

حماية المستهلك جنائياً من مخاطر التعاقد الإلكتروني

بقلم: أ/ مكّي إيمان *

ملخص:

نتيجة للتطور التقني الحديث في تكنولوجيا المعلومات والاتصالات ونظراً لخصوصية التعاملات الإلكترونية التي أصبحت تشكل واقعا افتراضيا لا ينكر، بدت الحاجة إلى تفعيل الآليات أو الميكانيزمات المقررة للمستهلك الإلكتروني وتطويعها. فبعض المستهلكين قد يرفضون التعامل بالتكنولوجيا الحديثة خوفهم من التعرض للغش والاحتيال والاعتداءات غير المتوقعة، ومن هنا بات من الضروري وجود ضوابط قانونية يعمل في إطارها التطور التكنولوجي والتي بدونها يصبح التقدم العلمي طامة كبرى على المجتمع وحقوق وأمن المستهلكين.

وترتب عن الأهمية المتزايدة للتجارة الإلكترونية عدة مشاكل قانونية أخطرها الجريمة المعلوماتية على نحو يهدد التنمية الاقتصادية، مما أدى إلى ضرورة توفير حماية جنائية للتجارة الإلكترونية.

ولعلّ تلك الإرهاصات والمتناقضات كانت الدافع وراء إجراء هذه الدراسة التي حاولنا من خلالها جمع شتات وأبعاد الموضوع عبر إطار قانوني متكامل ورؤية موجزة وشاملة، وهذا بالإضافة إلى استعراض التطورات التشريعية العالمية وبوأكير الأحكام القضائية، على مستجدات المسألة وتطوراتها المتلاحقة.

الكلمات المفتاحية: مخاطر التعاقد الإلكتروني، الأنترنت، التعاملات الإلكترونية، المستهلك الإلكتروني، الحماية الجنائية، أمن المستهلكين.

* أستاذة باحثة في صف الدكتوراه سنة ثالثة تخصص قانون المنافسة والاستهلاك بجامعة أبي بكر بلقايد- تلمسان.

Résumé:

Suite au développement technique contemporain que connaît la technologie de l'information et la communication, et vu la spécificité des transactions électroniques qui sont devenues de nos jours une réalité virtuelle évidente, il s'avère nécessaire de mettre en œuvre des mécanismes adaptés pour le consommateur de l'électronique. Certains consommateurs pourraient refuser en fait, l'utilisation de la technologie moderne, de peur de fraude et abus inattendus, par conséquent, il est désormais nécessaire d'avoir une régulation juridique allant de paire le développement technologique sans lequel le progrès scientifique devient une catastrophe pour la société, le droit et la sécurité des consommateurs.

L'importance du commerce électronique a engendré beaucoup de problème juridiques ainsi que le crime électronique qui menace le développement économique.

Ce sont ces signes avant-coureurs et ces contradictions qui nous ont motivés à mener cette étude, à travers laquelle nous avons essayé de cerner les dimensions du sujet dans un cadre juridique complémentaire et à travers une vision concise et globale, outre l'exposition des progrès législatifs mondiaux et les prémices des dispositions juridiques, et l'application des règles générales aux nouveautés en la matière et ses progrès successifs.

Mots clé: Les risques de contrats électroniques, internet, transactions électroniques, le consommateur électronique, La protection pénale, la responsabilité, la sécurité des consommateurs.

Summary:

As a result of modern technical development in information technology and communication, and according to the specificity of electronic transactions that have become an obvious reality, the necessity for suitable mechanisms has appeared as a mean to protect the electronics consumer. Some consumers would refuse to use technology for fear of fraud and unexpected abuse, consequently, it is necessary to have a legal framework in which could work technological development, and without which scientific progress is a plague on society, and on rights and safety of consumers.

It's importance baby many problems juridique, which menace the development économique such as: the electronic crimes.

All these problems and contradictions have motivated us to do this study, through which we have tried to collect the dimensions of the subject in a single legal framework and by concise and complete vision, in addition to reviewing global legislative developments and the content of juridical judgment, and the implementation of general rules on the new matter and its successive progress.

Keywords: The risks of electronic contracting, internet, electronic transactions, electronics consumer, civil and criminal protection, liability, security of consumers.

مقدمة:

الجريمة المعلوماتية (cyber crime) أو ما يعرف بالجريمة المستحدثة أثارت ضجة في الأوساط الفقهية فالبعض ينعونها بجرائم التكنولوجيا، والبعض الآخر يطلق عليها تسمية جرائم الإعلام الآلي أو جرائم التقنية العالية⁽¹⁾ (techno crimes). فتعددت تعريفات الجريمة المعلوماتية وتباينت فيما بينها ضيقا واتساعا، وقد أسفر ذلك عن تعذر إيجاد فهم مشترك لظاهرة الجريمة الالكترونية. فمصطلح الجريمة المعلوماتية مزيج بين مصطلحين: «الجريمة والمعلوماتية». ولعلّ تعريف منظمة التعاون الاقتصادي والتنمية الخاص باستبيان الغش المعلوماتي عام 1982 والذي أورده بلجيكا في تقريرها بأنّ الجرائم المعلوماتية هي: «كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية»⁽²⁾. فالجريمة المعلوماتية هي إفراز ونتاج لتقنية المعلومات واتساع نطاق تطبيقها في المجتمع فبعضها قد يتطابق مع خصائص طوائف أخرى من الجرائم وهي جرائم الياقات البيضاء white collar crime وبعضها الآخر يميزها عن الجرائم التقليدية لصعوبة كشف وإثبات الجرائم الأولى دون

(1) - وفي هذا الصدد وحسب تعريف الفقيه "SIEBER":

"est considéré comme crime informatique tout comportement illégal ou non autorisé qui concerne un traitement automatique de données ou de transmission de données".

(2) - انظر: حاجب هيام، الجريمة المعلوماتية، مذكرة لنيل إجازة المدرسة العليا للقضاء، 2005-2008،

ص 7.

الثانية⁽¹⁾.

فقد تطورت الظاهرة الإجرامية في الآونة الأخيرة تطورا مذهلا سواء في أشخاص مرتكبيها أو في أسلوب ارتكابها، والذي يمثل في استعمال آخر ما توصل إليه العلم وتطويعه في خدمة الجريمة، وقد زاد من أهمية البحث صعوبة تطبيق النصوص التقليدية على هذه الجرائم، وهو ما دفع العديد من الدول إلى التدخل التشريعي لمواجهة الجريمة المعلوماتية، فخطرها المحتمل في بيئتنا يمكن أن يكون كبيرا⁽²⁾.

إنّ الاستخدام المضطرب للمعلوماتية سواء في شكل أموال معلوماتية أو أساليب مستحدثة أدّى إلى ظهور ما يعرف بالإجرام المعلوماتي (délinquance informatique) كنتيجة حتمية لكل تقدم تقني مستحدث، إلّا أن ذلك لا ينفي ضرورة التصدي لبوادره كي لا يستفحل مع وتيرة التّمّو المتسارع الذي تشهده دول عربية عدّة ومن بينها الجزائر في استخدام النّظم المعلوماتية. فضلا عن ظروف العولمة والتبعية التكنولوجية من مناح موات لانتهاك حرمة البيانات الشخصية والمساس بالأمن القومي لهذه الدول والسيادة الوطنية⁽³⁾: وقد أكّدت هذا الطرح "روي جودسون" الخبيرة بمركز المعلومات الوطني الأمريكي بقولها: «لقد أصبحت الجريمة أكثر قوة بفضل التقنية الحديثة»⁽⁴⁾، وعليه وبالنظر إلى الأهمية المتزايدة للتجارة الإلكترونية ظهرت مشاكل قانونية عديدة تتعلق بفروع القانون المختلفة كالقانون المدني والقانون التجاري والقانون الدولي الخاص، وبصفة خاصة في

(1) - قارة آمال، الجريمة المعلوماتية، رسالة ماجستير في القانون الجنائي والعلوم الجنائية، جامعة الجزائر، 2001-2002، ص18.

(2) - هدى قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، الطبعة الأولى، دار النهضة العربية، القاهرة، 1992، ص15.

(3) - إبراهيمي سهام، الجريمة المعلوماتية، مذكرة تخرج لنيل شهادة المدرسة العليا للقضاء، 2004-2007، ص1-2.

(4) - انظر: قارة آمال، المرجع السابق، ص8.

القانون الجنائي، بحيث أصبح المستهلك (الطرف الضعيف في العملية التعاقدية) عرضة لاعتداءات إجرامية متزايدة على نحو يهدد التنمية الاقتصادية مما أدى إلى ضرورة اقرار حماية جنائية في مجال التعاقد الإلكتروني. فقيم تتمثل خصوصية الجرائم الإلكترونية المستحدثة؟ وما هو موقف التشريعات المقارنة في هذا الخصوص؟

ولمعالجة الإشكالية السالفة ارتأينا تقسيم المساهمة إلى ثلاثة مطالب:

المطلب الأول: الجرائم الماسة بالمواقع الإلكترونية والبيانات الشخصية

المطلب الثاني: الجرائم الماسة بانتهاك سرية وخصوصية البيانات الشخصية

المطلب الثالث: الجرائم الخاصة بالتوقيع الإلكتروني والبيانات المشفرة

المطلب الأول: الجرائم الماسة بالمواقع الإلكترونية

لقد شهد العصر المعاصر تضافرا للجهود على المستويين الوطني والدولي من أجل حماية مواقع التجارة الإلكترونية من خلال تجريم الدخول العمدي أو البقاء غير المشروع في نظام معالجة البيانات، وكذا تجريم الاعتداء على نظام معالجة المعلومات.

كما اهتمت القوانين المقارنة بحماية البيانات الشخصية أو الاسمية في برنامج المعلومات، ووضعت قيودا على الحكومات والأجهزة الإدارية العامة والخاصة والأفراد بصدد إنشاء أنظمة معلوماتية، حيث يحظر تخزين المعلومات الشخصية التي تمس الحريات والحياة الخاصة، ويحظر انتهاك السرية والخصوصية، أو استخدام بيانات التجارة الإلكترونية في غير الأغراض المخصصة لها⁽¹⁾.

الفرع الأول: الجرائم المتعلقة بالمواقع الإلكترونية

إنّ شبكات المعلوماتية هي موضوعا لبعض جرائم الأموال كالسرقة، والإتلاف

(1) -انظر: محمد حسين منصور، المسؤولية الإلكترونية، دار الجامعة الجديدة، الإسكندرية، مصر، 2007، ص 149-150.

العمدي لأجهزة الحاسب الآلي بالإضافة إلى الجرائم التي يكون محلها بيانات غير مادية⁽¹⁾، وفي هذا الصدد تشير الإحصائيات إلى وقوع ما بين 200 إلى 250 حالة اعتداء يوميا على الأنظمة المعلوماتية في الجزائر⁽²⁾. وإن تفاقم الاعتداءات الواقعة على الأنظمة المعلوماتية خاصة مع ضعف الحماية الفنية استدعى تدخلا تشريعا على المستويين الدولي والداخلي. فعلى المستوى الدولي تم وضع أول اتفاقية حول الإجرام المعلوماتي بتاريخ 2001/11/08 تضمنت مختلف أشكال الإجرام المعلوماتي. أما على المستوى الوطني فقد استدرك المشرع الجزائري الفراغ القانوني من خلال التعديل الأخير لقانون العقوبات⁽³⁾، وكذا القانون 09-04 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها⁽⁴⁾.

أولاً: مفهوم نظام المعالجة الآلية للمعطيات

يعد نظام المعالجة الآلية للمعطيات بمثابة الشرط الأول الذي يلزم تحققه لإثبات حدوث اعتداء على نظام المعالجة الآلية للبيانات من عدمه⁽⁵⁾، وتجدر الإشارة أن المشرع الجزائري تبنى التعريف الذي جاءت به الاتفاقية الدولية للإجرام المعلوماتي وهذا بموجب أحكام المادة الثانية الفقرة ب من قانون 04-09 وأطلق عليه تسمية «منظومة معلوماتية»⁽⁶⁾. ومن أجل الحفاظ على خصوصية

(1) - هدى قشقوش، المرجع السابق، ص 17.

(2)- Cf. K.BENLKADI, Les sites algériens vulnérables, journal el waten, 23/12/2002 n°-3668, p. 46.

(3) - راجع المواد: من 394 مكرر إلى غاية 394 مكرر من القانون رقم 23-06 المؤرخ في 20 سبتمبر 2006 المعدل والمتمم لقانون العقوبات الجزائري، الصادر في ج.رج.ج. رقم 84، ص 116.

(4)- القانون رقم 04-09 المؤرخ في 5 غشت 2009 المتضمن القواعد الخاصة بالوقاية من تكنولوجيا الإعلام والاتصال ومكافحتها، ج.رج.ج.ج. ع 47، ص 1.

(5) - عبد الفتاح بيومي حجازي، التجارة الالكترونية وحمايتها القانونية، دار الكتب القانونية، مصر، 2000، ص 21.

(6) - راجع نص المادة 2 من قانون رقم 04-09 سالف الذكر.

البيانات المتناقلة عبر الشبكات، أكد الخبراء والمتخصصون في مجال أمن المعلومات على ضرورة استخدام أسلوب التشفير لأنه يمثل أفضل وسيلة للحفاظ على سرية البيانات المتناقلة ولمنع الآخرين من الاطلاع على الرسائل الإلكترونية⁽¹⁾.

والسؤال المطروح حول مدى اعتبار الحماية الفنية للنظام كشرط للتمتع بالحماية الجنائية؟ وبالرجوع إلى النصوص المتعلقة بجرائم الاعتداء على أنظمة المعالجة الآلية نجد أنها لا تتضمن شرط الحماية، ونظرا لأن المشرع لم يتطرق لشرط الحماية الفنية فإنه يستكشف من ذلك أنه أراد استبعاده.

ثانياً: الأركان الأساسية لجرائم المواقع الإلكترونية

يمكن تحديد هذه الأركان في الركن المادي، الركن المعنوي.
فبخصوص الركن المادي فإنه يتمثل في الأشكال المختلفة للاعتداء على نظام المعالجة الآلية للمعطيات والتي يمكن تحديدها في العناصر التالية :

- الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات:

(accès et maintien frauduleux dans un système de traitement automatisé des données)

أي الدخول إلى العمليات الذهنية التي يقوم بها نظام المعالجة الآلية للمعطيات. ولم يحدد المشرع وسيلة الدخول إلى النظام فقد يتم عن طريق كلمة السر الحقيقية، أو استخدام برنامج أو شفرة خاصة، أو عن طريق استخدام الرقم الكودي لشخص

(1) - يمكن التمييز بين نوعين من التشفير:

الشكل الأول ويسمى (La cryptologie symétrique) ومفاده أن نفس المفتاح التشفيري يستعمل للتشفير ول فك الشفرة. أما الشكل الثاني المعروف ب (La cryptologie Asymétrique) يتطلب استخدام مفتاحاً خاصاً وآخر عاماً، والمرسل إليه وحده بإمكانه الاطلاع على الرسالة المشفرة باستعمال المفتاح الخاص. انظر في هذا الصدد: سوير سفيان، جرائم المعلوماتية، مذكرة الماجستير في العلوم الجنائية وعلم الإجرام، جامعة أبي بكر بلقايد، تلمسان، 2010 - 2011، ص 87.

آخر؛ فيستوي أن يتم الدخول مباشرة أو عن طريق غير مباشر⁽¹⁾. وتقع هذه الجريمة من كل إنسان أيّاً كانت صفته وكفاءته المهنية والفنية.

في حين يقصد بفعل البقاء (le maintien)⁽²⁾ التواجد داخل نظام المعالجة الآلية للمعطيات ضدّ إرادة من له الحق في السيطرة على هذا النظام، ويكون البقاء معاقباً عليه استقلالاً حيث يكون الدخول إلى النظام مشروعاً. ومن أمثلة ذلك أن يتحقق الدخول إلى النظام بالصدفة أو عن طريق الخطأ أو السهو، وكان على الشخص قطع وجوده أو انسحابه فوراً⁽³⁾، أو في حالة طبعه لنسخة من المعلومات في حين سمح بالرؤية فقط. فإنّه يعاقب على جريمة البقاء غير المشروع متى توافرت أركانها لا سيما منها الركن المعنوي. وقد يرتبط البقاء غير المشروع بالدخول غير المشروع، وذلك في الغرض الذي لا يكون فيه للجاني الحق في الدخول إلى النظام، ويدخل إليه فعلاً ضدّ إرادة من له حق السيطرة عليه⁽⁴⁾.

وعليه، توصف هذه الجريمة بأنّها سلوك مجرد أي إنّها تقع وتكتمل بمجرد الانتهاء من السلوك المكوّن لها وهو الدخول أو البقاء دون أن يتطلب المشروع في نموذجها القانوني أية نتيجة إجرامية⁽⁵⁾.

إلا أنّ الفقه لم يتفق حول ما إذا كانت هذه الجريمة وقتية أو مستمرة أو متتابعة الأفعال. غير أنّ الرأي الراجح اعتبر أنّ جريمة البقاء داخل النظام تبدأ منذ اللحظة التي يبدأ فيها الجاني التجول داخل النظام أو استمراره في التجول بداخله بعد انتهاء الوقت المحدّد. أمّا إذا بدأ في التجول فإنّ جريمة البقاء داخل النظام تبدأ منذ

(1) - سوير سفيان، نفس المرجع، ص 89.

(2) - حاجب هيام، المرجع السابق، ص 46.

(3) - زركي أحمد، المعلوماتية وجرائم الاعتداء على الأموال، مذكرة التخرج لنيل شهادة المدرسة العليا للقضاء، 2004-2007، ص 49.

(4) - قارة آمال، المرجع السابق، ص 110.

(5) - حاجب هيام، المرجع السابق، ص 47.

تلك اللحظة، وهذا ما يشكل الركن المادي لتلك الجريمة، بحيث يكون اعتبارها مستمرة أو وقتية ذات أثر ممتد بدون أثر⁽¹⁾.

وبخصوص تجريم هذا النوع من الاعتداء الإلكتروني فقد نصت عليه الاتفاقية الدولية للإجرام المعلوماتي لسنة 2001 على أنه: «يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50.000 دج إلى 100.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك، وتضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50.000 دج إلى 150.000 دج»⁽²⁾. وفي نفس السياق قرر المشرع الجزائري فرض عقوبات بالحبس والغرامة في المادة 394 مكرر/2 و3 من قانون العقوبات والتي نصت على أنه: «تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير المعطيات المنظومة».

وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50.000 دج إلى 150.000 دج».

وعليه، فإن ظرف التشديد هنا ظرف مادي يكفي أن توجد بينه وبين الجريمة الأساسية -الدخول أو البقاء غير المشروع⁽³⁾ - علاقة السببية للقول بتوافره، إلا إذا

(1) - انظر: علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للطباعة والنشر، بيروت، لبنان، 1999، ص 121.

(2) - انظر: علي عبد القادر القهوجي، المرجع نفسه، ص 135.

(3) - ومن بين جرائم الدخول أو البقاء لنظام معلوماتي الذي أدى إلى نحو النظام أو تدميره قيام مجموعة يطلق عليها "Action Direct" أتلفت برامج وملفات تخص شركة متخصصة في بيع الحاسبات الآلية وتوثيق المعلومات الحاسوبية وكان ذلك لحساب الشركات المنافسة. أضف إلى ذلك ظهور مجموعة تطلق على نفسها (Anonymous.dz) التي دمّرت وعبّثت بعدة مواقع الكترونية جزائرية وأجنبية. وللزيد من

أثبت الجاني انتفاء تلك العلاقة وأن تعديل أو محو المعطيات أو عدم صلاحية النظام بوظائفه يرجع إلى القوة القاهرة أو الحادث المفاجئ⁽¹⁾.

- الاعتداء العمدي على سير نظام المعالجة الآلية للمعطيات:

(Atteintes volontaires ou fonctionnement de STAD)

نصت مختلف التشريعات على حالة الاعتداء العمدي على سير نظام المعالجة الآلية للمعطيات، وهو ما نصت عليه المادتان 5 و 8 من الاتفاقية الدولية الإجرام المعلوماتي، إلا أنّ المشرع الجزائري لم يأت بنص خاص بالاعتداء العمدي على سير النظام واكتفي بالنص على الاعتداء على المعطيات الموجودة بداخل النظام⁽²⁾. الأمر الذي دفع الفقه للتفرقة بين الاعتداء على المعطيات والاعتداء على النظام. فإذا كان الاعتداء مجرد وسيلة فإن الفعل يشكل جريمة الاعتداء العمدي على النظام، أمّا إذا كان الاعتداء غاية فإن الفعل يشكل جريمة الاعتداء العمدي على المعطيات⁽³⁾.

ويتخذ الاعتداء العمدي عدّة صور من بينها:

- التعديل: الذي يقتضي وجود عمل إيجابي دون اشتراط أن يقتترن التعطيل بالعنف، وتمثل الوسيلة المادية في كسر الأجهزة المادية للنظام أو تحطيم الأسطوانة. أمّا عن الوسيلة المعنوية فهي التي تقع على الكيانات المنطقية للنظام كالبرامج والمعطيات، كأن يتم إدخال برنامج فيروسي، أو تعديل كلمة السر، أو جعل النظام يتباطأ في أدائه لوظائفه⁽⁴⁾.

التفاصيل راجع، عبد الفتاح بيومي حجازي، التجارة الالكترونية وحمايتها القانونية، ص 37.

(1) - انظر: قارة آمال، المرجع السابق، ص 114.

(2) - لقد اعتبر المشرع الجزائري أن برامج سير نظام المعالجة الآلية للمعطيات تدخل ضمن المعطيات المعلوماتية، راجع أحكام المادة 02 فقرة ج من قانون 04-09 السالف الإشارة إليه.

(3) - انظر: سوير سفيان، المرجع السابق، ص 92.

(4) - انظر: زريقي احمد، المرجع السابق، ص 52.

وعليه، فإنّ إعاقة سير النّظام هو "فعل يتسبب في تباطؤ أو ارتباك (Ralentissement) عمل نظام المعالجة، والذي يؤدي إلى تغيير (modification) في حالة عمل النظام⁽¹⁾."

-الإفساد: يجعل نظام المعالجة الآلية للمعطيات غير صالح للاستعمال السّليم، كأن يعطي نتائج غير تلك التي كان من الواجب الحصول عليها⁽²⁾. ومن وسائل التعيب أو الإفساد تقنية استخدام القنبلة المعلوماتية التي تدخل عن طريقها مجموعة معطيات تتكاثر داخل النظام تجعله غير صالح للاستعمال، كاستخدام البرامج المسمى «بحصان طروادة» والذي يقوم بتغيير في البرامج أو المعطيات⁽³⁾

وفي هذا السّياق جرّم المشرع الجزائري الاعتداءات العمدية على المعطيات إذ نص في المادة 394 مكرر 2 من قانون العقوبات على أنّه " يعاقب بالحبس من شهرين (02) إلى ثلاث (03) سنوات، وبغرامة من 1 000.000 إلى 5.000.000 دج كل من يقوم عمدا وعن طريق الغش بما يلي:

1. تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

2. حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها في إحدى الجرائم المنصوص عليها في هذا القسم: ويظهر أنّ المشرع الجزائري قد وسّع من مجال تجريم الأفعال التي ترد على المعطيات في المادة 394 مكرر 2/2 التي تجرم أفعال الحيازة، الإفشاء، النشر، الاستعمال أيا كان الغرض من هذه

(1) - انظر، شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الالكترونية، دار الجامعة الجديدة، الاسكندرية، مصر، 2007، ص 134.

(2) - انظر: عبد الفتاح بيومي حجازي، التجارة الالكترونية وحمايتها القانونية، ص 41.

(3) - انظر: علي عبد القادر القهوجي، المرجع السابق، ص 143.

الأفعال التي ترد على المعطيات المتحصل عليها من إحدى الجرائم الواردة في القسم السابع مكرر من قانون العقوبات بهدف المنافسة غير المشروعة، الجوسسة، الإرهاب⁽¹⁾.

وأما عن الركن المعنوي في مختلف الاعتداءات الماسة بالأنظمة المعلوماتية فيتمثل في صورة القصد الجنائي إضافة إلى نية الغش⁽²⁾.

ويتطلب الركن المعنوي لهذه الجريمة اتجاه إرادة الجاني إلى فعل الدخول أو إلى فعل البقاء وأن يعلم الجاني بأنه ليس له الحق في الدخول إلى النظام والبقاء فيه. وعليه، لا يتوافر الركن المعنوي إذا كان دخول الجاني أو بقاءه داخل النظام مسموح به أو مشروع. وتجدر الإشارة أن توافر القصد الجنائي بعنصره العلم والإرادة لا يتأثر بالباعث على الدخول فيبقى القصد قائماً حتى ولو كانت الباعث هو الفضول أو إثبات القدرة على المهارة والانتصار على النظام.

وعليه، فإن جريمة الاعتداءات على سير نظام المعالجة الآلية للمعطيات فإنها تعد بطبيعتها جريمة عمدية، إذ أنه من المفترض أن أفعال العرقلة والتعطيل تكون عمدية⁽³⁾. أضف إلى ذلك أن القصد الجنائي لا يعني ضرورة توافر قصد الإضرار بالغير، بل تتوافر الجريمة ويتحقق ركنها بمجرد فعل الإدخال أو المحور أو التعديل مع العلم بذلك واتجاه الإرادة إليه⁽⁴⁾.

(1) - انظر: حاجب هيام، المرجع السابق، ص 50.

(2) - انظر: خليفي مريم، الرهانات القانونية الالكترونية، رسالة دكتوراه في القانون الخاص، جامعة أبو بكر بلقايد-تلمسان-2011، ص 177.

(3) - انظر: محمد زلابي، حجة دليل الحاسوب الآلي في النطاق الجنائي، مجلة صادرة عن مخبر القانون الخاص الأساسي، جامعة أبو بكر بلقايد، تلمسان، العدد 07، 2010، ص 70.

(4) - انظر: علي عبد القادر القهواجي، المرجع السابق، ص 145.

المطلب الثاني: الجرائم الماسة بانتهاك سرّية وخصوصية البيانات الشخصية

يقصد بسرية البيانات في عقود التجارة الإلكترونية حصر المعلومات وعدم حركتها إلاّ في نطاق عدد محدود من الأشخاص، ومعنى الخصوصية هو ارتباط هذه البيانات بالمتعاقدين - بائع ومشتري أو منتج ومستهلك - وعدم اطلاع الغير عليها⁽¹⁾.

الفرع الأول: تجريم التعامل في بيانات التجارة الإلكترونية بدون ترخيص

تعرض عمليات التجارة الإلكترونية فيما يتعلق بتداول البيانات الكترونياً، باعتداء يتمثل في التعامل في البيانات بدون ترخيص، والترخيص من الجهات المختصة يناط بها منح التراخيص بالتعامل في هذه البيانات دون غيرها من الجهات. ويجب أن يتوافر لجرمة التعامل في بيانات التجارة الإلكترونية بدون ترخيص ركنين مادي ومعنوي⁽²⁾. يتحقق الركن المادي بمجرد التعامل في بيانات التجارة الإلكترونية بدون ترخيص من الجهة المختصة.

وقد اهتم قانون التجارة الإلكترونية والمبادلات التونسي المؤرخ في 9 أوت 2000 بهذه المسألة حيث نص في المادة 44 منه بأنّه: «يسحب الترخيص من مزود خدمات المصادقة الإلكترونية ويتم إيقاف نشاطه، إذا أخلّ بواجباته المنصوص عليها بهذا القانون أو بنصوص تطبيقية. وتؤول الوكالة الوطنية للمصادقة الإلكترونية سحب الترخيص بعد سماع المزود المعنى بالأمر»⁽³⁾.

أمّا بخصوص الركن المعنوي، فإنّ هذه الجريمة تقع بطريق العمد أو بطريقة الخطأ.

(1) - انظر: عبد الفتاح بيومي مجازي، التجارة الإلكترونية وحمايتها القانونية، ص 282.

(2) - انظر: خلفي مريم، المرجع السابق، ص 350.

(3) - انظر: عبد الفتاح بيومي مجازي، مقدمة في التجارة الإلكترونية العربية، دار الفكر الجامعي، الاسكندرية، مصر، 2003 ص 316.

فهي جريمة عمدية يكفي لتوافرها القصد الجنائي العام بعنصريه العام والإرادة. وتكون الجريمة غير عمدية عندما يخطأ الشخص في تداول البيانات بدون حصوله على الترخيص من الجهة المختصة⁽¹⁾.

الفرع الثاني: تجريم انتهاك سرية وخصوصية في البيانات في نطاق التجارة الإلكترونية

تأميناً لممارسة العملية التجارية يجب الحفاظ على سرية وخصوصية البيانات المعالجة إلكترونياً⁽²⁾ والتي يتم التعامل بها في نطاق التجارة الإلكترونية، ويلقى على عاتق نظام الأمن الخاص بحماية البيانات والمعلومات عيئ تأمين سريتها. وككل جريمة لا بد أن يتوافر في جريمة انتهاك سرية وخصوصية البيانات ركنها المادي والمعنوي. فالركن المادي يتحقق بمجرد انتهاك سرية البيانات وخصوصيتها حتى لو لم يترتب على الفعل أي نتيجة باعتبارها من جرائم السلوك المجرد أو جرائم الخطر العام. فلا يستوجب حصول الضرر حتى يعاقب الجاني على الفعل الذي ارتكبه لأن ذلك يضعف ثقة المتعاملين في التجارة الإلكترونية⁽³⁾.

أما الركن المعنوي فهو يتمثل في القصد الجنائي بعنصريه العلم والإرادة، ويتحقق ذلك متى سعى الجاني وانصرف لإرادته إلى فض مفاتيح التشفير الخاصة بالمعلومات والبيانات بما يخالف القانون.

وعليه، فإنه احتراماً للحق في الخصوصية، تسعى التشريعات إلى الاهتمام بموضوع البيانات المشفرة وذلك بتجريم كل فعل من شأنه انتهاك السرية والخصوصية، وإن كان التشفير ليس هو الوسيلة الوحيدة بل هناك وسائل فنية

(1) - انظر: خليفي مريم، المرجع السابق، ص 352.

(2) - تتضمن البيانات المعالجة إلكترونياً "مجموعة العمليات التي تتم آلياً أو باستخدام الحاسب الآلي، وتتعلق بالجمع، التسجيل، التعديل، الاحتفاظ ومحو المعلومات التي تتعلق بالتجارة الإلكترونية؛ علي عبد القادر قهوجي، الحماية الجنائية لبرامج الحاسب الآلي، المرجع السابق، ص 50.

(3) - Cf. J. LARRIEU, Droit de l'internet, Ellipses, Paris, 2005, p.64.

عديدة تتمثل في أنظمة الأمان المعلوماتي (1).

الفرع الثالث: تجريم التصريح عمداً بمعطيات خاطئة

يتجلى الهدف من هذه الجريمة هو حماية العملية التجارية وأطرافها من استقبال معلومات خاطئة تؤثر على حقوق أطراف التعاقد، ومن ثمّ تخلّ بثقة المستهلك والتي هي مفترضة في مجال التجارة الإلكترونية. فالمعلومات أو البيانات تلعب دوراً أساسياً في نجاح التجارة الإلكترونية وتزيد من نسبة رواجها.

وبخصوص الركن المادي لهذه الجريمة فيمكن القول أنّها من جرائم السلوك المجرد أو جرائم الخطر، وليست من جرائم الضرر. فالجريمة إذن تقتضي إعطاء معطيات غير صحيحة من جانب أي شخص الذي يتعين عليه الالتزام بصحة المعطيات التي صرح بها لثقة مورد الخدمة الإلكترونية، وكذلك الأطراف في توقيعه على غير ما صدر عنه (2).

وعلى سبيل المثال فإنّ المشرع التونسي يتطلب في المعطيات التي يتم الإدلاء بها، أن تكون خاطئة أي كاذبة، حيث يتم الإدلاء بها بهدف التأثير على عمل ونشاط مزود الخدمة الخاصّة بالتوثيق الإلكتروني، أو تصرف أحد أطراف العقد (3).

أمّا بخصوص الركن المعنوي فإنّ هذه الجريمة من الجرائم العمدية (4)، وصورة القصد فيها هو القصد الجنائي بعنصره العلم والإرادة (5).

(1) - انظر: أسامة أحمد بدر، حماية المستهلك في التعاقد الإلكتروني، دار الجامعة الجديدة، مصر، ص 196.

(2) - انظر: عبد الفتاح بيومي جازي، مقدمة في التجارة الإلكترونية العربية، ص 263.

(3) - انظر: عبد الفتاح بيومي جازي، التجارة الإلكترونية وحمايتها القانونية، ص 291.

(4) - تنص المادة 47 من قانون التجارة الإلكترونية والمبادلات التونسي المؤرخ في 9 أوت 2000 على أنّه: "يعاقب كل من صرح عمداً بمعطيات خاطئة...".

(5) - انظر: عبد الفتاح بيومي جازي، التجارة الإلكترونية وحمايتها القانونية، ص 293.

المطلب الثالث: الجرائم الماسة بالتوقيع الإلكتروني والبيانات المشفرة

تحدد القوة الثبوتية للتوقيع الإلكتروني إذا توافر فيه أمران : الأول استعمال وسيلة موثوق فيها والثاني أن يتوافر في المستند الإلكتروني شروط سلامته والمحدد وفقا لمرسوم المجلس الأوروبي⁽¹⁾.

الفرع الأول: جرائم الاعتداء على التوقيع الإلكتروني

تعتبر هذه الجريمة من الجرائم التي تقع على مضمون التجارة الإلكترونية، وليس على البيانات الخاصة بها، الأمر الذي يثير قلق الكثير من المستهلكين والمزودين. وعلى هذا الأساس ظهر اهتمام كبير للعديد من التشريعات الوضعية بخصوص التوقيع الإلكتروني كقانون التجارة الإلكترونية التونسي، وكذلك المشرع الجزائري الذي اعترف صراحة بالتوقيع الإلكتروني بموجب نص المادة 2/327 من القانون المدني⁽²⁾.

كما أكد التوجيه الأوروبي رقم 99/93 الصادر في 13 ديسمبر 1999 أن «التوقيع الإلكتروني معطيات تأخذ الشكل الإلكتروني، وترتبط بمعطيات أخرى إلكترونية وتستخدم كوسيلة لإثبات صحتها»⁽³⁾.

أولا: الدخول بطريق الغش على قاعدة بيانات تتعلق بالتوقيع الإلكتروني

تتضمن قاعدة البيانات والمعلومات المخزنة داخل الحاسب الآلي، أو على قرص منفصل كاليانات المتعلقة باسم صاحب التوقيع، ومهنته، وبياناته الشخصية، وكافة المعلومات المتعلقة بذلك التوقيع⁽⁴⁾.

(1) - انظر: شيماء عبد الغني محمد عطا الله، المرجع السابق، ص 411.

(2) - تنص المادة 327/2 على أنه "يعتد بالتوقيع الإلكتروني وفق الشروط المذكورة في المادة 323 مكرر1...". انظر القانون رقم 05-10 سالف الذكر.

(3) - Cf . Lionel. BOCHURBERG, 2ème edition, Delmas, Paris, 2001, p. 136.

(4) - انظر: عبد الفتاح بيومي حجازي، حماية المستهلك عبر شبكة الأنترنت، دار الكتب القانونية، مصر،

ويتحقق الركن المادي للجريمة عند الدخول إلى نظام معلومات أو قاعدة البيانات المتعلقة بالتوقيع الإلكتروني بطريق الغش والتدليس، الذي قد يؤدي إلى أضرار تتمثل في تدمير البرامج والبيانات، لأنّ هذه الجريمة ليست من جرائم الضرر، وإنما تصنف ضمن جرائم الخطر.

ويقصد بالغش أو التدليس المعلوماتي أن يكون الدخول إلى قاعدة البيانات مجرداً من المشروعية أي بدون إذن قضائي، أو ليس من قبل الأشخاص الذين لهم حق الاطلاع على هذا النظام.

أمّا الركن المعنوي لهذه الجريمة يتطلب توافر القصد الجنائي العام بعنصره العلم والإرادة، وذلك بأن يعلم الجاني بحقيقة سلوكه الإجرامي، وأن ذلك محظور بنص القانون، ومع ذلك تنصرف إرادته إلى السلوك الإجرامي⁽¹⁾.

ثانياً: جريمة صنع أو حيازة برنامج لإعداد توقيع الكتروني

محل الجريمة في هذه الحالة هو إعداد توقيع الكتروني دون موافقة صاحبه. أمّا الركن المادي لهذه الجريمة يتمثل في صور عديدة كصناعة نظام معلوماتي أو برنامج لإعداد توقيع إلكتروني، أو حيازة النظام أو البرنامج، ويستوي في هذا الغرض أن يكون الجاني من الأشخاص الطبيعية أو الاعتبارية.

وتجدر الإشارة أنّه لا عقاب على الشروع في العمل الإجرامي لأنّه من الأعمال التحضيرية، باعتبار أنّه لا عقاب على الشروع في الجنب إلاّ بنصّ خاص⁽²⁾.

أمّا الصورة الأخرى للركن المادي فتتضمن حيازة برنامج أو نظام معلوماتي

2008، ص 149.

(1) - للزيد من المعلومات، انظر: الجندي حسني، في شرح قانون قع التدليس والغش، دار النهضة العربية، القاهرة، 2000، ص 53.

(2) - انظر: عبد الفتاح بيومي جازي، التجارة الالكترونية وحمايتها القانونية، ص 300.

لإعداد توقيع الكتروني دون موافقة صاحبه، والحيازة المشروعة المرخص بها من الجهة المختصة لا عقاب عليها، وذلك بهدف توثيق هذه التوقيعات.

وصورة الركن المعنوي في هذه الجريمة هو القصد الجاني بعنصره العلم والإرادة، لأنّ الجريمة عمدية ولا يتصور قيامها بطريق الخطأ غير العمدي⁽¹⁾.

ثالثا: جريمة تزوير المحررات الإلكترونية والتوقيع الإلكتروني

إن جريمة التزوير في المجال المعلوماتي هي أخطر صور غش المعلوماتية⁽²⁾، وقد تضمنت توصية المجلس الأوروبي الخاصة بجرائم المعلوماتية الإشارة إلى جريمة التزوير المعلوماتي وإلى ضرورة تجريم استعمال المحرر المعلوماتي المزور.

وبالرجوع إلى التشريع الفرنسي، فإنّه شهد صدور قانون عقوبات جديد تضمن جريمة التزوير⁽³⁾، وبهذا أصبحت جريمة التزوير المعلوماتي ليس مجرد جريمة تقع على المستندات المعالجة آليا فقط، بل أصبحت جريمة تزوير المستندات المعلوماتية واستعمالها. وهذا بخلاف المشرع الجزائري الذي لم يتطرق إلى التزوير المعلوماتي كجريمة خاصة في تعديل 2006⁽⁴⁾.

ولقيام هذه الجريمة فإنّ الأمر يتطلب تحقق الركن المادي فيها الذي يأخذ صورا مختلفة تتمثل في تزوير أو تقليد محرر الكتروني أو توقيع الكتروني أو شهادة اعتماد توقيع الكتروني، أو استعمال محرر أو توقيع الكتروني مزور، أو شهادة مزورة باعتماد توقيع الكتروني⁽⁵⁾.

فلاعتداء على منتجات الإعلام الآلي يتجسد في فعل التزوير المعلوماتي الذي

(1) - انظر ما سيأتي تفصيلا بخصوص العقوبات المقررة في هذا المجال، ص من هذه الدراسة.

(2) - انظر: حاجب هيام، المرجع السابق، ص 54.

(3) - راجع نص المادة 1-441 من قانون العقوبات الفرنسي الصادر بموجب الأمر رقم 2000-916 بتاريخ 19 سبتمبر 2000.

(4) - Cf. Jacques LARRIEU, droit de l'internet, Ellyes, Paris, 2005, P.94.

(5) - انظر: عبد الفتاح بيومي مجازي، حماية المستهلك عبر شبكة الانترنت، ص 150.

نصت عليه المادة 7 من الاتفاقية الدولية للإجرام المعلوماتي لسنة 2001، كون أنّ التلاعب في المعطيات الذي نتج عنه معطيات غير أصلية يعد تزويراً⁽¹⁾.

وتجدر الملاحظة أنّ التغيير المشترط لقيام جريمة التزوير هو الذي ينصب على بطاقات الائتمان المغنطة: وفي هذا الصدد، اعتبر الفقه أنّ التغيرات المادية لبطاقة الائتمان كتغيير اسم الحامل أو الرقم الخاصّ بالبطاقة أو تاريخ انتهاء صلاحيتها يشكل تزويراً. وتجدر الملاحظة بأنّه من الضروري على المشرع الجزائري تحديد مفهوم المحرر الذي يكون محلاً لجريمة التزوير.

وبخصوص الركن المعنوي لهذه الجريمة فيتمثل في انصراف إرادة الجاني إلى تغيير الحقيقة في المحرر، واتجاه نيته إلى استعمال المحرر فيما زور من أجله.

الفرع الثاني: جرائم الاعتداء على البيانات المشفرة

وكما سبقت الإشارة إليه فإنّ تشفير البيانات يعني «التغيير في شكلها عن طريق تحويلها إلى رموز أو إشارات لحماية هذه البيانات من اطلاع الغير عليها أو تعديلها أو تغييرها».

وبما أنّ التوقيع الإلكتروني يتعرض لاعتداءات معلوماتية، فإنّ تشفير البيانات قد تكون عرضة للاعتداء باختراقها عن طريق فض الشفرة أو تسريبها من قبل من له حق الاحتفاظ بها، لذلك يتعين حمايتها جنائياً ضد هذه الاعتداءات.

أولاً: جريمة فض مفاتيح التشفير

يتحقق الركن المادي لهذه الجريمة في قيام الجاني بكشف مفاتيح التشفير أو بفك معلومات مشفرة محفوظة لدى مكتب التشفير، وكشف مفاتيح الشفرة يكون بتسليم برنامج الشفرة ذاته لمن ليس له حق في ذلك.

(1) - انظر: أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، ج2، جرائم الفساد، جرائم المال والأعمال، جرائم التزوير، الطبعة الثالثة، دار هومة، الجزائر، 2006، ص 336.

وعلى سبيل المثال يتم تشفير التوقيع الإلكتروني، بنظامين أحدهما يسمى النظام السيمتري وهو نوع من البرامج يعتمد الرموز الهندسية المعقدة، والآخر يسمى النظام البيومتري وهو يعتمد على مواصفات شخصية تتعلق بصاحب التوقيع ذاته⁽¹⁾.

- أما الصورة الثانية للركن المادي في هذه الجريمة، فهي فض المعلومات المشفرة في غير الأحوال المصرح بها قانوناً، كأن يقوم الجاني بفض شفرة بعض المعلومات وتسليمها لشركة منافسة، الأمر الذي يترتب عليه الإضرار بحق الشركة المجنى عليها⁽²⁾.

ويلاحظ على هذه الجريمة أنها من جرائم السلوك المجرد إذ لا يشترط ضرورة تحقق الضرر بالنسبة للمجني عليه من عملية فض الشفرة، لأن الضرر محقق الوقوع في المستقبل .

كما تعد هذه الجريمة من الجرائم العمدية التي تستلزم لقيامها توافر القصد الجنائي بعنصره العلم والإرادة⁽³⁾.

وعلى هذا الأساس جرم المشرع التونسي جريمة فض مفاتيح التشفير الإلكتروني في المادة 48 من قانون المبادلات والتجارة الإلكترونية لعام 2000. وبناءً على ذلك تقوم جريمة فض مفاتيح التشفير الإلكتروني عند قيام الجاني بفض مفاتيح التشفير المتعلقة بالتوقيع الإلكتروني وذلك بنقل التوقيع من صور مكتوبة إلى صور رقمية غير مفهومة⁽⁴⁾.

(1) - عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، ص 311.

(2) - محمد شكري سرور، التجارة الإلكترونية ومقتضيات حماية المستهلك، بحث مقدم إلى المؤتمر العلمي أكاديمية شرطة دبي، الإمارات العربية المتحدة 2003/2/26، الموقع الإلكتروني: www.kananaonline-com/users/ahmedkordy/posts/277936

(3) - خلفي مريم، المرجع السابق، ص 360.

(4) - عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، ص 319.

ثانياً: جريمة إذاعة واستعمال المحررات والتوقيعات الإلكترونية والشفرات دون مسوغ قانوني

يتعلق الركن المادي لهذه الجريمة بتسهيل أو إذاعة مضمون المحرر أو التوقيع الإلكتروني، وكذلك استعمالهما ولو في غير علانية وبدون رضا صاحبه، وإذا توافر الركن المادي للجريمة يتعين أن يقوم القصد الجنائي لدى الجاني بعنصره بوصفها جريمة عمدية⁽¹⁾.

وتجدر الإشارة في هذا الصدد على وجود جرائم أخرى لم يتم التعرض إليها كجريمة استغلال المتعامل في البيع الإلكتروني حيث عاقب المشرع التونسي كل من يستغل ضعف أو جهل المتعاقد في البيع الإلكتروني ودفعه إلى التعاقد عن ضعف أو جهل⁽²⁾. أما فيما يتعلق بجريمة اختراق (Hacking) البريد الإلكتروني وبطائق الائتمان، توجد طرق عديدة لاختراق البريد الإلكتروني سواء من قبل القراصنة الهواة hackers أو المخترقون crackers، بالاستيلاء على كلمة السر (password). ومن بين أحدث الطرق للاختراق قيام الشخص بالدخول إلى الموقع ووضع اسمه وكلمته السرية، فيقوم ذلك الموقع الكاذب بإرسالها إلى المخترق لأجل الاطلاع على الرسائل والعبث بها، وإرسال رسائل من بريد المخترق لتحقيق أغراضه الشخصية⁽³⁾. ومن بين الأمثلة الحية في هذا المجال قيام قراصنة باختراق موقع ياهو (yahoo)، وفي اسم الموقع تمت إضافة مكان 0 ليصبح الموقع yah0oo، فتم إرسال هذا الرابط لمجموعة من الأشخاص قصد الدخول إليها وبالتالي تم اختراق بريدهم الإلكتروني، أما الطريقة الثانية فهي تفجير الإيميل (Email) بإغراق البريد بالرسائل، وإرسال رسائل محملة بملفات ضخمة⁽⁴⁾.

(1) - كوثر سعيد عدنان، حماية المستهلك الإلكتروني، دار الجامعة الجديدة، الاسكندرية، مصر، 2012، ص 598.

(2) - للزيد من المعلومات انظر: خليفي مريم، المرجع السابق، ص 361.

(3) - مصطفى الفوري، الحماية القانونية والتقنية للتجارة الإلكترونية؛ الموقع الإلكتروني: www.MarocDroit.com

(4) - كوثر سعيد عدنان، حماية المستهلك الإلكتروني، دار الجامعة الجديدة، الاسكندرية، مصر، 2012،

وبخصوص قرصنة بطائق الائتمان (les cartes de credits) عن طريق محاكاة المواقع فيقوم الجاني بإنشاء موقع شبيه بالموقع الأصلي، ويقوم بتخفيض أثمان البضائع لأجل إغراء متصفح الموقع. فإذا تقدم المشتري لأجل شراء تلك البضائع يقوم بإدخال معلومات بطاقته الإلكترونية، ففي تلك اللحظة لا يجد مرحلة تنفيذ العقد، بل فقط صفحة بيضاء أو صفحة أخرى⁽¹⁾.

ومفاد هذه العملية أن تلك المعلومات قد تم إرسالها إلى القرصان، فيقوم بدوره بالتصرف فيها وشراء حاجاته الشخصية ببطاقة غيره. ومثال ذلك أنه في سنة 2009 قام مجموعة من الأشخاص بعمل صفحة على الأنترنت شبيهة بموقع (Ebay) برابط مزور هو (Ebay.com) وعدّلوا أثمان البضائع وجعلوها بخسة مما شجع المشتريين على القيام بعملية الشراء مما خلف خسائر تقدر بـ 40 مليون دولار أمريكي، نتيجة قيام القراصنة بإعادة التصرف في البيانات المدخلة للموقع المزيف من قبل القراصنة⁽²⁾.

وعلى هذا الأساس يمكن طرح التساؤل التالي: ما هي الجزاءات المقررة لحماية المستهلك وما مدى نجاعة آليات مواجهة الجرائم الإلكترونية في تحقيق أمن المستهلك الإلكتروني؟

الفرع الثالث: العقوبات المقررة في التشريعات الوضعية

لقد تعرضت التشريعات الوضعية لمسائل الإجرام المعلوماتي⁽³⁾ وإلى مختلف

ص 605.

(1) - شريف محمد غنام، حماية العلامة التجارية عبر الأنترنت في علاقتها بالعنوان الإلكتروني، دار الجامعة الجديدة، الإسكندرية، مصر، 2007، ص 102-103.

(2) - انظر: مصطفى الفوري، الحماية القانونية والتقنية للتجارة الإلكترونية، الموقع الإلكتروني www.MarocDroit.com ص 37.

(3) - في هذا الصدد راجع المادة رقم 1-323 من قانون العقوبات الفرنسي، والمعدلة بموجب القانون رقم 912-2015 والمؤرخ في 27 جويلية 2015.

الاعتداءات الماسة بالأنظمة المعلوماتية إذ خصّصت لها عقوبات ردعية سواء تعلق الأمر بالشخص الطبيعي أو الشخص المعنوي:

أولاً: التشريع المقارن

1- الجزاءات المتعلقة بجرائم المواقع الالكترونية:

لقد ساهمت التشريعات الدولية في إقرار عقوبات من شأنها منع أو التقليل من حدة الجرائم الإلكترونية، وفي هذا الإطار أكدت الاتفاقية الدولية للإجرام المعلوماتي على ضرورة تحقيق الردع بالنسبة لمرتكبي الجرائم المعلوماتية. فقد تضمنت عقوبات سالبة للحرية والمتمثلة في عقوبات أصلية وعقوبات تكميلية تطبق على الشخص الطبيعي⁽¹⁾، كما توجد عقوبات تطبق على الشخص المعنوي بناءً على تبني مبدأ مسؤولية الشخص المعنوي⁽²⁾.

ففيما يتعلق بالعقوبات المطبقة على الشخص الطبيعي يمكن تقسيمها إلى صنفين عقوبات أصلية وعقوبات تكميلية:

فبخصوص العقوبات الأصلية نص المشرع الفرنسي في المادة 1/323 من قانون العقوبات الفرنسي المعدل سنة 1994 على تجريم فعل الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للبيانات أو في جزء منه بالسجن لمدة عامين وغرامة قدرها 60000 يورو، وأيضا كل من أدى إلى حذف أو تعديل البيانات الموجودة في النظام، أو إعاقة سير عمل هذا النظام يعاقب بالسجن لمدة 3 سنوات وغرامة قدرها 100000 يورو⁽³⁾.

(1)- المادة 13 من الاتفاقية المؤرخة في 23 ديسمبر 2001 والمشار إليها سابقا.

(2)- المادة 12 من الاتفاقية السالف ذكرها.

(3)- وفي إطار استراتيجية الأمن الوطني والسياسة الدفاعية يضع رئيس الوزراء السياسة العامة وينسق العمل الحكومي في نظم المعلومات الأمنية والدفاعية، ولهذا الغرض تؤدي هيئة الأمن القومي لنظم المعلومات وظيفة الدفاع الوطني وسلطة أمن نظم المعلومات المعالجة آليا. انظر المادة: 1-L2321 والصادرة

عندما ترتكب الجرائم المنصوص عليها في الفقرتين المشار إليهما أعلاه ضد نظام المعالجة الآلية للبيانات الشخصية التي وضعتها الدولة، هو زيادة العقوبة بالسجن لمدة 5 سنوات و 150000 يورو غرامة⁽¹⁾.

أما المشرع الجزائري فقد نص في المادة 394 مكرر من قانون العقوبات الجزائري على عقوبة جريمة الدخول أو البقاء غير المشروع في صورته البسيطة بـ 3 أشهر إلى سنة حبس وغرامة من 50.000 دج إلى 100.000 دج.

أما فيما يتعلق بجريمة الدخول أو البقاء غير المشروع في نظام المعالجة الآلية في صورتها المشددة فقد نصت عليها المادة 323-2 من قانون العقوبات الفرنسي المعدل والمتمم بأنه إذا ارتكب أي جرم ضد نظام المعالجة الآلية للبيانات الشخصية التي وضعتها الدولة، يتم رفع العقوبة إلى سبع (7) سنوات سجن وغرامة قدرها 300000 يورو. وفي هذه النقطة التي تؤكد فكرة الردع في الجرائم الإلكترونية فقد سار المشرع الجزائري على نفس منوال المشرع الفرنسي إذ نص في المادة 394 مكرر الفقرتين 2 و3 على عقوبة الحبس من سنة (6) أشهر إلى سنين (2) وغرامة من 50.000 دج إلى 150000 دج إذا ترتب عن الدخول أو البقاء غير المشروع تخريب النظام⁽²⁾.

وفيما يخص جريمة إعاقة أو تحريف تشغيل نظم معالجة البيانات فإن المشرع الفرنسي قد جرم هذا السلوك في نص المادة 323/2 ويعاقب عليه بالحبس لمدة 3 سنوات وغرامة 300000 يورو لكل من قام بإعاقة أو إفساد تشغيل نظم معالجة البيانات. أما المشرع الجزائري فإنه لم يتطرق إلى هذه الجريمة بل نص على جريمة التلاعب في بيانات نظم معالجة المعطيات وعاقب عليها بالحبس من ستة أشهر إلى

بموجب القانون رقم 1168-2013 والمؤرخ في 18 ديسمبر 2013.

(1) - انظر قانون العقوبات الفرنسي الصادر سنة 1994، السالف ذكره.

(2) - انظر: القانون رقم 06-23 المؤرخ في 20 سبتمبر 2006، المعدل والمتمم لقانون العقوبات الجزائري، الصادر في ج.ر.ج.ج، عدد 84.

ثلاث سنوات وغرامة من 50000 دج إلى 200000 دج طبقا للمادة 394 مكرر¹.

ومن أجل مواجهة مرتكبي الجرائم الإلكترونية بكل صرامة تمّ اقرار عقوبات تكميلية تشمل وظيفته ومهنته لتمتد إلى المصادرة واغلاق الموقع.

وفي هذا السياق، قرر المشرع الفرنسي عقوبات تكميلية في نص المادة 323-5 التي تجيز حرمان الشخص من الحقوق السياسية والمدنية والعائلية مدة لا تتجاوز خمس سنوات، والحرمان من تقلد الوظائف العامة أو أي نشاط مهني⁽¹⁾.

ومن بين العقوبات الأخرى التي نص عليها المشرع الجزائري نجد:

- مصادرة الأجهزة والبرامج والوسائل المستخدمة في ارتكاب الجريمة مع مراعاة حقوق الغير حسن النية .

- إغلاق المواقع les sites التي تكون محلا لجريمة من الجرائم الماسة بالأنظمة المعلوماتية .

- إغلاق المحل أو مكان الاستغلال ومثال ذلك غلق المقهى الإلكتروني (cyber café) الذي ترتكب فيه مثل هذه الجرائم بشرط توافر عنصر العلم لدى مالكيها⁽²⁾.

وتجدر الملاحظة أنّ المشرع الجزائري ضاعف العقوبات تمشيا مع الظروف المشدّدة، إذا استهدفت الجرائم الماسة بالأنظمة المعلوماتية جريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام وذلك دون الإخلال بتطبيق عقوبات النشر⁽³⁾.

(1) - انظر: قانون العقوبات الفرنسي السالف ذكره.

(2) - انظر: المادة 394 مكرر 6 من قانون العقوبات الجزائري.

(3) - إبراهيمي سهام، المرجع السابق، ص 71.

هذا عن الشخص الطبيعي، أمّا الشخص المعنوي فقد تمّ إخضاعه للمساءلة الجنائية تفاديا لأي استغلال للوضع من قبل ممثليه. وفي هذا الصدد، نصّت المادة 12 من الاتفاقية الدولية للإجرام المعلوماتي، أنّ الشخص المعنوي يسأل عن هذه الجرائم سواء بصفته فاعلا أصليا أو شريكا، كما يسأل عن الجريمة التامة أو الشروع فيها بشرط أن تكون قد ارتكبت لحساب الشخص المعنوي⁽¹⁾. فالمسؤولية الجزائية للشخص المعنوي لا تستبعد المسؤولية الجزائية للأشخاص الطبيعيين بصفتهم فاعلين أو شركاء⁽²⁾.

وهو الطّرح الذي أكّده أيضا المشرع الجزائري الذي أقر بالمسؤولية الجزائية للشخص المعنوي من خلال المادة 18 مكرر⁽³⁾.

وكدليل على تشديد العقوبة في هذا المجال فقد تمّ تطبيق عقوبة الغرامة على الشخص المعنوي تعادل خمس مرّات الحدّ الأقصى للغرامة المطبّقة على الشخص الطبيعي⁽⁴⁾.

2- الجزاءات المرتبطة بجرائم انتهاك البيانات الشخصية:

من بين التشريعات الوضعية التي جرمت انتهاك البيانات الشخصية، المشرع التونسي الذي نص في المادة 52 قانون المبادلات الالكترونية لعام 2000 على أنّه: «يعاقب طبقا لأحكام الفصل 254 من المجلة الجنائية، مزود خدمات المصادقة الالكترونية وأعوانه الذين يفشون أو يحثون أو يشاركون في إفشاء المعلومات التي عهدت إليهم في إطار تعاظمي نشاط باستثناء تلك التي رخص بها صاحب الشهادة كتابيا أو الكترونيا في نشرها».

(1) - انظر الاتفاقية الصادرة بتاريخ 23/11/2001، السالف ذكرها.

(2) - سوير سفيان، المرجع السابق، ص 101.

(3) - راجع المادة 18 مكرر من قانون العقوبات الصادر في 20 ديسمبر 2006، سالف الذكر.

(4) - المادة 394 مكرر 4 من قانون العقوبات.

كما أنّه نص في المادة 47 من ذات القانون على معاقبة كل من صرّح عمداً بمعطيات خاطئة لمزود خدمات المصادقة الإلكترونية، بالسّجن لمدة تتراوح بين ستة أشهر وعامين وغرامة تتراوح بين ألف وعشرة آلاف دينار أو بإحدى هاتين العقوبتين⁽¹⁾.

3- الجزاءات المقررة بخصوص جرائم التوقيع الإلكتروني والبيانات المشفرة:

نصت المادة (26) من المشروع المصري على أنّه: «... يعاقب بالحبس وغرامة لا تقل عن 3000 جنيه أو بإحدى هاتين العقوبتين كل من دخل بطريق الغش أو التدليس على نظام معلومات أو قاعدة البيانات تتعلق بالتوقيعات الإلكترونية، ويعاقب بنفس العقوبة من اتصل أو أبقى الاتصال بنظام المعلومات، أو قاعدة البيانات بصورة غير مشروعة». وعليه، فيحقّ لمحكمة الموضوع أن تقضي بالحبس والغرامة معاً أو بأيّهما حسب ظروف الدعوى ذاتها⁽²⁾.

ونظراً لخطورة تقليد التوقيع الإلكتروني، لا سيما بالنسبة للمستهلك الذي يعتبر الطرف الضعيف في العقد الإلكتروني، فقد تمّ إقرار عقوبة الحبس وكذا الغرامة لمواجهة مثل هذه الأعمال. فعلى سبيل المثال نصت المادة "27" من المشروع المصري رقم 15 لسنة 2004 على معاقبة من صنع أو حاز برنامج لإعداد التوقيع الإلكتروني دون موافقة صاحبه بالحبس مدة لا تقل عن سنة وبغرامة لا تقل عن عشرة آلاف جنيه أو بإحدى هاتين العقوبتين⁽³⁾.

وفيما يتعلق بجريمة الاعتداء على البيانات المشفرة عاقب المشرع التونسي على فضّ مفاتيح التشفير بموجب نص المادة 48 والتي جاء فيها: «يعاقب كل من استعمل بصفة غير مشروعة عناصر تشفير شخصية متعلقة بإمضاء غيره بالسجن لمدة

(1) - انظر: انظر القانون التونسي الصادر سنة 2000 السالف ذكره.

(2) - خليفي مريم، المرجع السابق، ص 355.

(3) - انظر: مروك نصر الدين، الحماية الجنائية للتجارة الإلكترونية، مجلة الموسوعة القضائية الجزائية، العدد الثالث، بدون سنة نشر، ص 142.

تتراوح بين ستة أشهر وبخضية تتراوح بين ألف وعشرة ألف دينار أو بإحدى هاتين العقوبتين»⁽¹⁾.

يتضح من خلال دراسة تشريعات بعض الدول العربية والغربية بخصوص الجرائم الإلكترونية أنها أقرت حماية للمتعاملين مع الشبكة المعلوماتية العالمية من حيث تنوع العقوبات أصلية وتكميلية وكذا المعاقبة بالحبس والغرامة، وهذا إن دل على شيء فإنما يؤكد أسلوب الردع المتبع في مثل هذه الجرائم بغية تحقيق الثقة والائتمان في مجال التعاملات الإلكترونية ومن ثم تحقيق الأمن والاستقرار للمستهلك الإلكتروني كونه الطرف الضعيف في هذه العمليات المهمة والخطيرة⁽²⁾.

ثانيا: موقف القضاء

تجدر الإشارة في هذا الصدد إلى أهمية بعض الأحكام القضائية المشهورة بخصوص الجرائم الإلكترونية كونها تشكل الإطار التطبيقي للعمليات الافتراضية عبر النت.

- قضية **Hancock.V.State** (هانكوك ضد الدولة) لسنة 1966، وهي أول قضية تعرضت لموضوع إساءة استخدام الحاسبات الآلية بصفة عامة، وفي الولايات المتحدة بصفة خاصة. وتتلخص هذه القضية في اتفاق مبرمج للحاسبات بإحدى الشركات مع صديق له يعمل بشركة أخرى على أن يقوم الأول بطبع المعلومات التي يحتوي عليها 89 قرصا مجانا، وتسليمها إلى الشركة الأخرى في مقابل 5 ملايين دولار، وفي أثناء التسليم تم القبض على المتهم بتهمة السرقة⁽³⁾.

ومن بين القضايا التي عرضت على القضاء يمكن ذكر على سبيل المثال قضية

(1) - انظر: القانون التونسي الصادر سنة 2000 السالف ذكره.

(2) - عبد الفتاح حجازي، التجارة الالكترونية وحمايتها القانونية، ص 315.

(3) - انظر: زرقى أحمد، المعلوماتية وجرائم الاعتداء على الأموال، مذكرة لنيل شهادة المدرسة العليا للقضاء، 2004-2007، ص 66.

Word v. Superior court (ورد ضد المحكمة العليا) سنة 1976 بولاية كاليفورنيا والتي ثبت فيها قيام المتهم بإعطاء تعليمات إلى الحاسب الآلي لكي يقوم بطباعة نسخة من برنامج معقد يخص الشركة ويتعلق ببعض الرسوم البيانية، وقد قام المتهم بهذا الفعل بناءً على طلب شركة أخرى منافسة. وأثناء المحاكمة تمت إدانته بتهمة سرقة المعلومات التي احتوى عليها البرنامج. قضية أخرى تتعلق بإتلاف المعلومات هي قضية R.V. whitely (وايتلي) والتي تلتخص وقائها في قيام المتهم بالدخول قيد المصريح به إلى شبكة المعلومات "Janet"، ثم قام بنحو وإضافة بعض الملفات، وتغيير بعض الشفرات⁽¹⁾.

أما قضية Morris. V. United (موريس ضد الاتحاد) فتتمثل في قيام طالب أمريكي يدعى Morris بإعاقه أكثر من ستة 06 آلاف حاسب آلي عن العمل من بينها حاسبات آلية خاصة بوكالة الفضاء الأمريكي (NASA). وقد اتهمته المحكمة بالدخول العمدي غير المصرح به إلى الحاسب الآلي والسبب في خسارة قدرت بأكثر من ألف دولار، وأدانته المحكمة طبقاً للفقرة 5 من المادة 1030 (A) من القانون الفيدرالي الخاص بجرائم الحاسب الآلي لعام 1982⁽²⁾ computer abuse (amendment Act).

وأخيراً يمكن الإشارة إلى قضية تعتبر نموذجاً لمخاطر جرائم تخريب الكمبيوتر وهي قضية شركة أوميغا إذ قام مصمم ومبرمج شبكات الكمبيوتر ورئيس سابق لشركة (Oméga) من مدينة (Delmare)، ويدعى (Timothy Allen lioyd)، تم اعتقاله في 1998/02/17 بسبب إطلاقه قبلة الكترونية في عام 1996، بعد 20 يوماً من فصله من العمل استطاعت أن تلغي كافة التصاميم وبرامج الإنتاج لأحد كبرى مصانع التقنية العالية في نيوجرسي، ملحقاً خسائر بلغت 10 مليون دولار⁽³⁾.

(1) - نقلاً عن: شريف محمد غنام، المرجع السابق، ص 182-183.

(2) - نقلاً عن: زرقى أحمد، المرجع السابق، ص 68.

(3) - نقلاً عن: زرقى أحمد، المرجع نفسه، ص 70.

أما بخصوص الجرائم الإلكترونية الواقعة في الوطن العربي ومنها الجزائر فقد عالجت مصالح الدرك الوطني 21 قضية متعلقة بالجرائم المعلوماتية على مستوى 48 ولاية خلال 9 أشهر الأخيرة، حيث نتصدر جرائم المساس بالحريات الشخصية عن طريق الفايبروك والتوتير مجموع القضايا المعالجة. وحسب ما كشف عنه من قرصنة للمواقع الإلكترونية تورط دكتور وباحث علمي بجامعة قلمة والذي تسبب في المساس بالملكية الفكرية لـ 44 باحثا علميا، حيث قام بسرقة الرقم السري للبريد الإلكتروني الخاص برئيس مخبر بحوث العلوم والتكنولوجيا وتلاعب بأسرار الباحثين وحاول أن يشعل فتيل الفتنة بين الباحثين الجزائريين والمغاربة⁽¹⁾.

هذه القضية التي تعتبر الأولى من نوعها وفكّت خيوطها بمركز الوقاية من جرائم الإعلام الآلي وجرائم المعلوماتية ومكافحتها، التابع للدرك الوطني، تعود إلى شهر نوفمبر من سنة الفارطة، وبعد أن تم جمع الدلائل والأدلة التي تدين المتهم تم استدعاؤه إلى مقر الفصيلة الإقليمية للدرك الوطني وتم إخضاعه للرقابة القضائية في انتظار استكمال الإجراءات القانونية.

وما يمكن التنويه إليه في هذا المجال أيضا ما تعرضت إليه أهم المواقع الرسمية الإسرائيلية لحملة قرصنة من طرف قراصنة عرب حيث تم قرصنة موقع الشرطة الإسرائيلي ووضع آيات من القرآن الكريم في ذات الموقع. وفي السياق ذاته تم اختراق عدة مواقع حكومية إسرائيلية من طرف مجموعة (Danger haker) التي كشفت أنها اخترقت أكثر من 1500 موقع إسرائيلي، وعلى إثرها تكبدت إسرائيل خسائر كبيرة تعد بملايير الدولارات، خاصة بعد أن تم اختراق مواقع بنوك إسرائيلية وتحويل بعض الأموال منها، بالإضافة إلى تعطيل مواقع حكومية وأخرى خاصة⁽²⁾.

(1) - للاطلاع على وقائع القضية، انظر: محمد الفاتح خويجي، دكتور بجامعة قلمة وراء القضبان، جريدة الشروق اليومية بتاريخ 1 مارس 2013، العدد 3957، ص 05.

(2) - للاطلاع على وقائع القضية، انظر: أيوب أمزيان، قراصنة عرب يخترقون مواقع رسمية إسرائيلية

الخاتمة:

إنّ الوسائل المستعملة في التعاقد الإلكتروني والمتمثلة في التكنولوجيا الحديثة في عالم الحواسب الآلية، هي التي تفرض وجوب استحداث حماية إضافية وخاصة للمستهلك الإلكتروني من شأنها حمايته باعتباره الطرف الضعيف في هذا النوع من العقود، الذي زاد من اتساع عدم التوازن العقدي الذي ظهر مع ظهور عقود الاستهلاك.

فموضوع حماية المستهلك الإلكتروني لا يمسّ المستهلك وحده فقط، بل يتعلق بالتطور الاقتصادي. الأمر الذي يزيد من حرية المنافسة سواء الداخلية أو الخارجية، والتي كثيرا ما تكون ضدّ مصلحة المستهلك حسب التنوع في السلع والخدمات المعروضة عليه والاهتمام بجانب الربح على حساب صحة وسلامة المستهلك عن طريق عمليات الغش والاحتيال الممارسة عليه.

ومن جملة ما تمّ التوصل إليه من خلال هذه الدراسة هو أنّ الحماية القانونية للعقود الإلكترونية في جانبها الجنائي يتعلق أساسا بحماية المستهلك كمتعامل بالتجارة في شكلها المستحدث.

وقد حاول الفقه والقضاء تطويع هذه القواعد الكلاسيكية لنصوص القانون الجنائي لتطبيقها في مجال حماية المعلوماتية، لكن الواقع كشف عن ضرورة تدخل تشريعي خاص بإيجاد أنظمة قانونية جديدة تستوعب هذه الظواهر الحديثة. وعلى هذا الأساس اتجهت أغلب التشريعات المقارنة الى محاولة سدّ الفراغ التشريعي بتجريم العديد من الأفعال الماسة بالنظم المعلوماتية كالقانون الفرنسي الذي عدّل نص التجريم الخاص بجريمة التزوير التقليدية على نحو شمل نطاقها معه المستند الإلكتروني واستحدث تشريع لحماية بطاقة الائتمان وكذلك الشأن بالنسبة للتشريع الألماني الذي أضاف إلى باب التزوير نصوصا خاصة بتزوير المستند الإلكتروني.

ويكبدون الصهانية خسائر بالملايير، جريدة النهار اليومية بتاريخ 08 أفريل 2013، العدد 1677، ص 24.

وقد جاءت النصوص القانونية المتبناة من قبل المشرع الأوروبي في مجال مسؤولية وسطاء الانترنت بنظام قانوني متوازن وملائم لطبيعة العمل على الانترنت ولتحدد بالنتيجة التزامات كل مستخدم الشبكة والقائمين على إدارتها من متعهدي الإيواء، والأحكام الخاصة بكل منهم.

ونظرا لخطورة هذه الجرائم بات حتميا على الهيئات والمنظمات والمجالس الدولية أن تلعب دورا مهما في محاولة ترسيخ وجوب التعاون الدولي لمواجهة هذه الجرائم بهدف الحد من انتشارها وتعاضم آثارها، من خلال المساعدة القضائية الدولية وتسليم المجرمين، والتوسع في عقد الاتفاقيات الدولية للاستفادة من نظام الإنابة القضائية وتبادل المعلومات في المجال المعلوماتي لتفادي مشكلة البحث عن الدليل الرقمي خارج حدود الدول.