الحماية الجنائية لنظم المعالجة الآلية للمعطيات في التشريع الجزائري*

د. حمودي ناصر
قسم القانون العام،
كليّة الحقوق والعلوم السياسية،
جامعة آكلي محند أولحاج – البويرة

Dr. HAMMOUDI Nacer
Département de Droit Public,
Faculté de Droit et des Sciences Politiques,
Université Akli Mohand Oulhadj - Bouira

الملخص:

ظهور الإنترنت وما صاحبها من تطورات تكنولوجية رقمية مذهلة، وانتشارها وتطورها ودخولها مختلف مناحي الحياة، لدرجة أن أضحت إحدى مفردات التعامل اليومي بالنسبة للأفراد والمجتمعات على حد سواء، الاستفادة القصوى من مزايا يتطلب توفير حماية قانونية فعالة لها، تضفي الشرعية الحجية على التعاملات التي تتم من خلالها، وتواجه سوء استخدامها، وكذا حمايتها من كل الاعتداءات التي قد تكون عرضة لها.

ولأنّ التعامل عبر الإنترنت يتطلب اتخاذ مواقع إلكترونية عليها، والتي بدورها تحتاج إلى بناء وإنشاء وبرمجة نظم للمعالجة الآلية للمعطيات، فإنّه لا يمكن تصور إضفاء حماية قانونية فعلية وفعالة على التعاملات التي تتم عبر الإنترنت، وحمايتها من الاعتداءات التي يمكن أن تكون عرضة لها، ومحاربة سوء استخداماتها، إلا بإضفاء حماية جنائية موضوعية على النظم المعلوماتية التي تعدّ العصب الأساس في استغلال محاسن الثورة المعلوماتية.

الكلمات المفتاحية:

الثورة المعلوماتية، الجريمة المعلوماتية، نظم المعالجة الآلية للمعطيات، المساس بأنظمة المعالجة الآلية للمعطيات.

* تمّ استلام المقال بتاريخ 2014/01/05 وتمّ تحكيمه بتاريخ 2014/09/04 وقُبل للنّشر بتاريخ 2016/11/27.

Criminal protection of automated data processing Systems in Algerian law

Abstract:

The accession of internet was accompanied by a dazzling and unprecedented development in the field of information and communications technologies.

Issues related to the use of internet and its many tools, are considerable. It is not enough to know the risks; one must determine their real presence in a specific activity. To adequately supervise users, one must understand the activities and assess the issues.

In using the tools of internet and the systems of automated data processing, it is not enough to impose prohibitions and punish so that the respect for others is the order of the day and that such systems are protected.

In almost all cases, the person is master of what he does or does not do on internet. Therefore, the best way to ensure respect for the people, property and laws remains the criminalization of such infringements, without neglecting awareness, and training and education. And protect them from attacks that could be vulnerable to them, and fight the bad uses, but by giving objective criminal protection of information systems, which are key nerve to exploit the virtues of the information revolution.

Key words:

Computer revolution, automated data processing, computer offence, infringement of the automated data processing systems.

La protection pénale des systèmes de traitement automatisé des données en droit algérien

Résumé :

L'avènement de l'Internet était accompagné par un développement fulgurant et sans précédant dans le domaine des technologies de l'information et de la communication.

Les enjeux liés à l'utilisation d'Internet et de ses nombreux outils sont considérables. Ce n'est pas tout de connaitre les risques, encore faut-il déterminer leur présence réelle dans une activité spécifique. Pour encadrer adéquatement les usagers, il faut comprendre ces activités et en évaluer les enjeux.

Dans l'utilisation des outils de l'Internet et des systèmes de traitement automatisé des données, il ne suffit pas d'imposer des interdits et de sévir pour que le respect des autres soit au rendez-vous, et que ces systèmes soient protégés.

Dans la quasi-totalité des cas, l'individu est maître de ce qu'il fait ou ne fait pas sur Internet. C'est pourquoi, le meilleur chemin pour assurer le respect des personnes, des biens et des lois, demeure l'incrimination de ces atteintes, sans pour autant négliger, la sensibilisation, la formation et l'éducation.

Mots clés :

Révolution informatique, traitement automatisé de données, infraction informatique.

مقدمـة

مع التطورات التكنولوجية التي أفرزتها الثورة المعلوماتية، والتي فاقت كل خيال، ومع استعمالاتها التي أضحت إحدى مفردات الحياة اليومية للأفراد والمجتمعات، التي شكلت لهم عالما افتراضيا رقميا جديدا انفرد بمصطلحاته ومفاهيمه وآثاره، كانت لها الكثير من الانعكاسات القانونية على مختلف فروع القانون، إلا أنها طرحت تحديات كبيرة للقانون الجنائي. إذ أول ما أثارته من جدل فقهي ونقاش قانوني، كان بخصوص مدى قدرة القانون الجنائي بمد هذا العالم بالحماية الجنائية الفعالة، باعتباره الـقانون الذي يوفر مثل هذه الحماية كلما عجزت باقي فروع القانون الأخرى على حماية نفسها.

حتى وإن تم ضبط الكثير من المضامين وتحديد الكثير من الأبعاد القانونية المختلفة للعالم الافتراضي، سيما على مستوى النواحي المدنية والتجارية، بوضع قوانين خاصة مستحدثة، أو بإجراء بعض التعديلات والتطويعات للقواعد التقليدية. غير أن الإشكال الكبير الذي ظل ولا يزال مطروحا، يتعلق أساسا بمسألة الحماية الجنائية لأهم النظم المعلوماتية التي يقوم عليها العالم الافتراضي. خاصة وأن قانون العقوبات ألف الثبات والاستقرار، إلا أن التطورات المعلوماتية المتسارعة فاجأته بسرعة تحولاتها الرقمية، وبات السؤال مطروحا بخصوص أثر هذه التحولات على قدرة هذا القانون ومدى كفاية قواعده على مد النظم المعلوماتية بالحماية الجنائية الفعالة والكافية؟ أم أن الأمر يحتاج –مثلما احتاج في فروع القانون الأخرى- إلى التعديل والتطويع والملائمة، أم الأمر أعقد من ذلك بكثير ويحتاج إلى إحداث ثورة تشريعية جنائية حديثة؟

لذا بات موضوع الحماية الجنائية لنظم للمعالجة الآلية للمعلومات، من أكثر الموضوعات التي أثارت التشكيك في قدرة القواعد الجنائية التقليدية وما إن كانت ستظل هذه القواعد حاضرة وقادرة على مسايرة واقع الثورة المعلوماتية وما أفرزته من تحديات إجرامية حديثة، سميت بدورها بالإجرام المعلوماتي. الذي استدعى في بعض الحالات ضرورة التوصل لحلول غير تقليدية لموضوع مستحدث ذو تداعيات قانونية جنائية غير مسبوقة. ولعل ذلك راجع بالأساس لأهم الأسباب التالية:

أولا/النظم المعلوماتية مفهوم حديث وتطبيق تقني جديد: التطورات التكنولوجية غيرت كثيرا من المفاهيم القانونية التقليدية، وأدخلتنا في عصر العولمة وتدويل والرقمنة[1]، بوجود بيئة رقمية افتراضية، أزالت المسافات وتلاشت معها الحدود. الأمر الذي أحدث انقلابا حقيقيا وكبيرا على المفاهيم الجنائية التقليدية، وطرح السؤال حول قدرتها على التأقلم مع هذا التحول، أم عجزها عن ذلك، وما إن كان يتعين هجرها والبحث عن بدائل قانونية حديثة تواكب التطورات التقنية وما أفرزته من نظم معلوماتية لازمة للتعامل مع هذا الوسط الحديث.

ثانيا/مفاهيم مستحدثة تستدعي حلولا قانونية مبتكرة: البعد التقني الحديث للنظم المعلوماتية، غير الكثير من المفاهيم القانونية التقليدية وأحل مفاهيم أخرى محلها. هي مفاهيم لم يكن لرجل القانون معرفة بها إلى وقت قريب من الزمن،خاصة بحلول دعائم إلكترونية رقمية أوجبت الاعتراف بها وإضفاء الحجية القانونية عليها[2]، مما آثار في الوقت ذاته مسألة حمايتها جنائيا[3]. خاصة بعد أن أخذت الطابع الدولي[4]، باعتبارها تتم عبر شبكة دولية مفتوحة ترفض الاعتراف بالحدود وتأبى الخضوع لمفاهيم السيطرة والملكية. الأمر الذي أعجز أهم أحكام القانون الجنائي المتعلقة بالاختصاص المبنية على فكرة الحدود والإقليمية[5]. في حين أن الإنترنت ليست ملكا لأية جهة ولا يسيطر عليها أحد[6]، أضعفت كثيرا المبادئ الجنائية التي كانت متجذرة في السيادة الإقليمية للدولة. وكان لزاما أن يواكب التطورات المعلوماتية الجديدة، تطورات في المتطلبات القانونية، وتجاوز قصور القواعد القانونية الجنائية التقليدية، لمواجهة ظواهر إجرامية مستجدة، سميت عموما بالإجرام المعلوماتي أو الإلكتروني أو الرقمي.

ثالثا/ظاهرة إجرامية مستجدة تتطلب مواجهة مستحدثة: النظم المعلوماتية للإنترنت التي شكلت موضوعا قانونيا جديدا للحماية، صاحبتها ظـواهر إجـرامية معلوماتية حـديثة تتم عبر أساليب إجرامية جديدة لم تألفها مبادئ القانون الجنائي التقليدي. ظواهر إجرامية حديثة مستجدة تتمتع بذات خصائص التقنية متجاهلة طرق المواجهة الجنائية التقليدية، وتفاديا لفكرة الفراغ التشريعي الذي يتيح إفلات الكثير من المجرمين من العقاب[7]، تعين لبحث عن أساليب مستحدثة للمواجهة.

خاصة وأن النظم المعلوماتية أساليب تقنية وضعت لكي يتم من خلالها تبادل المعلومات المعالجة إلكترونيا، التي أضحت بدورها موضوعا للجريمة المعلوماتية، هي والنظم التي تعالجها، الأمر الذي حتم إعادة التفكير وإعادة صياغة المفاهيم الجنائية التقليدية لأجل مواجهة ظاهرة الإجرام المعلوماتي بتطوير الظاهرة القانونية.

وما زاد من خطورة هذا النوع من الجرائم، أنها انصبت على قيم معنوية لا تلمسها الأيدي ولا تبصرها الأعين، تتخطى حدود المكان في ظل انفتاح شبكة الإنترنت وتجاهلها للحدود الجغرافية للدول. وزادها تعقيدا؛ أنها جرائم ترتكب من قبل أشخاص من أصحاب المعارف والمهارات الفنية، وفي الغالب من المتخصصين في مجال المعلوماتية، وعلى قدر عال من الاحتراف[8]. يضاف لذلك خفاء الجريمة المعلوماتية كونها تتم عبر نبضات إلكترونية لا تجيد قراءتها سوى برامج الكمبيوتر[9]، كل ذلك في ظل غياب الكفاءات العالية وانعدام الخبرة لدى الأجهزة الأمنية والقضائية[10].

رابعا/وجوب مقابلة تطور الفكر الإجرامي بتطور في الفكر القانوني: ظهور الإنترنت وما أسفرت عنه من ظهور ظاهرة الإجرام المعلوماتي. يستدعي بالضرورة مواجهة جنائية جديدة[11]. كونه إجرام يقوم على انتهاك المواقع المعلوماتية وسرقة بياناتها وأموالها الإلكترونية. ووجوب أن يكون هناك تطور مواز ومواكب في الإطار القانوني[12]. خاصة في ظل واقع المعلوماتية يتسم بالحركية والتحول الدائمين[13]. وظهور الحاجة إلى الحماية الجنائية للنظم المعلوماتية والبيانات التي تتداول عبرها[14].

هذه الحماية الجنائية؛ في شقيها الموضوعي والإجرائي. كانت باستحداث نصوص حديثة من قبل المشرع الجزائري، مستفيدا في ذلك ببعض التجارب الدولية والإقليمية، مثلما هو الشأن بالنسبة لاتفاقية بوادبست، والتي بالرغم من كونها اتفاقية أوروبية، إلا أن طابعها وتوجهها عالميين[15]. كما وجد تجربة أخرى على المستوى العربي، وهي تجربة وضع القانون العربي النموذجي أو الاسترشادي الذي يعد عملا مشتركا بين مجلس وزراء الداخلية والعدل العرب، في نطاق الأمانة العامة لجامعة الدول العربية في شأن مكافحة جرائم تقنية المعلومات، الذي تم إقراره في 21 و22 ماي 2003 [16].

أما على مستوى تجارب الدول، نجد التجربة الفرنسية هي الأكثر ثراء وتوجيها للمشرع الجزائري، سيما وأن المشرع الفرنسي من بين المشرعين الذين اهتموا منذ البداية بمواجهة هذا النوع من الجرائم بقوانين خاصة، وبالكثير من التشريعات والتعديلات[17]. وبالتالي بادر المشرع الجزائري بتعديل قانون العقوبات بموجب القانون 04-15 المؤرخ في 10-11-2004 الذي أفرد القسم السابع مكرر من قانون العقوبات لهذا النوع من الجرائم تحت عنوان" المساس بأنظمة المعالجة الآلية للمعطيات" ضمن ثمانية مواد. وبعده بسنتين قام من جديد بإدخال تعديل آخر على قانون العقوبات، بموجب القانون رقم 06-23 المؤرخ في 20-12-2006. وهو التعديل الذي مس القسم المتعلق بالجرائم المعلوماتية، لكن في جانب العقوبة دون جانب التجريم. أما بخصوص الشق الإجرائي، فقام بتعديل قانون الإجراءات الجزائية، بموجب قانون رقم 04-14 مؤرخ في 10-11-2004 الذي من خلاله عامل الجرائم المعلوماتية مع جرائم أخرى بعض المعاملة الخاصة والاستثنائية خروجا عن القواعد العامة[18].

غير أنه أمام الخطورة المتزايدة لهذا النوع من الجرائم، وإدراكا من المشرع الجزائري بضرورة تعزيز الحماية الجنائية لنظم المعالجة الآلية للمعطيات، اضطر مرة أخرى للتدخل، وذلك بموجب القانون رقم 06-22 المؤرخ في 20-12-2006 معاملا هذا النوع من الجرائم معاملة خاصة، حيث أدرج تقنيات خاصة للمواجهة. غير أنه ارتأى مرة أخرى أن ذلك غير كاف، فاضطر مرة ثالثة إلى التدخل، لكن هذه المرة بموجب قانون خاص مستقل، وهو القانون رقم 09-04 مؤرخ في 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتـــصال ومكافحتها[19].

غير أن دراستنا في هذا المقال، سترتكز فقط على الجوانب الموضوعية للحماية الجنائية المقررة للنظم المعلوماتية في التشريع الجزائري، دون الجوانب الإجرائية لهذه الحماية. خاصة وأن الجانبين حديثين ويتضمنان العديد من التفاصيل المتوجب التطرق لدراستها، الإلمام بها كلها لا يتسع له المقام. لذا نأمل أن نوفق في دراسة الجوانب الموضوعية في هذا المقام، على أن يمكننا الله بعونه من تناول الجوانب الإجرائية في مقال آخر.

الهدف من هذه الدراسة؛ هو دراسة أهم الجرائم التي استحدثها المشرع الجزائري بموجب التعديل الذي أدخله على قانون العقوبات سنة 2004، كونه تعديل أضفى الحماية الجنائية على النظم المعلوماتية وما تحتويه من بيانات ومعلومات ومعطيات، محاولين قدر الإمكان الإحاطة بجميع أشكال الجرائم المعلوماتية التي يمكن أن تقع في أية بيئة إلكترونية[20]. محاولين التركيز على تبيان مدى قدرة هذا التعديل على مواجهة الإجرام المعلوماتي وبالتالي تكريس حماية جنائية فعالة للنظم المعلوماتية.

المبحث الأول:جريمة الدخول أو البقاء غير المصرح به داخل نظام المعالجة الآلية للمعطيات

جريمة الدخول غير المشروع لنظم المعالجة الآلية للمعلومات[21]، من أهم الظواهر الإجرامية التي أسفرت عنها التطورات التكنولوجية[22]، وهي وإن كانت جريمة شكلية، غير أنه في الغالب ما يرتبط بالدخول ارتكاب جرائم أخرى مادية. لذا عاقب المشرع على مجرد الدخول لنظم المعالجة الآلية للمعطيات تفاديا للتمادي في الاعتداءات على النظم وما تحتويه من معلومات[23]. وشدد العقوبات في حالة ما إذا ترتب على فعل الاختراق نتيجة مادية ما، تتمثل في الإضرار بالمعلومات أو بنظم معالجتها. وذلك بموجب نص المادة 394 مكرر المقابلة لنص المادة 313-1 من قانون العقوبات الفرنسي. والمادة 2 من اتفاقية بودابست[24]. وسنحاول تفصيل أركان هذه الجريمة من خلال المطالب التالي تناولها.

المطلب الأول:الركن المادي لجريمة الدخول أو البقاء غير المصرح به داخل النظام

باستقراء نص المادة 394 مكرر من قانون العقوبات الجزائري، يتضح لنا بأن الركن المادي لهذه الجريمة، يتحقق بإتيان سلوك يتمثل في صورة الدخول لنظم المعالجة الآلية للمعطيات أو البقاء فيها. غير أن بعض الفقه نجده يشترط بدون سند في القانون أن تكون هذه النظم مؤمنة بإجراءات فنية[25]. عكس البعض الآخر الذي لا يرى ضرورة لذلك - وهو الرأي الغالب [26]-. غير أننا وبدون الخوض في هذا الجدل، نرى أن المشرع الجزائري لم يتطلب ذلك. لذا سنتناول باختصار من خلال ثلاث فروع، دراسة عناصر الركن المادي لهذه الجريمة.

الفرع الأول:السلوك الجرمي لجريمة الدخول لنظام المعالجة الآلية للمعلومات

تتطلب كل من جريمتي الدخول للنظم المعلوماتية أو البقاء فيها، سلوكا أو نشاطا جرميا معينا، يتخذ صورتين، صورة الدخول وصورة البقاء؛ فعل الدخول يتطلب بداهة سلوكا إيجابيا، بينما فعل البقاء يتحقق بسلوك إيجابي عن طريق الترك أو الامتناع. وسنتناول صورتي السلوك الجرمي في النقطتين التاليتين.

أولا/الدخول غير المصرح به: الدخول "غير المصرح به" أو " عن طريق الغش" [27]، لنظم المعالجة الآلية للمعطيات، يعد دخولا معنويا، يستدعي أولا البحث عن معناه وعن متى يكون دخولا غير مصرحا به، وما الغش الذي يتم به؟ وهل يكفي الدخول وحده أم هناك أفعالا أخرى سابقة عنه يشترط إتيانها ؟ أم أن مجرد الدخول كاف لوحده للتدخل بالعقاب؟ وهي التساؤلات التي سنحاول الإجابة عنها في النقاط التالية:

1-مفهوم الدخول غير المصرح به : الدخول غير المصرح به، يستمد عدم مشروعيته من كونه غير مصرح به وتم دون رضاء من صاحب هذا النظام أو رغما عنه[28]. سواء كان الدخول لكل النظام أو لجزء منه فقط، وفي كلتا الحالتين نكون بصدد دخول معنوي لا يتم بالطرق التقليدية[29]. لذا نجد تعدد محاولات الفقه في تحديد معناه[30]، وهي محاولات ركزت جميعها على أنه ولوج بالطرق المعلوماتية ذو مدلول معنوي يشبه الدخول في ذاكرة الإنسان، ومدلول آخر مادي يتمثل في أن الشخص يكون قد حاول الدخول أو دخل بالفعل إلى النظام المعلوماتي [31]. له دلالتان: دلالة المكان وهو التسلل لداخل النظام المعلوماتي، ودلالة زمانية وتتمثل في تجاوز وقت وحدود التصريح أو الترخيص بالدخول، إن وجد مثل هذا التصريح[32].

ونجد المشرع الجزائري أسوة بالمشرع الفرنسي، قد صاغ النص بطريقة تشمل جميع طرق الدخول الممكنة، دون تحديد طريقة أو وسيلة بعينها. مما يمكن من مواجهة جميع اشكال الاختراق غير المشروع للنظم المعلوماتية. مع الإشارة أن هذه الجريمة تعد جريمة وقتية لها آثارا مستمرة، وفي ذات الوقت جريمة شكلية لا يتطلب فيها تحقق ضرر معين، كما لا يشترط فيها صفة معينة في الشخص الذي قام بهذا الدخول.

2- مفهوم عدم التصريح بالدخول : التصريح بالدخول يثير مسألتين هامتين، هما: من المسؤول عن إعطاء التصريح، وما هي حدود هذا التصريح وحالاته؟ بخصوص المسألة

الأولى، فإن التصريح يجب أن يمنحه الشخص المسؤول أو المسيطر أو المالك لتنظيم النظام المعلوماتي. وإن كان للنظام أكثر من مسؤول واحد، فهنا يكون لكل منهم الحق في منح التصريح. لذا فالجريمة التي نحن بصدد دراستها، تقوم في الحالة التي لا يكون هناك فيها تصريح بالدخول بتاتا، أو أن يوجد تصريح بالدخول، ولكن المصرح له يقوم بتجاوز الحدود التي رسمت له في هذا التصريح. سواء من حيث الوقت المخصص له أو من حيث تجاوز الغرض الذي لأجله منح الترخيص.

ثانيا/البقاء غير المصرح به: الصورة الثانية من صور السلوك الإجرامي للجريمة التي نحن بصدد دراستها، هي البقاء غير المصرح به في النظام. لذا سنحاول تناول المقصود بالبقاء غير المصرح به. ومن ثم النظر ما إن كان البقاء متلازما مع الدخول، أم أن كل منهما جريمة مستقلة.

1-المقصود بالبقاء غير المصرح به: لم يتطرق المشرع الجزائري ولا المشرع الفرنسي لمعنى البقاء، لذا نجد الفقه قد تصدى لبحث هذه المسألة، وتعددت تعريفاته[33]، غير أنها في مجملها تركز على أن البقاء هو أن يكون الجاني قد دخل النظام عن طريق الصدفة أو الخطأ، ومن بعدها يقرر البقاء داخله وعدم قطع الاتصال به[34]. وبالتالي هي جريمة سلوك إيجابي يتحقق بالترك أو الامتناع. كما أنها جريمة مستمرة.

2-مدى ضرورة التلازم بين فعلي البقاء والدخول: البقاء يتكون أصلا من فعلين؛ أن يكون هناك دخول والفعل الثاني وهو البقاء بعد هذا الدخول، أي أن تتجه إرادة الجاني إلى عدم قطع الاتصال بالرغم من علمه أنه داخل نظام ممنوع عليه الدخول إليه. لكن استعمال المشرع لمصطلحي الدخول والبقاء معا، يعني أن كل دخول غير مصرح به يترتب عليه بقاء غير مشروع. لكننا نرى أن كل جريمة مستقلة عن الأخرى، ولكل منهما سلوكها الخاص، خاصة وأنه سبق القول أن إحداهما جريمة مؤقتة والأخرى جريمة مستمرة، وبالتالي فهما من طبيعتين مختلفتين.

الفرع الثاني:محل النشاط الجرمي

هدف المشرع الجزائري من خلال المادة 394 مكرر، لإضفاء حماية جنائية فعالة لنظم المعالجة الآلية للمعطيات. أي حماية النظام ذاته، أيا كانت مكوناته، مادية أو

معنوية، وسواء كان ذلك بصفة جزئية أو بصفة كلية، وأيا كانت المعلومات التي يتضمنها النظام أو يتم تبادلها من خلاله.

أولا/نظم المعالجة الآلية للمعطيات:عرفت نظم المعلومات بأنها: " مجموعة الإجراءات التي تقوم بتجميع ومعالجة وتخزين وتوزيع المعلومات بهدف دعم عمليات صنع القرار"[35]. أو:" عبارة عن آلية وإجراءات منظمة تسمح بتجميع وتصنيف وفرز البيانات ومعالجتها ومن ثم تحويلها إلى معلومات يسترجعها الإنسان عند الحاجة، ليتمكن من إنجاز عمل أو اتخاذ قـــــــرار أو القيام بأية وظيفة عن طريق المعرفة التي سيحصل عليها من المعلومات المسترجعة من النظام"[36]. وعرف المشرع الجزائري، بموجب الفقرة (ب) من المادة 2 من القانون رقم 09-04 المتضمن القواعد الخاصة المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، نظام المعلومات بأنه:" أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة يقوم واحد منها أو أكثر بمعالجة آلية لمعطيات تنفيذا لبرنامج معين". ونرى أنه تم التركيز على فكرة " المعالجة الآلية "، التي يقصد بها مجموعة من العمليات المترابطة والمتسلسلة، التي تخضع لها معالجة المعطيات[37].

ثانيا/المعطيات:المعطيات ووفقا للمادة 2 الفقرة (ج) من القانون 09-04 السابق الذكر، هي :" 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". أي هي عبارة عن حقائق رقمية أو غير رقمية، وهي تختلف عن المعلومات التي تعتبر كل نتيجة مترتبة على تشغيل المعطيات أو تحليلها أو استقراء دلالتها واستنتاج ما يمكن استنتاجه منها[38]. ومن هنا نجد بأن الحماية الجنائية مكرسة للنظم المعلوماتية وما تحتويه من بيانات ومعطيات.

الفرع الثالث:النتيجة الإجرامية

بالرجوع لنص المادة 394 مكرر، نجد المشرع قد عاقب على فعلي الدخول والبقاء المجردين للنظم المعلوماتية، دون اشتراط أن يترتب عن ذلك تحقق نتيجة معينة. وبالتالي نحن بصدد جريمة شكلية هدف من خلالها المشرع حماية النظم المعلوماتية ذاتها دون المعلومات التي تحتويها. وإن حدث وأن يترتب عن فعل الدخـــول أو البقاء أثر

معين ضار كالتعطيل أو التخريب أو التدمير، فالمشرع هنا جعل هذا الأثر نتيجة جرمية تحول الجريمة من مجرد جريمة شكلية إلى جريمة مادية. وواجه المشرع الجزائري ذلك بالفقرتين الثانية والثالثة من المادة 394 مكرر، فنجد الفقرة الثانية من هذه المادة شددت العقاب في حال المساس بالمعطيات، إذ نصت بأنه:" ... تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة...". في حين نصت الفقرة الثالثة من ذات المادة، على أنه:" ... وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة...". ونرى هنا أن المشرع الجزائري قد اعتد ببعض النتائج فقط التي شدد بتحققها العقوبة، دون كل النتائج الأخرى. وهو ما نبينه في النقطتين التاليتين:

أولا/حذف أو تغيير المعلومات التي يحتويها النظام:بحسب الفقرة الثانية من المادة 394 مكرر، إذا ترتب عن الدخول غير المشروع للنظام، حذف في المعطيات أو إزالتها، أو إحداث تعديلات أو تغييرات فيها دون حذفها، يتم تشديد العقاب. وهي جريمة غير التي وردت بنص المادة 394 مكرر1 المتعلقة بجريمة التلاعب بالمعلومات، التي تعد جريمة مستقلة سنبين أركانها فيما بعد، وليست مجرد نتيجة يترتب عليها مضاعفة العقاب.

ثانيا/تخريب نظام المعالجة الآلية للمعطيات:وهي النتيجة التي تضمنتها الفقرة الثالثة من المادة 394 مكرر. ويقصد بتخريب النظام جعله غير قابل للاستخدام أو للاستعمال، وهي النتيجة الأخطر جسامة التي يمكن تصور إحداثها بالنظام، خاصة وأن تخريب النظام يعني ضمنا اعتداء على كل المعطيات التي يحتويها. وهنا نجد بأن المشرع الجزائري لم يبين موقفه من النتائج الأخف من ذلك، كمجرد التعطيل أو الإفساد الجزئي للنظام. ونرى أنه كان من الأجدر العقاب على كل فعل من شأنه جعل النظام يؤدي وظائفه على غير النحو الذي وجد لأجله. حتى يمكن مواجهة كل الأضرار التي قد تصيب النظم المعلوماتية.

المطلب الثاني:الركن المعنوي للجريمة

تعتبر جريمة الدخول أو البقاء غير المصرح به، جريمة عمدية. حيث استعمل المشرع الجزائري عبارة " عن طريق الغش"، واشتراط أن تكون هذه الجريمة عمدية أمر بديهي، كون الواقع اليومي يكشف أن الكثير من عمليات الدخول لنظم المعالجة الآلية للمعطيات والبقاء فيها عمليات روتينية تتكرر بشكل كبير في اليوم الواحد، لذا لو لم

تكن هذه الجريمة عمدية لوقع الملايين من حسني النية تحت طائلة العقاب. غير أن ما تجدر الإشارة إليه أن اشتراط القصد من قبل المشرع هو في صورتي الجريمة البسيطة، غير أن الأمر ليس كذلك في صورتها المشددة المبينة في المادة 394 مكرر 1 وهو ما نبينه في الفرعين التاليين.

الفرع الأول:الركن المعنوي للجريمة في صورتها البسيطة

جريمة الدخول أو البقاء بطريق الغش، من الجرائم العمدية التي يتطلب قصدا عاما بعنصريه العلم والإرادة: عنصر العلم؛ هو وجوب أن يعلم الجاني أن فعله ينصب على نظام معالجة آلية للمعطيات، وأنه ليس له الحق في الدخول إليه أو البقاء فيه، وبالتالي إذا انتفى العلم بذلك انتفى القصد[39]. وعنصر الإرادة؛ التي يجب أن تنصرف للسلوك فقط دون النتيجة، كون القانون لا يشترط في هذه الجريمة نتيجة معينة، وبالتالي لا يشترط إرادتها. لكن هناك قوانين تتطلب توفر قصد خاص أيضا، يتمثل في الغرض من ارتكاب هذه الجريمة، كغرض السرقة أو التهديد أو النصب، وهو موقف المشرع الإنجليزي في قانون إساءة استخدام الحاسبات الآلية لسنة 1990. في حين هناك قوانين تشترط أن يكون الغرض هو الحصول على فائدة أو ربح للجاني أو لغيره، مثلما هو الشأن بالنسبة للقانون البرتغالي لسنة 1991 الخاص بالجرائم المعلوماتية[40].

الفرع الثاني:الركن المعنوي للجريمة في صورتها المشددة

عكس الصورة السابقة، نجد المشرع الجزائري في نص المادة 394 مكرر 1 من تقنين العقوبات الجزائري، قد استعمل مصطلح الغش فقط مع فعل الإدخال. معتبرا أن الإدخال لا يمكن إلا أن يقع عمدا، عكس الحذف والتغيير اللذين لا يمكن أن يقعا إلا عن طريق الخطأ. وبالتالي فهذه الجريمة من جرائم الإهمال، مجرد ارتكاب فعلها المادي يعد كافيا لقيام الجريمة، إلا إذا استطاع الجاني إثبات وجود قوة قاهرة أدت إلى وقوعها[41]. فإذا قصد الجاني تحقيق النتيجة المشددة يطبق عليه نص المادة 394 مكرر 1 من قانون العقوبات وليس نص المادة 394 مكرر. أما بالنسبة لظرف التشديد المتعلق بتخريب نظام المعالجة الآلية الذي نصت عليه الفقرة الثالثة من نص المادة 394 مكرر، فهو يتعلق بنتيجة قد تقع في القانون الفرنسي كظرف تشديد غير مقصود، المنصوص والمعاقب عليه بنص المادة 323-1 من قانون العقوبات الفرنسي، أو كجريمة

خاصة مقصودة هي جريمة إعاقة أو إفساد نظام المعالجة الآلية (Atteint volontaire au fonctionnement d'un système de traitement automatisé) المنصوص والمعاقب عليها بالمادة 323-2 [42].

المبحث الثاني:جريمة التلاعب غير المصرح به بالمعلومات

بعد أن جرم المشرع الجزائري فعلي الدخول والبقاء بطريق الغش لنظم المعالجة الآلية للمعطيات، قام بتجريم فعل التلاعب غير المصرح به بالمعلومات التي تتضمنها نظم المعالجة الآلية. وهي جريمة مستقلة تضمنها نص المادة 394 مكرر 1 التي عاقبت عن كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها. حاميا بذلك المعلومات بكافة أنواعها وشاملا أيضا لكل وسائل التلاعب دون أن يميز بين وسيلة وأخرى. والعقاب على التلاعب يكون متى كان مقصودا. وسنتناول ركني هذه الجريمة تباعا في المطلبين التاليين.

المطلب الأول:الركن المادي لجريمة التلاعب غير المصرح به بالمعلومات

يتبين من نص المادة 394 مكرر1 من تقنين العقوبات الجزائري، المقابلة لنص المادة 323-3 من تقنين العقوبات الفرنسي، ونص المادة 4 من اتفاقية بودابست، أن الركن المادي لجريمة التلاعب غير المصرح به بالمعلومات، يتم بسلوك يمكن أن يتخذ صورة الإدخال أو التعديل أو المحو، وهي الصور التي نتناولها في فرع أول. وأن يرد هذا السلوك على محل معين، وهو المعلومات التي يتضمنها نظام المعالجة الآلية للمعطيات. وهو ما نبينه في الفرع الثاني. على أن يحقق نتيجة معينة، تتمثل في تغيير الحالة التي تكون عليها المعلومات في نظام المعالجة الآلية للمعطيات، وهو ما نبينه في الفرع الثالث.

الفرع الأول:النشاط الجرمي لجريمة التلاعب غير المصرح به بالمعلومات

بين المشرع الجزائري في نص المادة 394 مكرر1 ، ثلاثة صور لهذا السلوك الإجرامي الذي تقوم به الجريمة التي نحن بصدد دراستها. وهي الصور التي تمكن من مواجهة مختلف أشكال الاعتداء على المعلومات وهي: (الإدخال أو التعديل أو الإزالة)، وتكفي أية صورة من هذه الصور الثلاث لقيام السلوك الجرمي.

أولا/فعل الإدخال:فعل الإدخال بحسب البعض[43]، هو تغذية النظام بمعلومات أو إضافة خصائص ممغنطة جديدة في الدعامة الموجودة...[44]. وبالتالي الإدخال فعل

يتحقق بكل حالات تغذية النظام المعلوماتي بمعلومات مغلوطة أو خبيثة – الفيروسات-، أو غير صحيحة، أو إدخال معلومات صحيحة غير مصرح بإدخالها [45].

ثانيا/فعل التعديل:التعديل يتعين أن يكون بطريق الغش، ويعني تغيير المعلومات داخل النظام واستبدالها بمعلومات أخرى[46]، أي تغيير غير مشروع للمعلومات والبرامج، أو إمداد النظام بمعلومات مغايرة تؤدي إلى نتنائج مغايرة عن تلك التي صمم البرنامج لأجلها[47].

ثالثا/فعل الإزالة:الإزالة تعني التدمير، الإضرار، الإتلاف، المحو، الطمس... وكلها تعني اقتطاع خصائص البيانات والمعطيات عن طريق محوها أو عن طريق طمسها، أو ضغط خصائص أخرى فوقها. وهي مرحلة لاحقة على مرحلة إدخال المعلومات، حيث أن الإزالة تفترض الوجود السابق لعملية الإدخال[48].

الفرع الثاني:محل النشاط الجرمي

محل هذه الجريمة؛ هي المعلومات التي سبقت معالجتها آليا، والتي تكون متضمنة داخل النظام، وبمفهوم المخالفة، فإن المعلومات غير المعالجة التي لم تدخل إلى النظام، فهي خارج نطاق الحماية الجنائية المقررة بنص هذه المادة[49]. وذلك يستخلص من استعمال نص المادة 394 مكرر 1 ما يفيد بأن تكون المعلومات متضمنة بداخل النظام حيث استعمل عبارة " المعطيات التي يتضمنها".

الفرع الثالث:النتيجة الإجرامية

جريمة التلاعب بالمعلومات، تشترط وقوع ضرر فعلي على هذه المعلومات، ألا وهو تغيير حالتها، وذلك من خلال الإزالة أو التعديل أو المحو. وبالتالي هي من الجرائم المادية ذات النتيجة، وليست مجرد جريمة شكلية.

المطلب الثاني:الركن المعنوي لجريمة التلاعب غير المصرح به بالمعلومات

جريمة التلاعب بالمعلومات، وأيا كانت صورة السلوك المتخذ فيها، هي جريمة عمدية يتخذ فيها الركن المعنوي صورة القصد الجنائي العام. غير أنه مثلما جرت العادة، يثير الفقه مسألة ما إن كانت تشترط بالإضافة إلى ذلك قصدا جنائيا خاصا بالإضافة إلى القصد الجنائي العام. وهو ما يجعلنا نتناول هذا المطلب ضمن فرعين.

الفرع الأول:القصد الجنائي العام

جريمة التلاعب بالمعلومات من الجرائم العمدية، تتطلب القصد الجنائي العام الذي يقوم على علم الجاني بأنه يقوم بإحدى الأفعال التي جرمها النص القانوني، وأن من شأن أفعاله أن تؤدي إلى النتيجة المجرمة المتمثلة في التعديل أو الإزالة أو المـــحو، أو أن يقبل بحدوثها، وذلك تطبيقا للقواعد العامة دون الحاجة للنص عليها. غير أن الفقه وحتى في غياب النص الصريح أثار جدلا واسعا بخصوص مدى وجوب توفر قصد جنائي خاص حتى تقوم هذه الجريمة، وهو ما نتناوله ضمن الفرع الثاني.

الفرع الثاني:مدى وجوب توفر القصد الجرمي الخاص

من بناء المادة 394 مكرر1 ومن خلال مصطلح " الغش" الذي استعمله المشرع نستنتج أن الأخير اشترط أن تكون الجريمة عمدية [50]. وهو ذات الوضع في نص المادة 3-323 من تقنين العقوبات الفرنسي، وما استقر عليه القضاء الفرنسي وكرسه في العديد من أحكامه، منها النقض الجنائي في 08-12- 1999 [51]. وبالتالي هذه الجريمة لا تتطلب أي قصد خاص[52]. لكن هناك قوانين أخرى مثل القانون البرتغالي والفلندي والتركي تشترط قصدا خاصا لهذه الجريمة، وهو نية تحقيق الربح، الأمر الذي كان محل انتقادات فقهية كبيرة- لا يتسع المقام لها-[53]. ما يهمنا أن المشرع الجزائري لم يشترط صراحة القصد الجنائي الخاص.

المبحث الثالث:جريمة التعامل في معلومات غير مشروعة

بعد أن توجهت الحماية الجنائية التي قررها المشرع الجزائري إلى نظم المعالجة الآلية للمعلومات في الجريمة الأولى، وهي حماية النظام ذاته من الدخول أو البقاء غير المصرح بهما. اتجهت حمايته للمعلومات ذاتها التي يتضمنها النظام؛ فقام بتجريم أفعال التلاعب والإزالة والمحو فيها. ليقوم في هذه الجريمة بتجريم جملة من الأفعال التي تتعرض لها المعلومات أيضا. حيث عاقبت الفقرة الأولى من المادة 394 مكرر 2 على :" ... 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"، وهو ذات المعنى الذي ورد بالمادة 1/3-323 من تقنين العقوبات الفرنسي[54]. وسنفصل في أركان هذه الجريمة من خلال ماسيلي.

المطلب الأول:الركن المادي لجريمة التعامل غير المشروع في المعلومات

لهذه الجريمة صورتين كلاهما تنحصر في مجرد السلوك المجرم، دون تطلب أية نتيجة. بمعنى أنهما صورتين لجريمتين شكليتين. فيكفي للعقاب مجرد قيام الفاعل بأحد الأفعال المبينة بنص المادة 394 مكرر 2، دون اعتبار لأي نتيجة منظورا إليها ماديا. وأن ترد على محل معين. وهو ما نبينه في الفرعين التاليين.

الفرع الأول:النشـاط الجرمي لجريمة التعامل غير المشرع في المعلومات

تقوم هذه الجريمة على التعامل في معلومات صالحة لارتكاب جريمة من الجرائم التي سبقت دراستها، أو التعامل في معلومات متحصلة منها. وهي كلها صورا شكلية تقع وتكتمل بمجرد اكتمال الفعل دون تطلب نتيجة معينة [55]. لكنهما صورتين تنطويان على العديد من الأفعال لتي نتناولها في النقاط التالية.

أولا/التعامل في معلومات صالحة لارتكاب جريمة: التعامل في المعطيات فعل ينطوي على العديد من الأفعال والأعمال والعمليات السابقة على استعمال المعلومات، مثل تصميمها وبحثها وتجميعها، وصولا إلى توفيرها أو نشرها أو الاتجار فيها، ويكفي أيا منها لقيام السلوك المادي للجريمة. وسنبين معنى هذه الأفعال فيما يلي.

1-التصميـم: هو إعداد معلومات صالحة لارتكاب الجريمة، في العادة ما يقوم به أشخاص مختصين كمصممي البرامج، مثل تصميم الفيروسات أو برامج تمكن من الوصول لنظم المعالجة الآلية للمعطيات[56].

2-البـحث: البحث؛ فعل يقصد به البحث عن كيفية تصميم المعلومات وإعدادها، وليس مجرد البحث عنها، أي البحث عن المعلومات من أجل تصميمها لأغراض تجريمية[57]. مثل البحث عن الشفرات والبيانات التي تمكن من الاستيلاء على التوقيع الإلكتروني للشخص أو فك شفرات تعاملاته المالية الإلكترونية.

3-التجميـع: هو فعل يتمثل في القيام بجمع قدر كبير من المعلومات، يمكن أن ترتكب بها إحدى جرائم الاعتداء على نظم المعالجة الآلية للمعطيات[58].

4-التوفيـر: يقصد به عرض المعلومات وإتاحتها وجعلها في متناول الغير وتحت تصرفه وحيازته. مثل كلمات أو شفرات المرور التي تسمح بالولوج لجزء من النظام أو كله.

5-النشـــر: هو إذاعة المعلومات محل الجريمة وتمكين الغير من الاطلاع عليها، مهما كانت طبيعة هذه المعلومات[59]. ويرى البعض[60]، أن النشر يعد من أخطر الأفعال كونه يعني نقل هذه المعلومات إلى أكبر قدر ممكن من الأشخاص.

6-الاتجـــار : الاتجار؛ يعني تقديم المعلومات للغير بمقابل أيا كان نوع هذا المقابل. على عكس التوفير الذي قد يكون بدون مقابل. غير أنه للاتجار في مجالنا معنى يستوعب مختلف التعاملات التي يمكن تصور وقوعها على المعلومات، سواء كان ذلك بقابل أو بدون مقابل[61]. وهو ما يمكن من القضاء على الجرائم في المهد[62].

ثانيا/التعامل في معلومات متحصلة من جريمة: أفرد المشرع الجزائري صورة ثانية من صور التعامل في معلومات غير مشروعة، تتمثل في التعامل في معلومات متحصلة من جريمة، وذلك بفعل من الأفعال التي حصرتها الفقرة الثانية من المادة 394 مكرر 2 وهي الحيازة، الإفشاء، النشر والاستعمال، وهو ما لم ينظمه لا القانون الفرنسي ولا اتفاقية بودابست، وتقوم الجريمة بأي فعل من الأفعال التي نتناول تبيان معناها باختصار:

1- الحيـازة : حيازة المعلومات المتحصلة من إحدى الجرائم السابقة فعل غير مشروع، يعاقب من يحوزها، سواء كان ذلك بصفة دائمة أو بصفة مؤقتة[63]. ويمكن تشبيه هذه الجريمة بجريمة حيازة أشياء متحصل عليها من جنحة أو جناية، أو جنحة إخفاء أشياء مسروقة المعروفة في النصوص التقليدية لجرائم الأموال.

2- الإفشـاء: وهو إفشاء معلومات يكون قد تم الحصول عليها بارتكاب جريمة من جرائم الاعتداء على نظم المعالجة الآلية للمعطيات السابق تبيانها. وهو فعل يفترض انتقال المعلومات من حيازة الجاني إلى غيره من الأشخاص.

3- النشـــر: النشر شأنه شأن الإفشاء يعني اختراق للنظم المعلوماتية، والحصول على المعلومات منها ومن ثمة القيام بإفشائها، أيا كانت وسيلة هذا الإفشاء.

4- الاستعمـال: استعمال المعلومات المتحصل عليها بطريق غير مشروع فعل مجرم، أيا كانت نوعية هذا الاستعمال والغرض منه، رغبة من المشرع غلق الباب أمام أي استعمال معلومات متحصل عليها بطرق مجرمة[64].

الفرع الثاني:محل النشاط الجرمي

بموجب المادة 394 مكرر2 من تقنين العقوبات الجزائري، تم تجريم التلاعب في معلومات غير مشروعة، وبذلك تم إضفاء حماية جنائية واسعة للبيانات والمعطيات، سواء كانت في طور المعالجة، أو التخزين أو الإرسال. وهو حال غالبية البيانات والمعطيات التي تتم عبر النظم المعلوماتية.

الفرع الثالث:النتيجة الجرمية

جريمة التلاعب غير المشروع بالمعلومات من الجرائم الشكلية التي لم يتطلب فيها المشرع الجزائري تحقق نتيجة معينة منظورا إليها بمنظور مادي، رغبة منه في وقف هذه الجرائم عند مرحلة الخطر دون انتظار ترتيبها الضرر. وهو نوع من الحماية التي لا يقررها المشرع إلا للمصالح البالغة الأهمية، ومنها المعلومات[65]. وبالتالي هي جريمة شكلية تقوم على مجرد السلوك دون اشتراط نتيجة معينة.

المطلب الثاني:الركن المعنوي لجريمة التعامل في معلومات غير المشروع

نص المادة 394 مكرر من تقنين العقوبات الجزائري، تميز باستخدام المشرع الجزائري لعبارة: " عمدا" و " بطريق الغش"، عكس الجرائم السابقة أين اكتفى بمصطلح " عن طريق الغش"، وهو المصطلح الذي جعل البعض يرى أن استعماله من قبل المشرع الجزائري الغرض منه تطلب قصد خاص يضاف للقصد العام[66]. لذا سنحاول من خلال فرعين تناول القصد العام لهذه الجريمة في الأول، لنخصص الثاني لمسألة ما إن كانت هذه الجريمة تشترط قصدا جنائيا خاصا.

الفرع الأول:القصد الجنائي العام

تقوم جريمة التعامل في معلومات غير مشروعة على القصد الجنائي العام بعنصريه العلم والإرادة،. فالجاني يجب أن يكون يحيط علما بكافة العناصر التي تدخل في تكوين الجريمة، أهمها علمه بأنه يتعامل في معلومات غير مشروعة، وأن هذا التعامل قد يستخدم في ارتكاب الجريمة، سواء في صورتها الأولى، أي استعمالها في ارتكاب جرائم الاعتداء على نظم المعالجة الآلية للمعطيات. أو في صورتها الثانية، المتمثلة في كونها جرائم متحصلة عن جريمة من جرائم الاعتداء على نظم المعالجة الآلية للمعطيات. بينما عنصر الإرادة، يتضمن وجوب اتجاه إرادة الجاني إلى إتيان

وتحقيق أحد الأفعال السلوكية المجرمة في نص المادة 394 مكرر 2. وأن تنصرف هذه الإرادة إلى النشاط الجرمي فحسب دون إرادة أية نتيجة، على اعتبار أننا بصدد دراسة جريمة شكلية، كون النتيجة ليست عنصرا يعتد به في البناء القانوني لهذه الجريمة.

الفرع الثاني:مدى ضرورة توفر القصد الجنائي الخاص

بحث البعض، فيما إن كانت جريمة التعامل في معلومات غير مشروعة، تشترط بالإضافة إلى القصد الجنائي العام السابق، قصدا جنائيا خاصا، سواء في صورة الجريمة الأولى أو في صورتها الثانية. فبخصوص الصورة الأولى، ذهب هذا الاتجاه للقول بوجوب توفر قصد خاص إلى جانب القصد العام حتى تقوم جريمة التعامل في معلومات صالحة لارتكاب جريمة، ويتمثل هذا القصد الخاص في اتجاه إرادة الجاني إلى الإعداد والتمهيد لاستعمال هذه المعلومات في ارتكاب جريمة من جرائم الاعتداء على نظم المعالجة الآلية للمعلومات. غير أن المشرع الجزائري وصراحة لم يشترط هذا القصد الخاص في نص المادة 394 مكرر 2 . أما بخصوص الصورة الثانية لهذه الجريمة، فإن القصد الجنائي العام كاف لوحده لقيامها أيضا، وذات الوضع بالنسبة للمشرع الفرنسي، عكس اتفاقية بودابست التي تشترط قصدا خاصا، وهو نية استخدام المعلومات في جريمة من الجرائم - الفقرة (ب) من المادة 6- وأشارت المذكرة التفسيرية لهذه الاتفاقية لأهمية تطلب القصد الخاص، بأنه:" من أجل تجنب خطر العقاب المبالغ فيه، حيث يتم إنتاج هذه الأجهزة وعرضها في السواق لأغراض شرعية من أجل التصدي لاعتداءات على أجهزة الحاسب الآلي، فإنه يجب إضافة عناصر أخرى من أجل تضييق نطاق الجريمة. وبالإضافة إلى اشتراط القصد العام فإنه يجب توافر نية خاصة أو قصد خاص لاستخدام الجهاز من أجل ارتكاب جريمة من الجرائم المشار إليها في المواد من 2 إلى 5 من الاتفاقية" [(67)].

خاتمــة

يتضح لنا أن تدخل المشرع الجزائري بتعديل قانون العقوبات سنة 2004 كان بهدف مواجهة الاعتداءات المعلوماتية التي تكون نظم المعالجة الآلية للمعلومات عرضة لها. فقام بحماية هذه النظم في حد ذاتها من التخريب والإفساد والتعطيل وما إلى غير ذلك، وهي اعتداءات لا يمكن أن تتم إلا من خلال دخول هذه النظم أو البقاء غير

المشروع فيها. كما قام بتجريم الاعتداءات التي تكون البيانات والمعلومات والمعطيات عرضة لها بعد أن يتم مثل هذا الدخول أو البقاء غير المشروعين. وبالتالي يكون قد حمى نظم المعلومات ذاتها وكذا المعلومات التي تحتويها، أيا كان شكل ونوع وطبيعة هذه المعلومات. وبالتالي يمكننا القول أن قانون العقوبات أضحى بتعديلاته الأخيرة هذه قادرا على إضفاء حماية جنائية للنظم المعلوماتية، وبالتالي ثبت بأن لظاهرة المعلوماتية قد قابلها تطور في الظاهرة القانونية، وأن قانون العقوبات سيظل القانون الضابط لأي تقدم حضاري أو علمي، وأن ظاهرة الإجرام المعلوماتي شأنها شان كافة الظواهر الإجرامية الأخرى لا يمكن أن تفلت من حكم القانون، ولا أن يستفيد المجرمين من ظاهرة انفلات الإنترنت من فكرتي الخضوع والسيطرة وتجاهلها للحدود والمرتكزات المكانية والجغرافية.

وحتى وإن انفلتت الظاهرة من الخضوع لقواعد قانون العقوبات التقليدية، كونها قواعد لا تتلاءم في كثير من الأحيان مع متطلبات هذه البيئة الرقمية الافتراضية الحديثة واللامادية، وإن كان من الممكن تطويع وتكييف بعضها. إلا أن الأمر لا يزال يحتاج إلى بعض التحديث والتعديل في كثير من الأحيان، سيما ما تعلق الأمر بتعديل النصوص المتعلقة بجريمة السرقة والنصب وخيانة الأمانة وجعلها شاملة للمال المعلوماتي الذي ينتقل عبر النبضات الرقمية الإلكترونية، وكذا تعديل النصوص المتعلقة ببعض الجرائم التقليدية والتي يمكن أن تتم عبر النظم المعلوماتية، كجرائم التهديد والسب والقذف والتزوير المعلوماتي.....وحتى يمكن القول أنه تم إيجاد بيئة قانونية مناسبة للتعاملات الإلكترونية عبر النظم المعلوماتية، ولتجاوز التحديات الكبيرة التي واجهت في البداية النظم العقابية التقليدية، في ظل عجز قواعدها التقليدية على احتواء الظاهرة المعلوماتية وما أفرزته من ظاهرة إجرامية معلوماتية بدورها. يتعين أن يتم التركيز في عملية التجريم على محورين أساسيين؛ محور يتعلق بحماية النظم ذاتها وما تتضمنه من معلومات وبيانات، وهو ما قام به المشرع. ومحور يتعلق باستعمال النظم المعلوماتية كوسيلة لارتكاب الجرائم، وهو لا يزال يشهد نقصا كبيرا في التشريع الجزائري.

ومثلما سبقت الإشارة إليه في المقدمة، فإن تكريس الحماية الجنائية الموضوعية للنظم المعلوماتية يتطلب تدعيم في المواجهة الإجرائية، خاصة وأننا نعلم بأن قانون العقوبات مكون من شقين متلازمين ومتكاملين، هما الشق الموضوعي، الذي كان موضوع دراسة في هذا المقال. وشق إجرائي نأمل أن نتناوله في مناسبات أخرى بإذن الله. وبذلك تكتمل المواجهة الجنائية للإجرام المعلوماتي عموما، وتكرس حماية جنائية فعلية للنظم المعلوماتية التي أضحت عصب الحياة في مجتمعانا الحاضرة.

الهوامش:

(1) ظهور مصطلح التجارة الإلكترونية، كان نتيجة دخول الإنترنت مجال الاستعمال التجاري، شكل عامل مفاجأة بالنسبة للمشتغلين بهذا المجال، وأسفر عن اختلاف وتباين الآراء ووجهات النظر حول وضع مفهوم دقيق لها. غير أن ما أمكننا استخلاصه، هو أن مرد كل هذا الخلاف كان نتيجة التوصيف الإلكتروني لهذا النوع من التجارة. راجع رسالتنا بالتفصيل بخصوص مختلف جوانب هذا الخلاف:" النظام القانوني لعقد البيع الدولي الإلكتروني المبرم عبر الإنترنت"، رسالة دكتوراه في العلوم، تخصص قانون، كلية الحقوق، جامعة مولود امعمري – تيزي وزو، 2009، ص: 54-76.

(2) وهو الأمر الذي تنبه له المشرع الجزائري وقام بإحداث تعديل على القانون المدني سنة 2005 اعترف بموجبه بالمحررات والكتابة والتوقيع الإلكتروني. انظر: أمر رقم 75-58 مؤرخ في: 26 سبتمبر 1975 يتضمن القانون المدني المعدل والمتمم بالقانون رقم : 05-10 مؤرخ في: 20 جوان 2005.

(3) أنظر: أشرف توفيق شمس الدين: "الحماية الجنائية للمستند الإلكتروني"، بحث مقدم لمؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون المنعقد بدبي في الفترة 12/10 ماي 2003، ص: 432.

(4) راجع في هذا المعنى: حسام كامل الأهواني: "الحماية القانونية للحياة الخاصة في مواجهة الحاسب الإلكتروني"، مجلة العلوم القانونية والاقتصادية، كلية الحقوق جامعة عين شمس، يناير – يوليو 1990 ص: 9. وراجع كيفية خلق الإنترنت لاقتصاد جديد :

MAS-FOVEAU Séverine et BENACHOUR-VERSTREPEN Malika, « le commerce électronique en toute confiance, diagnostic des pratiques et environnement juridique », LITEC , Paris 2001, pp :153-154.

(5) راجع في هذا المعنى :

CAPRIOLI Eric et SORIEUL Renaud, le commerce international électronique: vers l'émergence des règles juridiques transnationales transnationales, J.D.I , 1997, p: 326

(6) ITEANU Olivier, Internet et le droit, aspects juridiques du commerce électronique, Paris, 2000, p :17

(7) راجع في هذا المعنى: جميل عبد الباقي الصغير :" الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة"، دار النهضة العربية، القاهرة، مصر، 1999، ص: 39 وراجع أيضا: محمد عبيد الكعبي:" الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت"، رسالة ماجستير، كلية الحقوق، جامعة القاهرة، 2004، ص: 1-2، وص:7. وراجع تفصيلا في ذلك: رشدي محمد علي محمد عيد علي:" الحماية الجنائية للمعلومات على شبكة الإنترنت – دراسة مقارنة-"، كلية الحقوق ، جامعة القاهرة، مصر 2009، ص: 78 وما بعدها. هدى حامد قشقوش :" جرائم الحاسب

الإلكتروني في التشريع المقارن"، مرجع سابق، ص: 15- 17، ولمزيد من التفاصيل انظر: أحمد بن زايد جوهر الحسن المهندي:" تفتيش الحاسب الآلي وضمانات المتهم"، رسالة ماجستير، القاهرة، مصر، 2009، ص: 11 وما بعدها.

(8) راجع: جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، مرجع سابق، ص: 10.

(9) راجع في ذلك: محمد عبيد الكعبي، مرجع سابق، ص: 27-28.

ومما زاد من صعوبة جرائم الإنترنت أن المجني عليهم يحجمون عن التبليغ عنها، راجع في أسباب ذلك: هشام محمد رستم:" الجوانب الإجرائية للجرائم المعلوماتية – دراسة مقارنة- "، مكتبة الآلات الحديثة، أسيوط، مصر، 1994، ص: 26. وكذا: محمد سامي الشوا:" ثورة المعلومات وانعكاساتها على قانون العقوبات"، دار النهضة العربية، القاهرة، مصر، 1998، ص: 60 وما بعدها.

(10) لمزيد من التفاصيل، انظر: ماجد عمار:" المسؤولية القانونية الناشئة عن استخدام فيروس وبرامج الكمبيوتر وحمايتها"، دار النهضة العربية، القاهر، مصر، 1989، ص: 293 وما بعدها.

(11) لكن الإنترنت استدعت البحث عن إطار قانوني مدني قبل الإطار القانوني الجنائي. انظر في ذلك:

E.BROUSSEAU « commerce électronique : ce que disent les chiffres et ce qu'il faudrait savoir » en ligne :http://www.minefi.gouv.fr/minefi/chiffres/comelec/tbce/doss/pdf/insee2.pdf. Et GAUTRAIS Vincent GOBERT Didier JULIA-BARCELO Rosa Etienne MONTERO Yves POULLET Anne SALAUN QUANTINVAN DAELE : commerce électronique : le temps des certitudes ; Bruyant, Bruxelles 2000 delta 2001 , p :150.

(12) راجع هذه الثورة وأثرها على القوانين: علي عبد القادر القهوجي: " الحماية الجنائية لبرامج الحاسب الآلي"، دار الجامعة الجديدة للنشر الإسكندرية، مصر، 1997، ص: 1.

(13) راجع تفصيلا في ذلك:

TRUDEL Pierre, *l'influence d'Internet sur la production du droit*, sur http://droit-internet-2001.univ-paris1.fr/pdf/trudel_p.pdf . ET pour le même auteur , *les mutations du droit à l'âge numérique*, juillet 2000 , revue droit & toile, http://www.unitar.org/isd/dt/ddt1-reflexion.html.

(14) وهنا حدث تطور في طرق المواجهة الجنائية التقليدية، فأضحت تتطلب حماية جنائية لمواقع وبيانات النظم الإلكترونية، كوننا في بيئة رقمية تقوم على بيانات ومعطيات إلكترونية، هي عبارة عن نبضات إلكترونية وكهرومغناطيسية مؤلفة من الرقمين (0) و(1) دون غيرهما، تعمل عبر أجهزة لا تعرف سوى هذه اللغة. لذا الأمر يقتضي تدخل تشريعي لفرض هيمنة القانون وحماية المصالح القائمة والمشروعة، لكن على أن يكون ذلك في إطار من الشرعية الجنائية التي تقتضي بألا جريمة ولا عقوبة بغير نص.

(15) اتفاقية بودابست اتفاقية أوروبية المنشأ إلا أنها دولية النزعة كونها مفتوحة لكل الدول للانضمام إليها (المادة 2/36 من الاتفاقية)، وهي الاتفاقية المنعقدة في 23-11-2001 ودخلت حيز النفاذ في 01-01-2007 بعد المصادقة عليها من قبل 30 دولة، من بينها أربع دول من خارج المجلس الأوروبي، وهي اليابان، كندا، الولايات المتحدة الأمريكية وجنوب إفريقيا. وهي اتفاقية يمكن اعتبارها الأولى دوليا لمكافحة الجريمة المعلوماتية.

(16) انظر: بوكر رشيدة:" جرائم الاعتداء على نظم المعالجة الألية في التشريع الجزائري والمقارن، رسالة ماجستير، دمشق، سوريا، 2010. ص: 94.

(17) حيث كان إدراك المشرع الفرنسي فشل النصوص التقليدية في حماية المعلومات ونظمها، أولا من مبادرة وزير العدل سنة 1985 والتي أثارت العديد من النقاشات والكثير من التعديلات لغاية تعديل أخير لقانون العقوبات الفرنسي، وذلك بموجب القانون رقم 2004-575 المؤرخ في 21 جوان 2004 المتعلق بالثقة في الاقتصاد الرقمي.

(18) سيما فيما يخص تمديد الاختصاص. راجع المواد 40- 40 مكرر من قانون الإجراءات الجزائية.

[19] العدد 47 من الجريدة الرسمية، المؤرخة في: 16 غشت 2009.

[20] المشرع الجزائري وإن كان لم يعرف الجريمة المعلوماتية بموجب تعديل سنة 2004 إلا أنه سمى الباب الذي نظمها ب:" المساس بأنظمة المعالجة الآلية للمعطيات". وسنة 2009 أدرج تعريفا لها بموجب المادة 2 من قانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها. بالقول:" جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن ريق منظومة معلوماتية أو نظام الاتصالات الإلكترونية."

[21] من الفقه من يستعمل مصطلح "الاختراق" للتعبير عن الدخول، انظر مثلا: عمر محمد أبو بكر بن يونس:" الجرائم الناشئة عن استخدام الإنترنت "، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، 2004، ص: 331. ومنهم من يستعمل مصطلح " الولوج" ، انظر على سبيل المثال: محمد سامي الشوا:" ثورة المعلومات وانعكاساتها على قانون العقوبات"، دار النهضة العربية، 1994 ، ص: 204. لكن هناك من يبقى يفضل مصطلح " الدخول" انظر: نائلة عادل محمد فريد قورة :" جرائم الحاسب الآلي الاقتصادية – دراسة نظرية وتطبيقية-"، منشورات الحلبي الحقوقية، 2005ص: 315.

[22] أشارت المذكرة التفسيرية لاتفاقية بودابست، بأن الدخول غير المشروع لنظم المعالجة الآلية للمعطيات، يعد الجريمة الرئيسية التي تنطوي على تهديد أمن المعلومات وسريتها وسلامتها ... كما يمكن أن تؤدي إلى إتلاف أو تدمير باهظ التكلفة في حالة إعادة البناء... مشار له لدى: هلالي عبد الله:" الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست الموقعة في 23 نوفمبر 2001"، دار النهضة العربية، القاهرة، مصر، 2003، ص: 69.

[23] انظر: بوكر رشيدة، مرجع سابق، ص: 116.

[24] المعنونة بالدخول غير القانوني.

[25] راجع في ذلك : أيمن عبد الله فكري:" جرائم نظم المعلومات – دراسة مقارنة-"، دار الجامعة الجديدة للنشر، الإسكندرية 2007، ص: 231 ويؤديه بعض الفقه العربي، مثل أحمد حسام طه تمام :" الجرائم الناشئة عن استخدام الحاسب الآلي"، دار النهضة العربية، القاهرة، مصر، 2000، ص: 267، وبلال أمين زين الدين :" جرائم نظم المعالجة الآلية للبيانات في التشريع المقارن والشريعة الإسلامية"، دار الفكر الجامعي، الإسكندرية، مصر، 2008، ص: 267.

[26] راجع تفصيلا حجج هذا الاتجاه: د. أيمن عبد الله فكري، مرجع سابق، ص: 233-234.

[27] كما تستعمل مصطلحات مثل "الدخول غير المشروع"، " الدخول دون حق" .

[28] انظر في تفصيل ذلك:

BENSOUSSAN Alain : Fraude informatique, La protection d'un système informatique par un dispositif de sécurité n'est pas une condition d'application de la loi Godfrain, en ligne : http://www.alain-bensoussan.com/pages/2903/

[29] راجع في معنى كل ذلك: محمد حماد مرهج الهيتي :" جرائم الحاسوب: ماهيتها، موضوعها، أهم صورها، والصعوبات التي تواجهها- دراسة تحليلية لواقع الاعتداءات التي يتعرض لها الحاسوب وموقف التشريعات الجنائية منها-"، دار المناهج للنشر والتوزيع، عمان، الأردن، ط1، 2006، ص: 182، وانظر: أسامة أحمد المناعسة، جلال الزعبي، صايل فاضل الهواوشة :" جرائم الحاسب الآلي والإنترنت"، دار وائل للنشر، عمان، الأردن، ص: 231.

(30) انظر: خالد ممدوح إبراهيم :" أمن الجريمة الإلكترونية"، الدار الجامعية، الإسكندرية، مصر، 2008، ص: 84. رامي عبد العزيز:" الفيروسات وبرامج التجسس" دار البراءة، الإسكندرية، مصر، 2005، ص: 82 .

(31) مشار له لدى: محمد عبيد الكعبي، مرجع سابق، ص: 336.

(32) أحمد حسام طه تمام، مرجع سابق، ص: 305.

(33) أيمن عبد الله فكري، مرجع سابق، ص: 238. عمر محمد أبو بكر بن يونس، مرجع سابق، ص: 332.

(34) بوكر رشيدة، مرجع سابق، ص: 154. وانظر: نائلة عادل محمد فريد قورة، مرجع سابق، ص: 347

(35) راجع في ذلك كله : بوكر رشيدة، مرجع سابق، ص: 29- 31.

(36) عامر قنديلجي ود.علاء الدين الجنابي :" ما هو نظام المعلومات المحوسب"، بحث منشور على الموقع: http://www.minshawi.com مشار له لدى: بوكر رشيدة، مرجع سابق، ص: 31.

(37) انظر: بوكر رشيدة، المرجع نفسه، الهامش رقم 2 ص: 32.

(38) مشار له لدى: محمد محمد شتا:" الحماية الجنائية لبرامج الحاسب الآلي"، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، 2002-، ص: 61.

(39) انظر في تفاصيل أكثر: نائلة عادل فريد قورة، مرجع سابق، ص: 365.

(40) مشار لهذه القوانين وقوانين أخرى لدى: بوكر رشيدة، مرجع سابق، ص: 173.

(41) انظر في هذا : أيمن عبد الله فكري، المرجع السابق، ص: 244. وبوكر رشيدة، مرجع سابق، ص: 174.

(42) انظر هـذا الرأي: بوكر رشيدة، مرجع سابق، ص: 176.

(43) انظر على سبيل المثال: نائلة عادل محمد فريد قورة، مرجع سابق، ص: 437.

(44) انظر في ذلك: د. علي عبد القادر القهوجي، مرجع سابق، ص: 144.

(45) هناك العديد من القضايا التي عرضت على القضاء الفرنسي بهذا الخصوص، راجع تفصيلا في ذلك: بوكر رشيدة، مرجع سابق، ص: 185-186. نائلة عادل محمد فريد قورة، مرجع سابق، ص: 449.

(46) انظر: علي عبد القادر القهوجي، مرجع سابق، ص: 144.

(47) انظر: بوكر رشيدة، مرجع سابق، ص: 187. نائلة عادل محمد فريد قورة، مرجع سابق، ص: 447.

(48) راجع قضية طرحت على القضاء بهذا الشأن: عبد الفتاح بيومي حجازي، مرجع سابق، ص: 49.

(49) راجع في ذلك: علي عبد القادر القهوجي، مرجع سابق، ص: 143.

(50) انظر في ذلك: بوكر رشيدة، مرجع سابق، ص: 198.

(51) مشار له لدى: المرجع نفسه وكذلك:

BENSOUSSAN Alain ; Fraude informatique, Les atteintes à un système de traitement automatisé de données, en ligne : http://www.alain-bensoussan.com/pages/2903/

(52) انظر في ذلك: علي عبد القادر القهوجي:" الحماية الجنائية للبيانات المعالجة إلكترونيا"، دار الجامعة الجديدة للنشر والتوزيع، الإسكندرية، مصر، 1997، ص: 60.

(53) راجع في ذلك: نائلة عادل محمد فريد قورة، مرجع سابق، ص: 223.

(54) نصت عليها أيضا اتفاقية بودابست في نص المادة 6 تحت عنوان " إساءة استخدام الأجهزة".

(55) انظر: بوكر رشيدة، مرجع سابق، ص: 206.

(56) المرجع نفسه.

(57) لمزيد من التفاصيل انظر المرجع نفسه، وفي المعنى: د. هلالي عبد الله أحمد، مرجع سابق، ص: 101

(58) المرجعين نفسهما.

(59) انظر: هلالي عبد الله أحمد، مرجع سابق، ص: 101 .

(60) انظر في ذلك: بوكر رشيدة، مرجع سابق، ص: 209-210.

(61) المرجع نفسه.

(62) حيث لا عبرة بالوقت الذي تستغرقه الجريمة، كونها جريمة وقتية تقوم وتكتمل وتستحق الزجر بمجرد الحيازة معا العم بأنها حيازة بطريقة غير مشروعة.

(63) متبعا في ذلك خطة المشرع الفرنسي الذي سبق في المجال، ومسترشدا بأحكام اتفاقية بودابست.

(64) حيث أضحت المعلومات ذات قيمة اقتصادية كبيرة في الوقت الحاضر، واضحت التفرقة بين الدول قائمة على أساس من يعلم ومن لا يعلم، لا بين من يملك ومن لا يملك.

(65) رشيدة بوكر، مرجع سابق، ص: 222 وما بعدها.

(66) بوكر رشيدة، مرجع سابق، ص: 218 وما بعدها.

(67) انظر في شرح الاتفاقية والبروتوكول الملحق بها: د. إيهاب السنباطي:" الترجمة الجديدة والكاملة للاتفاقية المتعلقة بالجريمة الإلكترونية (بودابست 2001)والبروتوكول الملحق بها"، دار النهضة العربية، القاهرة، 2008-2009.