



المكافحة الموضوعية للجرائم الإلكترونية في القانون الجزائري Objective Combat of Cybercrimes in Algerian Law

يخلف عبد القادر¹

جامعة عمار ثلجي بالأغواط، الجزائر

a.yekhlef@lagh-univ.dz

مخبر القانون وتطور المجتمع

تاريخ القبول للنشر: 2024-11-19

تاريخ الاستلام: 2024-03-02

ملخص:

لا يمكن مواجهة الجريمة المعلوماتية بدون توفير حماية كافية للبيئة والنطاق الذي تتواجد فيه المعلومات. ولهذا الغرض، قام المشرع الجزائري بمكافحة هذه الجرائم عن طريق وضع نصوص قانونية تجرم كل مساس بالأنظمة والبرمجيات المعلوماتية، المعروفة بـ "أنظمة المعالجة الآلية للمعطيات"، وهذا لضمان حماية المعلومات المتواجدة داخل هذه الأنظمة. وبناءً على هذا، يهدف هذا البحث إلى دراسة الحماية الموضوعية من الجرائم المعلوماتية، وتقييم مدى توفيق المشرع الجزائري في الاحاطة الموضوعية لمنع جميع الأفعال الماسة أنظمة المعالجة الآلية للمعطيات. الكلمات المفتاحية: السياسة الجنائية، المكافحة الموضوعية، الجرائم المعلوماتية.

Abstract:

Addressing cybercrime without adequately safeguarding the environments and platforms where information resides is impractical.

The Algerian legislature has made efforts to tackle severe offenses using information systems and software, commonly referred to as "data processing systems," to protect the data within. With this in mind, this research aims to explore the objective protection of cybercrimes and evaluate the effectiveness of the Algerian legislature in defining the objective criteria for these criminal acts to mitigate their occurrence.

Keywords: Criminal policy, Objective countermeasures, Cybercrimes.

¹ يخلف عبد القادر

مقدمة:

شهدت العقود الأخيرة تطوراً غير مسبوق في تكنولوجيا المعلومات والاتصالات، الأمر الذي أفرز نمطاً جديداً من الإجرام، يُعرف بالجرائم المعلوماتية أو الإلكترونية، والتي تجاوزت في خطورتها وأسلوب ارتكابها الجرائم التقليدية مثل السرقة والنصب وخيانة الأمانة، وقد أثار هذا الواقع المستجد نقاشاً واسعاً في الأوساط القانونية حول مدى كفاية النصوص الجنائية الموضوعية التقليدية لمواجهة هذه الأفعال المستحدثة، خاصةً مع الطبيعة الخاصة للجرائم الإلكترونية التي تتسم بالتعقيد والتطور السريع وسهولة الانتشار عبر الحدود.

ورغم محاولة بعض الاتجاهات الفقهية التمسك بفكرة الاكتفاء بالنصوص التقليدية واعتبارها كافية لاستيعاب هذه الأفعال، إلا أنّ التجربة العملية أثبتت محدودية هذا الطرح، إذ إن تطبيق النصوص التقليدية على الجرائم المعلوماتية قد يؤدي إلى المساس بالمبادئ القانونية المستقرة في التجريم والعقاب، ويفتح المجال لظهور ثغرات قانونية يصعب سدّها بغير تدخل تشريعي خاص. وانطلاقاً من ذلك، اقتنع الفكر القانوني بضرورة إفراغ الجرائم المعلوماتية بنصوص قانونية مستقلة تواكب طبيعتها وتسدّ النقص التشريعي القائم.

وفي هذا السياق، أدرك المشرع الجزائري خطورة هذه الجرائم وآثارها على المجتمع، فسعى إلى وضع إطار قانوني خاص لمكافحة الأفعال الإجرامية التي تمسّ أنظمة وبرامج المعالجة الآلية للمعطيات، إيماناً منه بأن حماية المعطيات والمعلومات المخزّنة في هذه الأنظمة تمثّل خط الدفاع الأول في مواجهة هذا النوع من الإجرام، ومع ذلك، يظل التساؤل مطروحاً حول مدى كفاية هذه النصوص في توفير حماية جنائية فعّالة لهذه الأنظمة والمعلومات التي تحتويها.

أهمية الموضوع تكمن في كونه يتناول مسألة ذات أبعاد تقنية وقانونية شديدة الترابط والتعقيد، تلامس جوهر الأمن المعلوماتي وحماية الحياة الرقمية للأفراد والمؤسسات والدولة على حد سواء، في ظل بيئة دولية يشهد فيها الفضاء السيبراني تزايداً مطّرداً للتهديدات والهجمات الإلكترونية.

أهداف البحث تتمثل في تحليل وتقييم مدى نجاعة المنظومة التشريعية الجزائية في مجال التجريم الخاص بالمساس بأنظمة المعالجة الآلية للمعطيات، والكشف عن الثغرات التي قد تحدّ من فعاليتها، واقتراح الحلول القانونية المناسبة لسدّ هذه الثغرات وتعزيز الحماية الجنائية للفضاء المعلوماتي الوطني.

وانطلاقاً من هذه الأهمية والأهداف، تتمحور إشكالية البحث حول التساؤل الرئيس الآتي: إلى أي مدى تُعتبر النصوص الجنائية الحالية المتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات كافية لتحقيق حماية قانونية فعّالة للمعطيات المعلوماتية في الجزائر؟

وللإجابة على هذه الإشكالية، اعتمدنا على المنهج الاستدلالي التحليلي من خلال تحليل النصوص القانونية ذات الصلة، ومقارنتها بالممارسات الفقهية والقضائية ذات العلاقة، بغية تحديد أوجه القصور والقصور، واقتراح سبل تطويرها بما ينسجم مع المتطلبات التقنية الراهنة.

المبحث الأول: أمن الأنظمة والبرمجيات تحت مظلة القانون الجنائي

لقد أدرك المشرع الجزائري خطورة الأفعال التي تمسّ بالأنظمة والبرمجيات المعلوماتية، وبناءً على ذلك بادر إلى تجريم هذه الأفعال من خلال تعديل قانون العقوبات بموجب القانون رقم 09/04، وذلك في المواد من 394 مكرر إلى 394 مكرر 7، تحت عنوان "المساس بأنظمة المعالجة الآلية للبيانات".

كما تجدر الإشارة إلى أنّ المشرع الجزائري قد صادق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بتاريخ 08 سبتمبر 2014، والتي تضمّنت بدورها تجريم الأفعال التي تمسّ بالبرمجيات والأنظمة، وذلك في المواد 7 و8 و9 منها.

وبالعودة إلى النصوص القانونية السالفة الذكر، يتّضح أنّ المساس بأنظمة المعالجة الآلية للمعطيات قد يتّخذ عدّة صور تختلف باختلاف السلوك الإجرامي المرتكب؛ فقد يظهر ذلك في شكل المساس بالبرامج والأنظمة (مطلب أول)، كما قد يتجلّى في صورة المساس بسير نظام المعالجة ذاته (مطلب ثاني).

المطلب الأول: الإطار الجنائي لحماية البرامج والأنظمة المعلوماتية

إن مسألة وضع نصوص قانونية جنائية لمواجهة الجرائم المعلوماتية قد أثارت جدلاً فقهيّاً واسعاً حول مدى إمكانية توسيع نطاق القوانين الجنائية التقليدية لاستيعاب هذا النوع المستحدث من الجرائم. وبالفعل، فإن الاتجاه الفقهي الذي أيد هذا التوسع لم يكتب له النجاح المرجو، إذ يُعتقد أن تبني هذه الأفكار من شأنه أن يؤدي إلى تشويه المبادئ الأساسية التي تقوم عليها القوانين الجنائية، مما قد يترتب عليه وجود ثغرات قانونية يصعب معالجتها في إطار التشريع التقليدي. وقد دفع ذلك الفكر القانوني إلى الاستقرار والاعتناع بضرورة إفراد هذه الجرائم بنصوص قانونية خاصة لمعالجتها بفعالية.

وبما أنه لا يمكن مواجهة الجريمة المعلوماتية دون توفير حماية كافية للبيئة والنطاق الذي تتواجد فيه المعلومات، فقد سعى المشرع الجزائري إلى مكافحة هذه الجرائم من خلال وضع نصوص خاصة بحماية الأنظمة والبرمجيات المعلوماتية، والتي يُفضل تسميتها بـ «أنظمة المعالجة الآلية للبيانات»، وذلك بهدف حماية المعلومات المحفوظة داخل هذه الأنظمة. ويتحقق ذلك سواء عن طريق تجريم الدخول إلى نظام المعالجة أو البقاء فيه بصفة غير مشروعة (فرع أول)، أو من خلال تجريم الأفعال التي تمسّ بسير نظام المعالجة (فرع ثانٍ).

الفرع الأول: تجريم التسلل والبقاء غير المشروع داخل أنظمة المعالجة الآلية

إن تجريم الدخول إلى نظام المعالجة أو البقاء فيه بصفة غير شرعية يُعبّر عن توجه قانوني واضح نحو حماية الأنظمة المعلوماتية من الاعتداءات غير المشروعة، كما أنّ هذا التجريم يساهم في تعزيز الأمن الرقمي وصون البيانات الحساسة، ويشكّل في الوقت ذاته رسالة قانونية مفادها أنّ انتهاك قواعد الأمن المعلوماتي يُعدّ جريمة تستوجب العقوبة القانونية المناسبة.

لقد نتج عن ربط الحاسبات الآلية ببعضها البعض عن طريق شبكات الاتصال سرعة كبيرة في انتقال وتداول المعلومات والبيانات، الأمر الذي يساهم في اختصار الزمن وتحقيق ما يسعى إليه المتعامل الإلكتروني من سرعة وكفاءة، غير

أنّ هذا التطور سهّل في المقابل عمليات التطفّل على تلك المعلومات أو البيانات، مما قد يؤدي في النهاية إلى قرصنتها أو السطو عليها، حيث غالباً ما تستهدف هذه الجرائم المؤسسات المصرفية وشركات التأمين والشركات الخاصة وكذلك مؤسسات القيم المالية ومواقع التجارة الإلكترونية.

وقد استشعر المشرّع في العديد من الدول الحاجة الماسّة إلى إدخال تشريعات جديدة تحمي المعلومات داخل نظم الكمبيوتر، وذلك بالنظر إلى قصور القواعد التقليدية في قانون العقوبات عن توفير الحماية اللازمة لهذه الأنظمة.

وبناءً على ذلك، تم استحداث نصوص تجرّيمية تعاقب على مجرد الدخول غير المشروع إلى نظام الحاسب الآلي، فضلاً عن تجريم إتلاف المعلومات المبرمجة أو المخزّنة داخله.

أولاً: الدخول إلى نظام المعالجة

ورد في المادة 394 مكرر من قانون العقوبات أنّه: «يُعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة مالية 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...»، وهو ما نصّت عليه كذلك الاتفاقية العربية لمكافحة الجريمة المعلوماتية، حيث جاء في المادة 1/6 منها: "الدخول أو البقاء وكل اتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار به".

ويتضح من هذه المادة أن الركن المادي لهذه الجريمة يتكوّن من عنصرين أساسيين هما: الدخول إلى نظام المعالجة، أو البقاء فيه بعد الدخول. ويتحقق الدخول من خلال الولوج إلى المعلومات والمعطيات المخزّنة داخل نظام الحاسب الآلي دون رضا المسؤول عن هذا النظام، وتشير المذكرة التفسيرية لاتفاقية بودابست إلى أن الولوج غير القانوني يجب أن يكون «دون حق»، وهو ما يعني أنه لا عقوبة على الولوج المصرّح به أو على الولوج الذي يكون متاحاً للجمهور (أحمد، 2007، صفحة 54 وما بعدها).

وبناءً على ذلك، يتضح أن مفهوم الدخول يختلف عن التقاط الإرسالات أو الإشارات عن بُعد، إذ لا يقوم المتهم في هذه الحالة بدخول نظام معين. ومن ثم، يصبح من الضروري وجود نص قانوني خاص يعاقب على أفعال التلصص والتجسس على الرسائل والبيانات المرسلة، وهو ما أشارت إليه المادة 1/6 من الاتفاقية العربية لمكافحة الجريمة المعلوماتية بعبارة «وكل اتصال غير مشروع». كما نصّت المادة 7 من الاتفاقية ذاتها على تجريم الاعتراض المتعمّد دون وجه حق على خطّ سير البيانات باستخدام أي وسيلة تقنية، إضافةً إلى قطع بثّ أو استقبال بيانات تقنية المعلومات، وهو ما يؤكّد الحاجة إلى استحداث نصوص قانونية واضحة لتجريم هذه الأفعال ومعاقبة مرتكبيها.

ومن خلال التوضيح السابق لعنصر الدخول غير الشرعي إلى نظام المعالجة الآلية للمعطيات، يتبيّن أن هذه الجريمة تتحقّق بمجرد وقوع النشاط المادي، إذ يُعدّ الدخول بحدّ ذاته جريمة قائمة بذاتها، بغضّ النظر عن الأفعال التي قد تترتّب عليه لاحقاً. فعندما يدخل الشخص إلى النظام المعلوماتي، تُعتبر الجريمة قد وقعت حتى وإن لم يلحق الدخول أي ضرر أو لم يحقق الجاني أي منفعة من ورائه، سواء شمل الدخول النظام بأكمله أو اقتصر على جزء منه. كما يُعدّ مرتكباً لهذه الجريمة كل من يُسمح له بالدخول إلى جزء معين من النظام، لكنه يتجاوز نطاق التصريح ليصل إلى أجزاء أخرى محظور عليه الولوج إليها (القهوجي، 1999، الصفحات 130-133).

ثانياً: البقاء غير المشروع داخل نظام المعالجة

يتحقّق السلوك المجرّم هنا بتواجد الشخص داخل النظام المعلوماتي دون موافقة من الشخص الذي يمتلك سلطة التحكم فيه (الحليم، 2009، صفحة 17)، وقد يحدث ذلك إمّا بعد دخول غير مشروع إلى النظام، أو عند البقاء في النظام بعد انقضاء الوقت المحدد قانوناً أو تعاقدياً للبقاء فيه، وهو الوقت الذي قد يكون مشروطاً أحياناً بدفع مقابل زمني.

ويُطلق على هذا السلوك المجرّم في بعض الأحيان اسم «سرقة وقت الآلة» (عطالله، 2007، صفحة 124) (قارة، 20077، صفحة 111). وقد تقع جريمة البقاء في النظام حتى دون أن تترافق مع جريمة الدخول إليه، وذلك في حال كان دخول الشخص إلى النظام قد تمّ عن طريق الخطأ أو الصدفة. ويذهب بعض الفقه إلى أنّ هذه الجريمة غالبًا ما تحدث من قبل العاملين في الشركات والمؤسسات، عندما يستمرون في استخدام النظام بعد انتهاء الوقت المحدد لهم، الأمر الذي يجعل تجريم البقاء موجّهًا بصفة خاصة لهذه الفئة. ويُعتبر استخدام النظام بعد انقضاء الوقت المحدد استمرارًا للدخول والبقاء في النظام معًا. ومع ذلك، تشير أحكام القضاء الفرنسي إلى وجوب توقّر القصد الجنائي، حيث يُعتبر البقاء في النظام لغرض استخدامه لأغراض شخصية جريمة قائمة بذاتها؛ فعلى سبيل المثال، يلجأ بعض موظفي الشركات إلى استخدام أجهزة الحاسوب للعب ألعاب التسلية بعد انتهاء وقت العمل المحدد، مما يؤدي إلى تكبيد الشركة تكاليف إضافية نتيجة استخدامهم خطوط الهاتف (عطالله، 2007، صفحة 124).

وفي هذا السياق، نشير إلى أن موضوع التجريم أو محلّه هنا هو بقاء الجاني داخل النظام في حين كان يجب عليه في هذه الحالة أن يقطع اتصاله بالنظام وينسحب منه فورًا (قارة، 20077، صفحة 110).

ونضيف هنا أن تحقق عنصر البقاء داخل النظام يتمّ بمجرد التواجد في أي جزء منه دون الحاجة لقيام الجاني بأي أفعال أخرى كالتقاط المعلومات أو محوها؛ إذ يكفي أن يتجوّل الشخص في النظام بعد انتهاء الوقت المسموح به لاستخدامه ليُعتبر هذا الفعل سلوكًا مجرمًا (القهوجي، 1999، الصفحات 134-136). ويُشترط وفقًا للمادة 394 مكرر من قانون العقوبات أن يتم الدخول أو البقاء عن طريق الغش، وهو ما يدلّ على ضرورة توافر سوء نية الشخص وعلمه بأنه لا يملك الحق في الدخول أو البقاء في النظام، ومع ذلك يُقدم على هذا الفعل.

وغالبًا ما يظهر سوء النية من خلال قيام الجاني باختراق نظام الحماية. أمّا بخصوص عنصر البقاء، فيُستدلّ على توقّره من خلال تصرفات الشخص داخل



النظام. ويُعتبر الدخول مشروطاً إذا تمّ عن طريق الصدفة أو الخطأ أو السهو، وفي هذه الحالة يُلزم الشخص بالخروج فوراً من النظام. أمّا إذا رفض الخروج، فإن هذا يُعدّ دليلاً على وجود القصد الجنائي ونية الغش. ولا يتوافر القصد الجنائي إذا كان الدخول أو البقاء في الأصل مسموحاً به، أو إذا وقع الشخص في خطأ يتعلق بحقه في الدخول أو البقاء، سواء من حيث النطاق أو من حيث الزمن.

ويمكن للقاضي أن يستدل على توقّر القصد لدى الجاني من خلال عدّة قرائن، مثل استخدام برامج اختراق أو العثور بحوزته على برامج أو بيانات لها علاقة بعمليات القرصنة. وفي هذا الشأن، نذكر أن محكمة باتنة قد استندت في حكمها إلى الأدلة المقدّمة في القضية، وخاصة الخبرة الفنية المتعلقة بتحليل البريد الإلكتروني للمتهم، حيث تأكّد من خلالها أن المتهم كان يدخل النظام بطرق غير مشروعة باستخدام برامج متنوعة للقرصنة.

ومن خلال تحليل النصوص المتعلقة بجريمة الدخول والبقاء غير الشرعي في نظام المعالجة، نلاحظ أنّ المشرّع قد أحسن صنعاً في صياغة هذه المواد، إلا أنّه يُعاب عليه عدم النص على فعل «التداخل» الذي يختلف عن فعل الدخول إلى النظام. ومن جهة أخرى، تبدو عقوبة الحبس من ثلاثة أشهر إلى سنة والغرامة المالية من 50.000 دج إلى 100.000 دج غير كافية لردع هذه الجريمة، خاصةً في مجال المعاملات التجارية الإلكترونية التي تقوم أساساً على الثقة والأمان. ومن ثمّ، نقترح أن يكون النص على النحو الآتي: «يُعاقب بالحبس من ثلاثة أشهر إلى ثلاث سنوات وبغرامة مالية من 50.000 دج إلى 500.000 دج كل من يدخل أو يتداخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك...».

وبناءً على ما سبق من تحليل للنصوص المتعلقة بجريمة الدخول والبقاء غير الشرعي في نظام المعالجة، يتبيّن تقديرًا واضحًا لجودة صياغة المشرّع من جهة، إلّا أنّنا نلاحظ من جهة أخرى وجود نقص في تضمين فعل التداخل، في حين تمّ التركيز فقط على الدخول. كما نلاحظ أنّ عقوبة الحبس الحالية المحددة بثلاثة أشهر إلى

سنة والغرامة المالية من 50.000 دج إلى 100.000 دج، تبدو غير كافية لردع مثل هذه الجرائم، لا سيما في سياق المعاملات التجارية الإلكترونية التي تركز على الثقة والأمان.

الفرع الثاني: سير المعالجة تحت الحماية الجنائية

تُعتبر جريمة التلاعب أو التغيير في عمل النظام امتدادًا لجريمة الدخول أو البقاء غير المشروع في النظام، حيث يعمد الجاني إلى إجراء تغييرات داخل النظام تؤدي إلى تعطيل سيره أو تخريبه، ويُعدّ هذا التحديث أو التدخل في النظام تهديدًا خطيرًا للأمن المعلوماتي، مما يستوجب تشديد العقوبات لردع مرتكبي هذه الأفعال. ومن الجدير بالذكر أنّ المشرّع الجزائري اختار تضمين هذه الجريمة ضمن أحكام الدخول أو البقاء في النظام، مع تشديد العقوبة إذا ترتب على هذه التغييرات حذف أو تعديل للمعطيات، وعلى النقيض من ذلك، يعتبر المشرّع الفرنسي هذه الجريمة جريمة قائمة بذاتها، وينصّ عليها بشكل منفصل في قانون العقوبات الفرنسي في المادة 2/323.

ويُجسّد هذا الاختلاف في النهج التشريعي مدى استجابة المشرّعين للتطوّرات التكنولوجية والتحديات المتعلّقة بالأمن السيبراني، إذ يسعى المشرّعون إلى تطوير القوانين وتشديد العقوبات لمكافحة الجرائم الإلكترونية بفعالية. وهو ما نصّت عليه الاتفاقية العربية السالفة الذكر، في المادة 2/6 منها، حيث جاء فيها: «تُشدّد العقوبة إذا ترتّب على هذا الدخول أو البقاء أو الاتصال أو الاستمرار بهذا الاتصال: أ) محو أو تعديل أو تشويه أو نسخ أو نقل أو تدمير البيانات المحفوظة والأجهزة والأنظمة الإلكترونية وشبكات الاتصال، وإلحاق الضرر بالمستخدمين والمستفيدين.

ب) الحصول على معلومات حكومية سرّية.

وعليه، فإنّ هذه الجريمة تتحقّق بالأفعال التالية:

- الإخلال بسير نظام المعالجة عن طريق الحذف: يُعدّ جزءًا من جريمة التلاعب في النظام، إذ يقوم الجاني بحذف جزء من المعطيات المتعلّقة بالنظام دون الحاجة

إلى تعطيله كلياً. ويُعتبر الحذف - حتى وإن كان جزئياً - كافياً لتشديد العقوبة وتحديد المسؤولية الجنائية للفاعل. ومن الملاحظ أنّ المشرع الجزائري لم يشترط أن يترتب على هذا الحذف تعطيل للنظام أو إحداث ضرر فعلي به، بل يكفي وقوع الحذف في معطيات النظام لتطبيق العقوبة. ويعكس هذا التوجّه حرص المشرع على مكافحة مختلف أشكال الاعتداءات على الأنظمة المعلوماتية، بما فيها الأفعال التي قد لا تؤدي إلى تعطيل النظام بالكامل، لكنها قد تؤثر سلباً على سير عمله أو أدائه ولو جزئياً.

- الإخلال بسير نظام المعالجة عن طريق التغيير: يُعتبر كذلك جزءاً من جريمة التدخل غير المشروع في النظام، إذ يقوم الجاني بتعديل المعطيات داخل النظام دون الحصول على إذن قانوني. وقد يحدث هذا التغيير تشويشاً في سير عمل النظام أو يؤدي إلى تعطيله جزئياً، حتى لو كان الهدف من التغيير - في الظاهر - تحسين أداء النظام. ومن المهم أن نفهم أنّ الجريمة تقوم على التدخل غير المشروع بحدّ ذاته، بغضّ النظر عن النتيجة النهائية لهذا التغيير. ومع ذلك، يمكن للقضاء أن يأخذ في اعتباره مدى تأثير التغيير على سير عمل النظام عند تقدير العقوبة، بحيث تتضاعف العقوبة إذا أدّى التغيير إلى تعطيل النظام أو إفساده فعلياً.

لذلك، ينبغي تفسير النص القانوني بحيادية وبما يتفق مع السياق القانوني العام ومبادئ القانون الجنائي، مع التركيز على الفعل غير المشروع في ذاته دون النظر إلى النتائج المحتملة له (شهرة، 2009-2010، صفحة 95).

- التخريب: تُعدّ جريمة التخريب داخل نظام المعالجة الآلية من أخطر الأفعال، حيث يقوم الجاني بإحداث أضرار جسيمة بالنظام بهدف تعطيله عن أداء مهامه الطبيعية. وقد يشمل التخريب تدمير أو تعطيل أجزاء محدّدة من النظام بحيث يتعدّر استعادتها أو إصلاحها بسهولة. ولهذا السبب يُعتبر التخريب أخطر من التغيير أو الحذف، نظراً لأنه يؤدي إلى شلل النظام بالكامل وعدم قدرته على أداء وظائفه المعتادة. ومع ذلك، يتوجّب على القضاء إثبات توافر القصد الجنائي لتحميل الجاني

المسؤولية؛ إذ يمكن للمتهم دائماً الدفع بوجود ظروف تقنية أو قوة القاهرة خارجة عن إرادته تجعله غير قادر على السيطرة على أفعاله.

وبوجه عام، تُصنّف هذه الجريمة بناءً على النتيجة النهائية للتدخل غير المشروع وتأثيره على سير عمل النظام، سواءً كانت النتيجة تغييرات أو حذفاً أو تخريباً. ومن الضروري أن يراعي القضاء جميع الملبسات والعناصر المؤثرة عند تحديد العقوبة المناسبة للمتهم (قارة، 2007، صفحة 114).

المطلب الثاني: حماية الأنظمة المعلوماتية؛ تجريم الاعتداء العمدي على سير نظام المعالجة وحتمية تطوير التشريع الجزائري

إن جريمة التعديل أو التخريب في نظام المعالجة الآلية للمعطيات تُعد من أخطر الجرائم الإلكترونية المستحدثة، والتي تشهد انتشاراً متزايداً في العصر الرقمي الراهن. ورغم خطورة هذه الجريمة، إلا أنّ العديد من التشريعات ما تزال لا تنص عليها بشكل صريح وواضح، مما يفتح الباب أمام التأويلات والتفسيرات القضائية المتعددة.

وتكمن خطورة هذه الجريمة في كونها تُشكّل تهديداً مباشراً للأمن السيبراني وخصوصية البيانات الإلكترونية، فضلاً عن تسببها بخسائر مالية جسيمة وانعكاسات سلبية على الأفراد والمؤسسات على حدّ سواء، ومن هنا تبرز الحاجة الملحة لتدخل التشريعات الوطنية والدولية، عبر تشديد العقوبات على مرتكبي هذا النوع من الجرائم لضمان الردع الفعّال وتحقيق العدالة الرقمية.

كما إن إدراج التعديل والتخريب في إطار التجريم وضمن نصوص القانون الجنائي يُعد خطوة إيجابية تؤكد جدية المشرّع في مكافحة الجرائم الإلكترونية وتعزيز الحماية القانونية للبيئة الرقمية. ويهدف الجاني من وراء ارتكاب هذه الأفعال إلى تعطيل سير نظام المعالجة أو إضعاف قدرته على أداء مهامه بكفاءة، من خلال ارتكاب سلسلة من الأفعال المندرجة تحت مسمى «الإعاقة».

وتشمل هذه الأفعال جميع الأنشطة التي قد تُوقف النظام جزئياً أو كلياً عن العمل، بما في ذلك التدخل في برامج معيّنة ضمن النظام. وبالعودة إلى التقرير



التفسيري لاتفاقية بودابست لمكافحة الجريمة المعلوماتية، يُشترط أن تصل الإعاقة إلى مستوى من الخطورة يحرم صاحب النظام من استخدامه بشكل طبيعي. كما يُدرج ضمن ذلك أعمال حجب الخدمة أو التشفير بنية خبيثة، رغم أن القانون الفرنسي لم يتناول هذه الحالات بتفصيل خاص. وبناءً على ذلك، يُعتبر حدوث الإعاقة سواء أكانت دائمة أو مؤقتة أو متقطعة أمراً مخالفاً للقانون، إذ إنّ توقفاً بسيطاً في نظام المعالجة قد يخلّف خسائر باهظة (عطالله، 2007، صفحة 128).

ويدخل ضمن الإخلال أيضاً كل فعل من شأنه المساس بحسن سير نظام المعالجة، كالأعمال التي تؤثر على قدرة النظام على أداء مهامه بشكل طبيعي، سواء عبر تقليل سرعته أو عرقلة إتمام العمليات المبرمج لأجلها أو حتى عبر زيادة سرعته بما يُربك سير العمل (حجازي، 2004، صفحة 41).

ويشير بعض شراح قانون العقوبات الفرنسي إلى أنّ أفعال الإعاقة أو التعطيل يمكن وصفها بأنها «عرقلة» أو «إعاقة»، غير أنّ هذا الوصف لا يعكس تماماً جوهر الجريمة؛ إذ إنّ الإعاقة قد تعني مجرد إبطاء العمل، بينما المقصود الحقيقي هنا هو تعطيل النظام بالكامل عن أداء وظائفه، لذا فإن المصطلح الأكثر دقة وتعبيراً عن طبيعة الفعل هو «تعطيل النظام» لا مجرد عرقلته.

وعلى خلاف الأفعال الأخرى مثل الدخول أو البقاء غير المشروع في النظام، يتطلب هذا الفعل تحديداً أن يكون التعطيل أو الإخلال بسير النظام قد تمّ عن قصد وبإرادة متعمدة. لذلك يُصنّف ضمن الجرائم العمدية التي لا تتحقق إلا بتوافر القصد الجنائي لدى الفاعل.

وانطلاقاً من التحليل السابق، يبدو من الضروري أن يتدخل المشرع الجزائري باستحداث نص قانوني صريح وواضح يُجرّم الأفعال التي تعيق أو تعطل عمل النظام، ويكون نصّه كالتالي: "يعاقب على الأفعال التي تعوق أو تعطل سير نظام المعالجة الآلية للمعطيات أو البيانات بالحبس من سنة إلى خمس سنوات والغرامة من 200.000 إلى 1.000.000 دج"، وذلك اتساقاً مع التزام الجزائر بالاتفاقية العربية سالفه الذكر.

المبحث الثاني: أمن المعلومات في مواجهة الجريمة: نحو حماية جنائية شاملة للمعطيات الإلكترونية

إنَّ المشرّع الجزائري لم يقتصر في حمايته للأنظمة المعلوماتية على الجانب المادي المتمثل في البرامج والتطبيقات فقط، بل امتد نطاق هذه الحماية ليشمل المعطيات والمعلومات المخزّنة ضمن هذه الأنظمة، إدراكاً منه لخطورة الاعتداءات التي تستهدف محتوى البيانات وخصوصيتها.

وفي هذا الإطار، يُطلق بعض الفقهاء على هذا النوع من الجرائم مسمّى «القرصنة المعلوماتية»، بالنظر إلى طبيعتها الاعتدائية التي تنال من جوهر النظام المعلوماتي وبياناته الجوهرية.

وتتعدّد صور هذه الجريمة وفقاً للسلوك المرتكب، حيث قد تتحقق في شكل التلاعب بالمعطيات داخل نظام المعالجة الآلية للمعطيات (مطلب أول)، كما قد تظهر في شكل التصرف في تلك المعطيات بصفة غير مشروعة أو بدون إذن قانوني (مطلب ثاني)، وذلك كلّه بما يشكلّ مساساً مباشراً بسرية البيانات وسلامتها ويستوجب تدخل المشرّع بنصوص واضحة لردع مرتكبيها.

المطلب الأول: الأبعاد الجنائية للتلاعب في أنظمة المعالجة الآلية

نصّ المشرّع الجزائري صراحةً على هذه الجريمة في المادة 394 مكرر 1 من قانون العقوبات، إذ جاء فيها:

«يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدّل بطريق الغش المعطيات التي يتضمنها»

ويلاحظ أن الأفعال المجرّمة هنا تتعلق حصرياً بالمعطيات داخل نظام المعالجة الآلية، أي البيانات التي تم إدخالها في النظام بهدف معالجتها وتحويلها إلى رموز وإشارات تجسّد المعلومة، وبناءً عليه، فإن هذا النص لا ينطبق على المعلومة في حدّ ذاتها إذا كانت محفوظة خارج النظام، كالمعلومات المحمّلة على قرص مدمج، لأنّها بذلك تصبح خارج نطاق المعالجة أو لم تدخل فيه بعد.

وبالتالي، فإن الحماية الجنائية المقررة وفق هذا النص تشمل فقط المعلومات التي ما تزال داخل النظام أو في مرحلة المعالجة، ويرى بعض الفقهاء أنّ هذه الحماية تبقى قائمة طالما أنّ المعلومة لم تُستخرج من النظام ولا تزال جزءاً من عملية المعالجة (حجازي، 2004، صفحة 45).

ويتضح كذلك من المادة المذكورة أن الأفعال المجرّمة تتحقق عبر ثلاثة صور أساسية:

1- دخال معطيات في نظام المعالجة:

ويقصد به إضافة بيانات جديدة إلى النظام الآلي، وهو سلوك يُعد من صميم الغش المعلوماتي، إذ يهدف الجاني من خلاله إلى إدخال بيانات وهمية أو غير حقيقية بهدف تغيير الحقيقة أو التلاعب بها (حجازي، 2004، صفحة 46).

يترتب عن ذلك المساس بصحة المعلومات ونسبتها وقيمتها، وعادةً ما يقع هذا الفعل من قبل أشخاص لهم صلاحية الوصول للنظام مثل مسؤولي أقسام المحاسبة أو موظفي المواقع الإلكترونية. وغالباً ما تُرتكب هذه الجريمة في البنوك والمؤسسات المالية؛ على سبيل المثال، تَوَرَّط موظف بأحد الفروع المصرفية في تحويل وهي بمبلغ يقارب 7 ملايين فرنك فرنسي إلى حسابه الشخصي، بعد تلاعبه ببيانات الذاكرة الخاصة بالحاسب الآلي (حجازي، 2004، صفحة 47).

ومما يجدر التنويه إليه أنّ المشرع لم يشترط تحقق ضرر فعلي من فعل الإدخال، إذ يكفي وقوع الإدخال ذاته حتى لو لم يترتب عليه تغيير أو ضرر، ولا يُشترط صحة البيانات المدخلة من عدمها.

2- إزالة معطيات من نظام المعالجة:

ويقصد بها محو جزء أو كل من البيانات المخزنة داخل النظام، أو إتلاف الحوامل المادية لهذه البيانات. ويتم ذلك عادةً باستخدام برامج متطورة قادرة على مسح البيانات بشكل كامل (مسعود، 2008، صفحة 102).

3- تعديل معطيات داخل نظام المعالجة:

ويُقصد بالتعديل إجراء أي تغيير أو تحريف للبيانات القائمة داخل النظام، أو استبدالها ببيانات أخرى. على سبيل المثال، في فرنسا، وُجه الاتهام لأحد الموظفين بعد قيامه بتعديل السجلات الورقية للشركة وإعادة إدخالها إلى النظام الآلي مع البيانات المعدلة (عطالله، 2007، صفحة 135)، كما تشمل التطبيقات الشائعة اقتطاع أجزاء بسيطة من الحسابات الجارية وتحويلها لحساب خاص، وهي حيلة يصعب اكتشافها نظرًا لضالة المبالغ المقتطعة لكنها تدر أرباحًا ضخمة بمرور الوقت. ومن صور ذلك أيضًا، إقدام أحد المجرمين في ألمانيا على زرع فيروس في شبكة معلوماتية لجمع بيانات المستخدمين والتلاعب بمحتواها (الحليم، 2009، صفحة 17).

وجدير بالذكر، أن هذه الجريمة تُعد من الجرائم العمدية التي لا تتحقق إلا بتوافر القصد الجنائي المتمثل في العلم والإرادة. فقد نصّ المشرع صراحةً على عبارة «بطريق الغش»، وهو ما يستلزم ثبوت سوء نية الجاني وعلمه بأن أفعاله غير مشروعة، فلا تتحقق الجريمة إذا تم الفعل عن طريق الخطأ أو بإذن المالك الشرعي للبيانات.

وتوضح التطبيقات القضائية الفرنسية ذلك؛ فقد قضت محكمة الاستئناف ببراءة متهم باع مجلة مرفقة بقرص ممغنط يحتوي فيروسًا أُلّف ببيانات المشتري، لعدم علمه بوجود الفيروس، ومن ثمّ انتفاء نية الغش (عطالله، 2007، صفحة 138).

ومن ثمّ، يشترط لقيام القصد الجنائي أن تتجه إرادة الجاني إلى الإدخال أو الإزالة أو التعديل، مع علمه أن فعله غير مشروع وأنه يمسّ بحقوق الغير، وتُشير محكمة النقض الفرنسية إلى أنّ نية الغش يمكن استخلاصها من طبيعة الوسيلة المستعملة كزرع فيروس أو استخدام «قنبلة معلوماتية» (عطالله، 2007، صفحة 138).

يتضح من التحليل أنّ المشرع قد أحسن صياغة النص في شقّه المادي والمعنوي عبر تحديد الأفعال بدقة واشتراط العمدية، إلا أنّ العقوبة المقررة تبدو غير متناسبة مع خطورة هذه الجرائم وآثارها الجسيمة، خصوصاً في بيئة المعاملات التجارية الإلكترونية التي تقوم على الثقة وسرية البيانات. وعليه، يُقترح تعديل العقوبة برفعها إلى مستوى الجنائية لتكون المادة 394 مكرراً 1 كما يلي:

«يعاقب بالسجن من خمس سنوات إلى عشر سنوات وبغرامة من 1.000.000 دج إلى 7.000.000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدّل بطريق الغش المعطيات التي يتضمنها».

المطلب الثاني : الحماية الجنائية للمعلومات من الاستخدام غير الشرعي

لقد تطرّق المشرع الجزائري إلى تجريم التصرف غير المشروع في المعطيات خارج نظام المعالجة الآلية، وذلك بموجب المادة 394 مكرراً 2 من قانون العقوبات. ويهدف هذا النص إلى حماية المعطيات في أي حالة أو موضع كانت فيه، سواء كانت محفوظة على أقراص ممغنطة أو مرسلة عبر منظومات معلوماتية، دون اشتراط بقائها داخل نظام المعالجة نفسه.

ويُظهر نص المادة 394 مكرراً 2 أن الركن المادي لهذه الجريمة يتكوّن من صورتين رئيسيتين:

1- التصرف في المعطيات ذات الصلة بالجرائم الماسة بأنظمة المعالجة

ويتخذ هذا التصرف صوراً متعددة، منها:

- التصميم: كتصميم فيروسات أو قنابل إلكترونية أو مواقع وهمية بقصد الاحتيال. مثال ذلك ما أوردته محكمة عنابة في حكمها رقم 05637/10 المؤرخ في 2010/06/28 بشأن طريقة تحويل الأموال من خلال إنشاء مواقع إلكترونية شبيهة بالمواقع الرسمية للبنوك، حيث يقع الزبائن ضحية لهذه المواقع فيقدمون بياناتهم البنكية السرية للقرصنة دون علمهم، كما أشار حكم محكمة باتنة في القضية ذاتها إلى قيام المتهم بتصميم مواقع إنترنت بطرق غير شرعية.

- البحث: أي السعي لاكتشاف طرق التصميم أو تطوير أدوات التنفيذ، وقد صيغت العبارة بصيغة عامة لتشمل جميع الأبحاث ذات العلاقة (محمد، 2011/2010).

التجميع: ويقصد به جمع معطيات يمكن استخدامها لاحقاً في ارتكاب الجرائم الإلكترونية (محمد، 2011/2010، صفحة 234).

- التوفير: أي وضع المعطيات في متناول الآخرين، كما ورد في حكم محكمة باتنة رقم 05272/10 المؤرخ في 2010/06/01، حيث قام المتهم بنشر معطيات تخص شركات مختلفة وأقرّ بإرسالها إلى أحد القراصنة مع التزامه بعدم نشر صورة تخص شركة أمريكية (محمد، 2011/2010، صفحة 236).

النشر: وهو إذاعة المعطيات بوسائل تتيح وصولها لعدد كبير من الأشخاص، بما يشكّل خطورة أكبر لوقوع الجريمة (أحمد، 2007، صفحة 81).

- الإتجار: أي بيع المعطيات أو تقديمها للغير مقابل عوض مالي، واستدلّت المحاكم بذلك على حالات واقعية مثل قضية المواقع الوهمية التي عالجتها محكمة عنابة، حيث تبين أن المتهم تلقى تحويلات مالية من كندا نتيجة بيعه لموقع بنك كندي وهي بهدف خداع الزبائن (حكم محكمة عنابة رقم 05637/10 بتاريخ 2010/06/28). ويُميز القانون هنا بين الإتجار الذي يتم بمقابل، وفعل التوفير الذي قد يكون بلا مقابل.

2- التصرف في المعطيات المتحصلة من الجرائم الماسة بأنظمة المعالجة وتشمل هذه الصورة امتلاك المعطيات الناتجة عن جرائم سابقة كإبقائها أو تحميلها أو حفظها في حواسيب خاصة، كما يشمل السلوك أيضاً إفشاء هذه المعطيات أو نشرها للغير، وهو ما يُخرجها من حيازة الجاني ويجعلها عرضة للاستخدام الإجرامي مجدداً.

وفيما يخص الطبيعة القانونية لهذه الجريمة فإنها تصنّف ضمن الجرائم العمدية، إذ يشترط القانون توافر القصد الجنائي المتمثل في علم الجاني بطبيعة

المعطيات وخطورتها، مع اتجاه إرادته إلى التصميم أو البحث أو التجميع أو التوفير أو النشر أو الإتجار بها (محمد، 2010/2011).

يتحقق القصد الجنائي في الصورة الثانية أيضاً إذا علم الجاني بأن المعطيات متحصلة من إحدى الجرائم الماسة بأنظمة المعالجة، بغض النظر عن الغرض من استخدامها لاحقاً.

كما يُلاحظ أن المشرع لم يكتفِ باشتراط توافر العمد بل أضاف قيد "الغش" للدلالة على نية الاحتيال والتدليس، إلا أنّ بعض الفقه يرى أن الاكتفاء بكلمة «عمداً» يحقق الغرض ويمنع إفلات الجناة من العقاب بحجة عدم ثبوت الغش صراحة.

ويُلاحظ كذلك أن المشرع حدّد الأفعال المكوّنة للركن المادي بدقة، غير أنّ العقوبة المقررة تظل غير كافية بالنظر إلى خطورة هذه الأفعال خاصة في ظل الانتشار الواسع للجرائم المعلوماتية.

وعليه، يُقترح إعادة صياغة المادة 394 مكرر2 من قانون العقوبات على النحو الآتي:

"يعاقب بالحبس من ستة أشهر إلى خمس سنوات وبغرامة مالية من 1.000.000 دج إلى 5.000.000 دج كل من يقوم عمداً بما يأتي:

تصميم أو بحث أو تجميع أو وضع تحت التصرف أو نشر أو إتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

حيازة أو إفشاء أو نشر أو إتجار أو استعمال لأي غرض كان للمعطيات المتحصلة من إحدى الجرائم المنصوص عليها في هذا القسم".

الخاتمة

عند النظر في جهود الجزائر لمكافحة الجريمة المعلوماتية، يتّضح وجود تفاوت في مستويات الحماية التي أقرّها المشرع الوطني؛ إذ اكتفى بسنّ بعض الأحكام ضمن قانون العقوبات لمواجهة الجرائم المعلوماتية والإلكترونية بوجه عام، ومن

أبرزها: تجريم الدخول أو البقاء غير المشروع في نظام المعالجة، وتجريم التصرف غير المشروع في سير عمل هذا النظام، فضلاً عن تجريم المساس بالمعلومات والمعطيات داخله. غير أنّ هذه الحماية تظلّ جزئية، حيث لم يشمل المشرع بعض الأفعال التي تُعدّ من أبرز صور الجرائم المعلوماتية المعاصرة، مما يخلق فراغاً تشريعياً قد يُسهّل ارتكاب هذه الأفعال دون رادع قانوني رادع.

في ضوء ذلك، يظهر جلياً أن المنظومة الحالية تفتقر إلى التكامل الذي يستجيب لطبيعة التطور السريع للجريمة المعلوماتية وما تستلزمه من حماية خاصة للبيانات والمعلومات الشخصية. لذلك، نرى من الضروري أن يتدارك المشرع هذا النقص من خلال تبني قانون خاص لمكافحة الجريمة المعلوماتية يُنظّم بدقة جميع الأفعال المجرّمة ويوفّر إطاراً ردعياً متكاملًا يتماشى مع المعايير الدولية وأفضل الممارسات المقارنة.

ويمكن في هذا الشأن أن تعتمد صياغة هذا القانون على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات كمرجع رئيسي، ما من شأنه تحقيق الانسجام التشريعي بين الدول العربية وتسهيل التعاون القضائي في هذا المجال. كما نتطلع إلى تحويل أحكامها إلى تشريع وطني فعّال يُسهم في رفع مستوى الحماية المعلوماتية ويعزّز الثقة في البيئة الرقمية والمعاملات الإلكترونية.

قائمة المصادر والمراجع:

النصوص القانونية

1. قانون العقوبات الجزائري
2. قانون رقم 04-09 المؤرخ في 14 شعبان عام 1430 الموافق 05 غشت 200. يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ع 47.
3. إتفاقية بودايست للإجرام المعلوماتي لسنة 2001.
- الكتب:
4. أسامة أحمد المناعسة، جرائم الحاسب الآلي والانترنت، دار وائل، ط1، عمان، 2001.
5. أمال قارة، الحماية الجنائية للمعلوماتي في التشريع الجزائري، دار هومة للنشر، ط 2007.



6. بن عبد الله الأزرق، نظام المعلوماتية في القانون الجزائري، المؤتمر السادس حول البيئة المعلوماتية الآمنة، جمعية المكتبات والمعلومات، السعودية، الرياض، 2010.
 7. جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الجرائم الناشئة عن الحاسب الآلي، الكتاب الأول، دار النهضة العربية، ط 1992.
 8. سليم عبد الله الخيوري، الحماية القانونية لمعلومات شبكة الانترنت، منشورات الحلبي الحقوقية، ط 2011، 1.
 9. عبد الغني محمد عطالله، الحماية الجنائية للتعاملات الالكترونية، دار الجامعة الجديدة، 2007.
 10. عبد الفتاح بيومي حجازي، الحماية الجنائية لنظام، دار الفكر الجامعي، الإسكندرية، 2004.
 11. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير المعلوماتي في جرائم الكمبيوتر والانترنت، دار الكتب القانونية مصر، ط 1، 2001.
 12. علي عبد القادر القهوجي، الحماية الجنائية لبرامج الكمبيوتر، الدار الجامعية للطباعة والنشر، بيروت، 1999.
 13. هلالى عبد الإله أحمد، اتفاقية بودابست لمكافحة جرائم المعلومات، دار النهضة العربية، القاهرة، 2007.
- رسائل الدكتوراه والمجستير
- 10 - خثير مسعود، الحماية الجنائية لبرامج الحاسب الآلي، مذكرة ماجستير، كلية الحقوق، جامعة أبي بكر بلقايد تلمسان، 2008.
 - 11 - شول بن شهرة، الحماية الجنائية للتجارة الالكترونية، رسالة دكتوراه، جامعة محمد خيضر بسكرة، 2009/2010.
 - 12 - خليفة محمد، جريمة التواجد غير المشروع في الأنظمة المعلوماتية، رسالة دكتوراه كلية الحقوق جامعة باجي مختار عنابة، 2010/2011.
- المداخلات العلمية
- 13 - رامي عبد الحليم، جرائم الاعتداء على أنظمة المعالجة الآلية للمعلومات، مجموعة الملتقى الدولي حول التنظيم القانوني للانترنت...، مجلة دراسات، 2009.
- محمد أحمد طه، المسؤولية الجنائية عن الاستخدام غير المشروع لبطاقة الائتمان، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، جامعة الإمارات العربية المتحدة، 2003.