفترض أنه يتضمن معلومات تخص الأمن الداخلي أو الخارجي للدولة أو أسرارا، تهم الاقتصاد الوطني.

نلاحظ أيضا، أن المشرع المغربي، حدد عقوبة أشد من تلك الواردة بالفصل السابق وهذا طبيعي نظراً لقيمة المعلومات والمعطيات محل الحماية الجنائية، حيث إنها تتعلق بالأمن الداخلي أو الخارجي للدولة أو متعلقة بأسرار مرتبطة بالاقتصاد الوطني، فمثل هذه المعلومات يمثل الاعتداء عليها اعتداءا على مقومات الدولة من الناحية السياسية، أو الاجتماعية، أو الاقتصادية[22]، وقد يطرح التساؤل هنا، إذا كان الولوج إلى نظام المعالجة الآلية للبيانات، قد تم بصفة شرعية ثم ترتب عنه، أو عن البقاء بالنظام إفساد أو تدمير البيانات، فهل يمكن تجريم هذه الفعل ؟.

يبدو أن الإجابة لا يمكن أن تكون إلا بالنفي، باعتبار المشرع ربط بين فعل الدخول الغير الشرعي للنظام، وتدمير وإفساد البيانات التي يحتويها النظام، فمتى ترتب هذا الأثر الأخير عن ولوج شرعي بنظام المعالجة الآلية للبيانات فلا يمكن الحديث عن جريمة أو عقاب مشدد على معنى ما ذهب إليه الفصل 4-607.

وقد عمل المشرع المغربي على تشديد العقوبة أكثر، إذا ما تسبب فعل الدخول، أو البقاء غير المشروع داخل نظام المعالجة، إلى حذف، أو تغيير للمعطيات، أو خلق اضطراب في سير النظام المعلوماتي، كما أضاف المشرع عنصر التشديد في العقوبة إذا ارتكبت من قبل موظف أو مستخدم أثناء مزاولته لمهامه أو بسببها.

وقد حدد المشرع العقوبة في مثل هذه الحالات، في الحبس من سنتين إلى خمس سنوات والغرامة من 100.000 إلى 200.000 درهم، كما جاء في الفقرة الثانية من الفصل 4-607 في حين أن الفقرة الأولى حددت العقوبة في الحبس من ستة أشهر إلى سنتين والغرامة من 10.000 إلى 100.000 درهم مغربي.

الفصل 5-607 حيث العقوبة تصل لثلاث سنوات وبالغرامة من 10.000 إلى 200.000 درهم أو بإحدى هاتين العقوبتين، وكل من عرقل عمداً سير نظام للمعالجة الآلية للمعطيات أو أحدث فيه إخلالا، حيث يستشف من هذا الفصل أنه عاقب على عرقلة سير نظام المعالجة الآلية للمعطيات، والعرقلة قد تتخذ صوراً كثيرة منها : إرسال الفيروسات المدمرة للمعطيات الموجودة داخل النظام.

22. أمين أعزان، مواجهة الجريمة الإلكترونية في ضوء القانون الجنائي المغربي، مرجع سابق.

وقد حدد المشرع عقوبة هذا الفعل في الحبس من سنة إلى ثلاث سنوات والغرامة من 100.000 إلى 200.000 درهم أو بإحدى هاتين العقوبتين. ويبدو جليا من خلال هذا الفصل أن المشرع المغربي، اشترط العمد لقيام الجريمة، وبالتالي لابد أن تتجه إرادة الجاني إلى عرقلة سير نظام المعالجة مع علمه بذلك.

مسألة إتلاف، أو حذف، أو تغيير النظم المعلوماتية، لم تكن غائبة على ذهن المشرع المغربي وخصها في الفصل 6-607، مضيفا عنصرا آخر، هو عنصر الاحتيال، وأقر له نفس عقوبة الفصل السابق.

كما أن المشرع الفرنسي لم يتعرض للقصد الجنائي في الفقرة الثانية للفصل 323-1 من القانون الجنائي الفرنسي، وقد اعتبر أغلب الفقهاء الفرنسيين أن القصد الجنائي الخاص غير مفترض، وفي هذا الإطار أصدرت المحكمة الابتدائية بـ«Nanterre» حكما ابتدائيا بتاريخ 10 فبراير 2006 [23] أدانت فيه المتهم «Hugues. B» من أجل حذف وتغيير البيانات نتيجة دخول غير شرعي لنظام المعالجة الالكترونية لشركة «BCA» وقد اعتبر هذا الأخير مذنبا لمجرد حصول النتيجة عن الدخول غير الشرعي بنظام المعالجة المعلوماتية وإفساد البيانات، دون الخوض في وجود تعمد لتحقيق هذه النتيجة من عدمه.

أما في صورة توفر النية لإحداث الضرر فإن الفعل يقع تحت طائلة الفصول التي تهتم بجرائم الاعتداء العمدي على بيانات نظام المعالجة المعلوماتية[24].

ثانيا: الاعتداء العمدي على بيانات نظام المعالجة المعلوماتية

اقتضى الفصل 607 في فقرته الخامسة من القانون الجنائي أنه: "يعاقب بالحبس من سنة إلى ثلاث سنوات وبالغرامة من 10.000 إلى 200.000 درهم أو بإحدى هاتين العقوبتين كل من عرقل عمداً سير نظام للمعالجة الآلية للمعطيات أو أحدث فيه إخلالا "وتجدر الإشارة أن المشرع المغربي عاقب على عرقلة سير نظام المعالجة الآلية للمعطيات، هذه الأخيرة تتخذ صوراً كثيرة منها: إرسال الفيروسات المدمرة للمعطيات الموجودة داخل النظام، وقد حدد المشرع عقوبة هذا الفعل في الحبس من سنة إلى ثلاث سنوات والغرامة من 100.000 إلى 200.000 درهم أو بإحدى هاتين العقوبتين.

ويبدو جليا من خلال هذا الفصل أن المشرع المغربي اشترط العمد لقيام الجريمة، وبالتالي لابد أن تتجه إرادة الجاني إلى عرقلة سير نظام المعالجة مع علمه بذلك، ومسايرة للنهج الذي

23. Tribunal de grande instance de Nanterre 15ème chambre jugement du 10 février 2006.

24. Gassin, article précité, page 34.

سلكه المشرع الفرنسي الذي خصصته المادة 3-323 لتجريم إدخال معطيات، غشاً داخل نظام المعالجة الآلية للمعطيات، أو حذف أو تعديل هذه المعطيات الموجودة داخل هذا النظام.

لكن الملاحظ هو أن المشرع المغربي من خلال الفصل 6-607 جرّم كذلك مسألة تغيير طريقة معالجة أو إرسال المعطيات عن طريق الاحتيال.

وقد حدد المشرع عقوبة الجريمة المذكورة في هذا الفصل في الحبس، من سنة إلى ثلاث سنوات، والغرامة من 10.000 درهم إلى 200.000 أو إحدى العقوبتين.

يتبين من خلال هذا الفصل تشدد المشرع في العقاب المقرر إذا ما تعلق الاعتداء بالبيانات التي يحتويها نظام المعالجة المعلوماتية، وهو يعكس الأهمية التي تشكلها هذه البيانات الإلكترونية.

وقد اتخذ المشرع الفرنسي نفس الموقف حيث ارتفع بالعقاب في صورة إدخال بيانات أو محو أو تعديل بيانات بنظام المعالجة الآلية إلى خمس سنوات وبغرامة 75.000 أورو حسب منطوق الفصل 3-323 الجديد من القانون الجنائي الفرنسي[25].

ويتكون السلوك الإجرامي في هذه الجريمة من إدخال بيانات جديدة لنظام المعالجة الآلية للمعلومات التي من شأنها إفساد البيانات الأصلية، أو طريقة تحليلها، أو تحويلها وفعل الإدخال يتم إما بصورة مباشرة وذلك بالتواصل بين الفاعل وأجهزة الإعلامية إذا كان من العاملين بالنظام المعلوماتي.

كما يمكن أن يكون النفاذ عن بعد ودون الحاجة للتواجد قرب الجهاز المعلوماتي عبر ما توفره الشبكات المفتوحة من إمكانية الوصول إلى مختلف الأنظمة المعلوماتية كلما كانت هذه الأخيرة مرتبطة بهذه الشبكات، ويكفي الحصول على كلمة السر أو مفتاح الدخول للولوج لهذه الأنظمة والعبث بالبيانات التي تحتويها.

إن إدخال بيانات غريبة عن النظام المعلوماتي، يؤدي بالضرورة إلى إفساد البيانات الأصلية أو تغيير طريقة تحليلها وتحويلها، باعتبار أن هذه البيانات هي عبارة عن رموز يقع إعدادها حسب منطق معين، وتسلسل مدروس في غاية من الدقة، ومجرد المساس بذلك التنظيم من شأنه أن يدخل اضطرابا على طريقة تحليل المعطيات، وذلك إما بتحويل أماكنها الأصلية، أو بقلب الرموز الأصلية بحيث تصبح غامضة ولا تؤدي الوظيفة المطلوبة منها بصفة طبيعية.

25. Art. 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 cinq ans d'emprisonnement et de 75000 euros d'amende. Code pénal partie législative liée à la sécurité informatique par Sébastien Fontaine sur www.authsecu.com.

وما يلاحظ كذلك أن المشرع المغربي، قد جرم إفساد البيانات، عبر إدخال بيانات جديدة للنظام المعلوماتي، في حين أن الإفساد يمكن أن ينتج أيضا، عن استعمال طرق أخرى، مثل حذف البيانات جزئيا أو كليا، أو تغييرها بدون إدخال بيانات جديدة، وهو ما أشار له المشرع الفرنسي، بالفصل 3-323 من القانون الجنائي الذي اقتضى أنه : «إدخال بيانات بصفة غير شرعية في نظام المعالجة الآلية أو تعديل البيانات الموجودة به، أو حذفها يعاقب عليه بالسجن لمدة خمس سنوات وبغرامة بمبلغ 75000 أورو».

وربما كان من الأسلم لو أشار المشرع المغربي، إلى مختلف هذه الطرق حتى يشمل التجريم مختلف طرق التلاعب بالبيانات المعالجة الكترونيا، وحتى يكون الحل واضحا عند إفساد البيانات، أو طريقة تحليلها أو تحويلها، لا عبر إدخال بيانات جديدة وإنما عبر تعديل الأصلية أو حذفها.

وبالنظر للطبيعة المعقدة لهذه الجريمة، فإنه غالبا ما يكون مقترفها من قبل الفنيين الذين لهم إلماما واسعا بالمجال المعلوماتي وتفاصيله الدقيقة، وفي أغلب الأحيان بمناسبة مباشرتهم لنشاطهم المهني.

المحور الثاني : الحماية الجنائية المقررة من خلال القانون 08-09

يمكن أن تخضع المعطيات الشخصية للمعالجة الإلكترونية، وبذلك تصبح هذه المعطيات على شكل بيانات إلكترونية، تعكس جوانب من الحياة الخاصة للفرد، وتدخل بذلك في زمرة الوثائق الإلكترونية، بما تشكله من مجموع البيانات المعالجة إلكترونيا، ويمكن أن تكون محل اعتداء، سواء برفع جانب السرية عنها أو بتحريفها. وقد تضمن القانون 08-09 جملة من الأحكام الجنائية، التي من شأنها زجر المخالفات عند المعالجة الإلكترونية للبيانات الشخصية، المتعلقة بالاستعمال غير الشرعي للمعطيات المعالجة إلكترونيا (الفقرة الأولى) أو بعدم أخذ تدابير الحماية اللازمة عند معالجتها (الفقرة الثانية).

الفقرة الأولى: المعالجة غير المشروعة للمعطيات الشخصية

تعتمد المواقع التجارية في سياستها التسويقية، على المعطيات الشخصية، كآلية من آليات التسويق المباشر، التي تسمح بتحديد احتياجات المستهلكين، والعمل على تلبيتها وهو ما من شأنه أن يجعل هذه المعطيات، ذات القيمة الاقتصادية، عرضة للاعتداء سواء بمعالجتها بطريقة غير شرعية، ومن ثم شرعية الحماية أثناء المعالجة (أولا) أو بإساءة استعمالها (ثانيا)

أولا : معالجة المعطيات الشخصية وشرعية الحماية:

سبق وإن وقع التعرض على أن المشرع قد نظم عملية معالجة المعطيات الشخصية وذلك تكريسا للحماية الوقائية لهذه المعطيات، باعتبار أن عدم احترام تلك الضوابط لتخزين ومعالجة المعطيات الشخصية من شأنه أن يمس بالحريات الفردية والحياة الخاصة[26].

حيث يعتبر المشرع من قبيل التعسف في استعمال المعطيات الشخصية، إنشاء بطاقات سرية وذلك في حالة ما إذا تمت معالجة المعطيات الشخصية دون تقديم التصريح المنصوص عليه في القانون، أو في حالة استمرارية معالجة المعطيات، بعد منعها من طرف اللجنة الوطنية لحماية المعطيات الشخصية، كما تشكل اعتداء على حق الفرد في السيطرة على المعطيات الشخصية المتعلقة به، عملية الجمع التي تتم بدون موافقة صريحة من المعني بالأمر أو إذا وقع استعمال أساليب غير مشروعة في الجمع.

كما أن عدم احترام واجب إخبار الشخص المعني بالمعالجة، يعد تعديا على الحقوق الشخصية للفرد. باعتبار أن الموافقة الصريحة لا تكون قائمة إلا إذا صدرت على بينة قانونية تؤكد رضا الشخص المعني بالمعالجة، هذا وقد لوحظ أن العديد من الأشخاص يتمكنون من الولوج إلى الأنظمة المعلوماتية لجهاز الكمبيوتر، عن طريق استغلالهم النقاط الضعيفة في منظومة الأمن[27]، لذلك يكون المسؤول عن المعالجة سواء قام بها بنفسيه أو بواسطة غيره، مسؤول عن الاعتداءات التي تتعرض لها المعطيات الشخصية، باعتبار أنه لم يمنع ذلك باتخاذ الإجراءات والاحتياطات اللازمة والمنصوص عليها في القانون، وذلك ضد أي فعل من شأنه تعديل أو الإضرار بالمعطيات، أو الاطلاع عليها دون إذن صاحبها وسنتعرض لاحقا إلى الممارسات التي تمثل تعديا على نظام المعالجة الآلية للمعطيات.

هذا وقد لا تسلم المعطيات الشخصية، من أن تكون محل اعتداء، ولو تمت عملية جمعها بطريقة شرعية، وذلك إذا ما احتفظ المسؤول عن المعالجة بهذه المعطيات بطريقة غير شرعية وذلك في صورة تجاوز مدة الاحتفاظ المنصوص عليها بالتصريح أو في حالة تحقق الغرض الذي جمعت من أجله، أو إذا لم تعد ضرورية لنشاطه.

---

26. عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الالكترونية، مرجع السابق، ص: 66.
27. عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون دراسة مقارنة، منشورات الحلبي الحقوقية، الطبعة الثانية، ص: 273.

ثانيا – إساءة استعمال المعطيات الشخصية:

كما سبق بيان ذلك، فإن المعطيات الشخصية، تمثل ركيزة من ركائز التجارة الإلكترونية، حيث تزود منها أصحاب المواقع التجارية كما يتزودون من السلع، وقد يكون هذا التزود شرعيا، إذا ما وقع احترام الضوابط التي أقرها المشرع في معالجة وجمع المعطيات الشخصية، إلا أنه كثيرا ما يقع الانحراف باستعمال هذه المعطيات وذلك باستعمالها في غير الأغراض التي جمعت من أجلها، التي وقع التنصيص عليها في التصريح المقدم للجنة الوطنية لحماية المعطيات الشخصية، وحصلت الموافقة عليها من طرف الشخص المعني بالأمر.

فالمستهلك الذي يقوم بمد صاحب الموقع التجاري، بمعطياته الشخصية بغاية شراء سلعة أو خدمة معينة فإنه يقوم بذلك على أساس أن هذه المعطيات، لن يقع استعمالها إلا بهدف القيام بإجراءات المعاملة «الأمر الذي يجعل من تغيير وجهة المعلومة المجمعة إلى ميادين أخرى خارجة عن إطار موافقة المعنى يشكل انتهاكا للحريات الفردية »[28].

هذا، ويطالب المسؤول عن المعالجة إلى جانب عدم الانحراف بالغرض الذي جمع من أجله المعطيات، أن يحافظ على سريتها، باعتباره مؤتمنا عليها، فإذا كانت حاجة المستعمل قد اضطرته إلى البوح بالمعطيات الشخصية المتعلقة به لإتمام المعاملة، فإن من حقه على صاحب الموقع التجاري، أن يبقيها في إطار السرية، فلا يقوم بإفشائها ونشرها بطريقة تسيء لصاحبها أو لحياته الخاصة »[29].

والحقيقة أن سرية المعطيات الشخصية، ليست فقط محل تهديد من طرف المسؤول عن المعالجة، أي الذي بحوزته هذه المعطيات، ولكن قد تتعرض هذه المعطيات للاعتداء أيضا من خارج المؤسسة، وذلك عن طريق الأنظمة المعلوماتية.

28. علي كحلون، الإطار القانوني للإعلامية في تونس، المجلة القانونية التونسية، مركز النشر الجامعي 2005، ص: 356.
29. نفس المرجع والصفحة.