التهديدات السيبرانية، إتلاف معطيات نظم الحماية الاجتماعية أنموذجا

Cyber threats; Destruction of social protection systems data as an example

عبد الإله شني Chenni Abdelilah

دكتور في القانون الخاص

ahlamchenni82@gmail.com

الملخص باللغة العربية

لقد أمسى العالم أكثر اعتمادا على التكنولوجيا التي ترتب عليها ازدياد إنشاء البيانات الرقمية؛ حيث باتت تشكل بعدا استراتيجيا للدول؛ فضلا عن اعتبارها أساس تطور هذه الأخيرة؛ فجهاز الحاسوب والأنترنت أصبحا جزءا لا يتجزأ من حياتنا المعاصرة؛ إذ يعتمد عليهما في كل مناحي الحياة؛ بدءا من الترفيه والتواصل إلى الخدمات العمومية والمصرفية؛ والمعاملات التجارية وغيرها كثير...

ولا مراء أن المغرب بات يشهد تحولا رقميا باهرا؛ في مختلف القطاعات؛ ولعل المرفق العمومي أكبر المستفيدين من هذه الطفرة التكنولوجية؛ فرقمنة الإدارة العمومية لا شك أنها أسهمت بشكل كبير في الانتقال من المحتوى الورقي إلى المستندات الإلكترونية؛ فضلا عن توفير المنصات الرقمية التي تعتمد في تدبير العديد من الأوراش منها ورش الحماية الاجتماعية؛ حيث أطلقت الحكومة المغربية منصة رقمية لتدبير وتنزيل هذا الورش من خلال نظم معلوماتية وطنية. وبالرغم من الدور الإيجابي المشرق لهذه النظم المعلوماتية إلا أنها قد تطالها السلوكات المجرمة من قبيل الجرائم الإلكترونية التي تعرضت إليها العديد من المنصات الإلكترونية، كسرقة المعلومات، والدخول غير المرخص له إلى النظام المعلوماتي، وتغيير البيانات؛ وعرقلة سير النظام المعلوماتي؛ علاوة على تدمير المعطيات المخزنة في هذه النظم.

وفي هذا السياق؛ فإن جريمة الإتلاف المعلوماتي تعد من أخطر الجرائم السيبرانية التي تشكل تحد للجهات الساهرة على تدبير وحماية النظم المعلوماتية التي تدبر ورش الحماية الاجتماعية؛ وبناء على ذلك؛ فإن موضوع "التهديدات السيبرانية؛ إتلاف معطيات نظم الحماية الاجتماعية أنموذجا" يثير إشكالية تتعلق بمدى قدرة النصوص القانونية المرتبطة بالمس بنظم المعالجة الآلية للمعطيات، خاصة الفصل 607-6 من مجموعة القانون الجنائي المغربي، على مواجهة جريمة إتلاف المعطيات الخاصة بالنظم المعلوماتية المخصصة للحماية الاجتماعية.

لمعالجة الموضوع المشار إليه؛ ارتأينا مقاربة الإشكالية المثارة وفق تصور، نراهن تعميق البحث فيه، انطلاقا من مبحثين اثنين؛ حيث تناولنا في المبحث الأول الإطار العام لجريمة إتلاف معطيات نظم الحماية الاجتماعية؛ من حيث المفهوم والخصائص وتمييز هذه الجرائم عن بعض المؤسسات المشابهة، ثم تطرقنا بعد ذلك إلى نظامها القانوني من خلال المبحث الثاني؛ حيث توقفنا عند الأركان التكوينية لهذه الجريمة؛ والعقوبات الناجمة عن قيام المسؤولية الجنائية للجريمة محل الدراسة.

الملخص باللغة الانجليزية

The world has become more dependent on technology, which has led to an increase in the creation of digital data; it has become a strategic dimension for countries; in addition to being considered the basis for the development of the latter; the computer and the Internet have become an integral part of our contemporary life; as we depend on them in all aspects of life; starting from entertainment and communication to public and banking services; commercial transactions and many others...

There is no doubt that Morocco is witnessing a remarkable digital transformation; in various sectors; and perhaps the public service is the biggest beneficiary of this technological boom; the digitization of public administration has undoubtedly contributed significantly to the transition from paper content to electronic documents; in addition to providing digital platforms that are relied upon in the management of many projects, including social protection projects; where the Moroccan government launched a digital platform to manage and download this project through national information systems. Despite the bright positive role of these information systems, they may be affected by criminal behaviors such as cybercrimes that many electronic platforms have been exposed to, such as theft of information, unauthorized access to the information system, changing data; and obstructing the operation of the information system; In addition to destroying the data stored in these systems.

In this context, the crime of information destruction is one of the most dangerous cybercrimes that pose a challenge to the authorities responsible for managing and protecting the information systems that manage social protection workshops; Accordingly, the topic of "Cyber threats; Destruction of data of social protection systems as a model" raises a problem related to the extent of the ability of legal texts related to harming automated data processing systems, especially Article 607-6 of the Moroccan Penal Code, to confront the crime of destroying data specific to information systems dedicated to social protection.

To address the aforementioned topic, we decided to approach the raised problem according to a concept, which we bet on deepening research into, based on two topics; where we addressed in the first topic the general framework of the crime of destroying data of social protection systems; in terms of concept and characteristics and distinguishing these crimes from some similar institutions, then we addressed its legal system through the second topic; where we stopped at the constitutive elements of this crime; And the penalties resulting from the establishment of criminal responsibility for the crime under study.

مقدمة:

شهدت المملكة المغربية إصلاحات تشريعية متعددة في مجال الحماية الاجتماعية؛ حيث تم توسيع صلاحيات الصندوق الوطني للضمان الاجتماعي؛ لتشمل علاوة على العمل التابع فئات أخرى من المهنيين والعمال المستقلين والأشخاص غير الأجراء الذين يزاولون نشاطا خاصا؛ بالإضافة إلى فئات العاملات والعمال المنزليين.

ولبناء مجتمع تسوده العدالة الاجتماعية، والمجالية المستمدة من الرؤية المولوية السامية؛ في تنزيل العديد من البرامج الاجتماعية للنهوض بالعنصر البشري باعتباره الحلقة الأساس في التنمية، وفي ضوء ما ورد في الفصل 31 من دستور 2011[1] الذي ينص على أنه:" تعمل الدولة والمؤسسات العمومية والجماعات الترابية، على تعبئة كل الوسائل المتاحة، لتيسير أسباب استفادة المواطنين والمواطنات، على قدم المساواة، من الحق في:

- العلاج والعناية الصحية؛
- الحماية الاجتماعية والتغطية الصحية، والتضامن التعاضدي أو المنظم من لدن الدولة؛

سن المشرع المغربي القانون الإطار رقم 09.21 المتعلق بالحماية الاجتماعية[2] الذي يشمل حسب ما نصت عليه المادة الثانية منه:

- الحماية من مخاطر المرض؛
- الحماية من المخاطر المرتبطة بالطفولة وتخويل تعويضات جزافية لفائدة الأسر التي لا تشملها هذه الحماية؛
- الحماية من المخاطر المرتبطة بالشيخوخة؛
- الحماية من مخاطر فقدان الشغل.

وللتنزيل الأمثل لورش الحماية الاجتماعية؛ كان من اللازم الاستفادة من التطور التكنولوجي الذي تشهده المملكة المغربية؛ لا سيما على مستوى الرقمنة التي تشكل آلية لمواكبة هذا الإصلاح، وتسريع تعميمه. وفي هذا السياق أطلقت الحكومة المغربية المنصة الرقمية لتدبير وتنزيل هذا الورش من خلال نظم معلوماتية وطنية. وبالرغم من الدور الإيجابي المشرق لهذه النظم المعلوماتية إلا أنها قد تطالها السلوكات المجرمة من قبيل الجرائم الإلكترونية التي تعرضت إليها العديد من النظم المعلوماتية، كسرقة المعلومات، والدخول غير المرخص له إلى النظام المعلوماتي، وإتلاف المعلومات...

[1] ظهير شريف رقم 1.11.91 صادر في 27 من شعبان 1432 (29 يوليو 2011)، منشور بالجريدة الرسمية عدد 5964 مكرر بتاريخ 28 شعبان 1432 (30 يوليو 2011).

[2] ظهير شريف رقم 1.21.30 صادر في شعبان 1442 (23 مارس 2021) بتنفيذ القانون- الإطار 09.21 المتعلق بالحماية الاجتماعية، الجريدة الرسمية عدد 6975 -22 شعبان 1442 (5 أبريل 2021)، الصفحة 2178.

وفي هذا الصدد؛ تعد جريمة الإتلاف المعلوماتي من أخطر الجرائم المهددة لاشتغال النظم المعلوماتية المدبرة لورش الحماية الاجتماعية من زاوية؛ وللمعطيات والبرامج المخزنة بها من زاوية أخرى، وبالتالي كان لزاما علينا البحث في إشكاليات هذه الجريمة التي ستخلق تحديا كبيرا في مواجهة المقتضيات التشريعية سواء التقليدية والقواعد الخاصة.

وغني عن البيان؛ أن المشرع المغربي قد أقدم على سن تشريعات لمكافحة الجرائم المعلوماتية عامة وجريمة الإتلاف المعلوماتي خاصة، مستندا في ذلك على الاتفاقيات الدولية والإقليمية في إطار التعاون الدولي، ومنها اتفاقية بودابست[1] سنة 2003 وكذا الاتفاقية العربية لمكافحة جرائم تقنية المعلومات[2] سنة 2010؛ فضلا عن الاتفاقيات الثنائية التي تروم تفعيل آليات التعاون الدولي المتجسدة في التعاون الأمني والقضائي من خلال الإنابة القضائية، وتسليم المجرمين، والتعاون على مستوى الأجهزة الأمنية.

بناء عليه؛ ولمكافحة جريمة الإتلاف المعلوماتي تضمنت مدونة الجمارك[3] الصادرة في 5 يونيو 2000 تجريم كل عمل يتعلق بإتلاف بيانات أو أكثر في النظم المعلوماتية للإدارة من خلال الفقرة السابعة من المادة 281، علاوة على ذلك سن المشرع المغربي القانون 07.03 الصادر سنة 2003 المتعلق بالإخلال بسير نظم المعالجة الآلية للمعطيات[4]؛ حيث تطرق هذا القانون للجريمة المذكورة بمقتضى الفصل 607-6 الذي ينص على أنه:" يعاقب بالحبس من سنة إلى ثلاث سنوات وبالغرامة من 10.000 إلى 200.000 درهم أو بإحدى هاتين العقوبتين فقط كل من أدخل معطيات في نظام المعالجة الآلية للمعطيات أو أتلفها أو حذفها منه أو غير المعطيات المدرجة فيه، أو غير طريقة معالجتها أو طريقة إرسالها عن طريق الاحتيال."

كذلك؛ إذا كانت جريمة الإتلاف الماسة بنظم المعالجة الآلية للمعطيات لها علاقة عمدا بمشروع فردي أو جماعي يهدف إلى المس الخطير بالنظام العام بواسطة التخويف أو الترهيب أو العنف؛ فإنها تكيف فعلا إرهابيا يعاقب عليه بموجب القانون 03.03 المتعلق بمكافحة الإرهاب[5].

---

[1] تم إبرام اتفاقية بودابست لمكافحة الإجرام المعلوماتي بتاريخ 23 نونبر 2001 من قبل الدول الأعضاء في مجلس أوروبا، وقد صادق عليها المغرب سنة 2014 (ظهير شريف 1.14.85 صادر في 12 رجب 1435 (12 ماي 2014) بتنفيذ القانون رقم 136.12 الموافق بموجبه على اتفاقية الجرائم المعلوماتية، الموقعة ببودابست في 23 نوفمبر 2001 وعلى البروتوكول الإضافي لهذه الاتفاقية، الموقع بستراسبورغ في 28 يناير 2003، الجريدة الرسمية ع 6260 بتاريخ 29 رجب 1435 (29 ماي 2014)، الصفحة 4711.

[2] ظهير شريف رقم 1.13.46 صادر في فاتح جمادى الأولى 1434 (13 مارس 2013) بتنفيذ القانون رقم 75.12 الموافق بموجبه على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، الموقعة بالقاهرة في 21 ديسمبر 2010، الجريدة الرسمية عدد 6140 الصادر بتاريخ 23 جمادى الأولى 1434 (4 أبريل 2013.

[3] ظهير شريف رقم 1.77.399 الصادر في 25 من شوال 1397 (9 أكتوبر 1977)، كما وقع تغييره وتتميمه، الجريدة الرسمية عدد 3392 مكرر بتاريخ 21 ذو القعدة 1397 (4 نونبر 1977)، الصفحة 3289.

[4] القانون رقم 07.03 بتميم مجموعة القانون الجنائي في ما يتعلق بالجرائم المتعلقة بنظم المعالجة الآلية للمعطيات، الصادر بتنفيذه ظهير شريف رقم 1.03.197 بتاريخ 16 من رمضان 1424 (11 نوفمبر 2003)؛ الجريدة الرسمية عدد 5171 بتاريخ 27 شوال 1424 (22 ديسمبر 2003)، الصفحة 4284.

[5] ظهير شريف رقم 1.03.140 صادر في 26 من ربيع الأول 1424 (28 ماي 2003) بتنفيذ القانون رقم 03.03 المتعلق بمكافحة الإرهاب، الجريدة الرسمية ع 5112 بتاريخ 27 ربيع الأول 1424 (29 ماي 2003)، ص1755.

وحرصا من المشرع المغربي على التصدي للجرائم السيبرانية؛ سن قانونا يتماشى وهذه الجرائم؛ ويتعلق الأمر بالقانون رقم 05.20[1] المتعلق بالأمن السيبراني الذي يتغيا وضع مجموعة من القواعد؛ والتدابير الأمنية الرامية إلى تعزيز أمن وصمود نظم معلومات إدارات الدولة والجماعات الترابية والمؤسسات والمقاولات العمومية، وكل شخص اعتباري خاضع للقانون العام، وكذا البنيات التحتية ذات الأهمية الحيوية التي تتوفر على نظم معلومات حساسة[2].

أهمية الدراسة:

في ضوء ما تقدم، يكتسي موضوع "التهديدات السيبرانية؛ إتلاف معطيات نظم الحماية الاجتماعية أنموذجا" أهمية متزايدة تتعلق بموضوع هام أفرزته وسائل التقنية الحديثة التي تُسَوِق الكثير لارتكاب الأفعال الإجرامية المستحدثة؛ وبالتالي الوقوف عند أهم الاتجاهات التشريعية الدولية والإقليمية المتخصصة في حماية النظم المعلوماتية، علاوة على ذلك؛ فإن أهمية هذا الموضوع تكمن في استلهام الحلول لما يثيره تنزيل ورش الحماية الاجتماعية من صعوبات تستهدف المعطيات المخزنة في النظم الإلكترونية المخصصة لذلك.

إشكالية الدراسة:

تأسيسا عليه؛ يثير الموضوع المشار إليه الإشكالية الآتية:

ما مدى قدرة النصوص القانونية المرتبطة بالمس بنظم المعالجة الآلية للمعطيات، خاصة الفصل 607-6 من مجموعة القانون الجنائي، على مواجهة جريمة إتلاف المعطيات الخاصة بالنظم المعلوماتية المخصصة للحماية الاجتماعية؟

الأسئلة الفرعية:

لمقاربة الإشكالية المثارة يقتضي منا الأمر الإجابة عن الأسئلة الآتية:

- كيف تناول الفقه والقانون والعمل القضائي مفهوم إتلاف معطيات النظم المعلوماتية؟
- ما هي وضعية الإتلاف المعلوماتي في التشريع المغربي والمقارن؟
- هل من خصوصية للأركان التكوينية لجريمة الإتلاف المعلوماتي في ضوء ورش الحماية الاجتماعية؟
- هل العقوبات المقررة في النصوص التشريعية كافية ردع الجناة المحتملين في جريمة الإتلاف المعلوماتي للمعطيات المخزنة في النظم المعلوماتية الخاصة بتدبير أوراش الحماية الاجتماعية؟

فرضية الدراسة:

[1] ظهير شريف رقم 1.20.69 صادر في 4 ذي الحجة 1441 (25 يوليو 2020) بتنفيذ القانون رقم 05.20 المتعلق بالأمن السيبراني، الجريدة الرسمية عدد 6904 – ذو الحجة 1441 (30 يوليو 2020)، الصفحة 4160-4166.

[2] انظر المذكرة التقديمية للقانون 05.20 المشار إليه والمتعلق بالأمن السيبراني، المنشورة على الموقع الرسمي لإدارة الدفاع الوطني: https://dgssi.gov.ma

من أجل مقاربة إشكالية الدراسة والتساؤلات المتفرعة عنها، نفترض أن النصوص التشريعية التي تستهدف حماية النظم المعلوماتية غير كافية لمواجهة جريمة الإتلاف المعلوماتي للنظم المدبرة لأوراش الحماية الاجتماعية، وهو ما يقتضي من المشرع المغربي الاستفادة من التقنينات المقارنة والاتفاقيات والمعاهدات الدولية والإقليمية التي تروم مكافحة الجرائم المستجدة، لا سيما الجريمة محل الدراسة.

الدراسات السابقة:

تجدر الإشارة في هذا الإطار؛ أن الدراسات السابقة بالرغم من تناولها للجرائم الإلكترونية من حيث التجريم والعقاب إلا أنها لم تتوسع في جريمة الإتلاف المعلوماتي خصوصا في ظل رقمنة أوراش الحماية الاجتماعية وما قد يتهددها من سلوكات غير مشروعة؛ خاصة جريمة إتلاف معطيات النظم المعلوماتية، وعليه سننطلق مما انتهت إليه هذه الدراسات السابق لسبر أغوار الجريمة المشار إليها.

منهج الدراسة:

في ضوء ما تقدم؛ ولفحص مدى صلاحية الفرضية المقترحة، سنعتمد في هذه الدراسة منهجا وصفيا تحليليا مقارنا، تبسيطا لمجال هذه الدراسة، وإبراز خصوصياتها، وذلك من خلال معالجة مختلف التساؤلات التي تثيرها الدراسة في الشق الموضوعي.

خطة الدراسة:

لمعالجة موضوع المداخلة؛ ارتأينا مقاربة الإشكالية المثارة وفق تصور، نراهن تعميق البحث فيه، انطلاقا من مبحثين اثنين؛ سنتناول في المبحث الأول الإطار العام لجريمة إتلاف معطيات نظم الحماية الاجتماعية، ثم نتطرق بعد ذلك إلى نظامها القانوني من خلال المبحث الثاني.

المبحث الأول: الإطار العام لجريمة إتلاف معطيات نظم الحماية الاجتماعية

تعد جريمة الإتلاف المعلوماتي من أخطر صور الجرائم المعلوماتية؛ نظرا للدور الهام الذي أصبح يقوم به الحاسب الآلي في كافة المجالات؛ حيث أضحى يجري من خلاله كم هائل من المعطيات ذات الآثار القانونية المهمة؛ ومنها معالجة بيانات ورش الحماية الاجتماعية؛ وفي هذا الإطار؛ سنقسم هذا المبحث إلى مطلبين نتناول في أولهما الإطار المفهومي لجريمة إتلاف معطيات نظم الحماية الاجتماعية؛ ونعالج في ثانيهما رأي الفقه والتشريع في هذا النوع من الجرائم المستجدة.

المطلب الأول: الإطار المفهومي لجريمة إتلاف معطيات نظم الحماية الاجتماعية

يقتضي منا الأمر تقسيم هذا المطلب إلى فقرتين؛ سنبرز في الفقرة الأولى مفهوم جريمة إتلاف معطيات نظم الحماية الاجتماعية؛ ثم نتطرق في الفقرة الثانية إلى خصائصها التي تتسم بها.

الفقرة الأولى: تعريف جريمة إتلاف معطيات نظم الحماية الاجتماعية

سنخصص هذه الفقرة لتعريف الإتلاف (أولا)؛ نظام المعالجة الآلية للمعطيات (ثانيا)؛ فضلا عن ذلك سنبين المقصود بنظم الحماية الاجتماعية (ثالثا)؛ ثم نميز جريمة الإتلاف عن بعض المؤسسات المشابهة (رابعا).

أولا: تعريف الإتلاف

الإتلاف لغة: من أتلف يتلف إتلافا، فهو متلف والمفعول متلف، ويقال: أتلف الفيضان الزرع أي: أفسده، وأعطبه، وأهلكه. ويقال: أتلف المال: أفناه إسرافا، ويقال: أتلف الشيء: ألحق به ضررا فأفسده، ويقال أتلف الجهاز: أعطله عن العمل[1].

وفي الاصطلاح: يعرف الإتلاف على أنه التأثير في مادة الشيء، على نحو يذهب أو يقلل من قيمته الاقتصادية عن طريق الإنقاص من كفاءته للاستعمال المعدل له. فجوهر الإتلاف هو إفقاد المال المتلف منفعته أو صلاحيته للاستعمال في الغرض الذي أعد من أجله[2].

ويقصد بالإتلاف المعلوماتي أو تدمير المعلومات: "مدى صلاحية البرامج والمعلومات المعالجة آليا لأن تكون محلا يرد عليه العدوان في جريمة الإتلاف، عندما لا يترتب على المساس بها أي إتلاف لأي من العناصر المادية التي يتكون نظام المعالجة الآلية للمعطيات"[3].

وقد تم تعريفه أيضا بكونه عملية تعطيل أو تعييب الشيء وجعله غير صالح للاستعمال من أجل التقليل من قيمته الاقتصادية باستعمال وسائل تقنية متطورة، وقد يكون عن قصد أو بغير قصد، كما يمكن أن يكون كليا كمحو البرامج والمعلومات المخزنة داخل جهاز الحاسوب أو يكون جزئيا؛ فيطلق عليه بالتشويه أو التعييب، كإدخال فيروس بالجهاز لإبطال حركته أو أدائه[4].

ثانيا: تعريف نظام المعالجة الآلية للمعطيات

لم يعرف المشرع المغربي نظام المعالجة الآلية للمعطيات؛ حيث ترك ذلك للفقه والاجتهاد القضائي، لأن المجال المعلوماتي مجال سيشهد تطورا مذهلا في قطاع تكنولوجيا الاتصال والمعلوميات، وبالتالي فأي تعريف يتم وضعه قد يصبح متجاوزا في ما بعد؛ مما يجعلنا ننوه بما فعله المشرع المغربي حين تفادى وضع تعريف خاص لهذا النظام. وهكذا عرفت محكمة النقض نظام المعالجة الآلية للمعطيات باعتباره كل مركب يتكون من وحدة أو مجموعة وحدات معالجة تتكون من الذاكرة والبرامج والمعطيات وأجهزة الربط

[1] انظر: مجاني الطلاب، دار المجاني ش.م.ل، بيروت، لبنان، الطبعة الثالثة، سنة 1996، الصفحة 103.

[2] نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، الأردن، السنة 2008، الصفحة 123.

[3] محمد عبد الله أبو بكر سلامة، جرائم الكمبيوتر والأنترنت، منشأة المعارف الإسكندرية، مصر، سنة 2006، الصفحة 152.

[4] المرجع نفسه.

والإدخال والإخراج تربط بينها مجموعة من العلاقات عن طريقها تتحقق نتيجة معينة وهي معالجة المعطيات شريطة أن يكون ذلك المركب خاضعا لنظام حماية[1].

نستشف من التعريف أعلاه أنه اشترط خضوع نظام المعالجة الآلية للمعطيات للحماية التقنية؛ وهو نفس التعريف الذي أورده مجلس النواب الفرنسي الذي عرف هذا النظام على أنه:" مجموعة متكونة من وحدات المعالجة ومن الذاكرة وطرق المعالجة والبيانات ووحدات الإدخال والإخراج والربط بشرط أن تكون محمية بواسطة آلية لضمان السلامة"؛ غير أن المشرع الفرنسي لم يشر إلى شرط خضوع النظام للحماية الفنية عند صدور القانون، في صيغته النهائية، ولم يقصر توفر جريمة الاعتداء على نظام المعالجة الآلية على شرط الحماية التقنية لهذا النظام؛ وهو التوجه عينه الذي سار عليه المشرع القطري من حلال قانون العقوبات رقم 11 لسنة 2004 والذي لم يشترط توافر أجهزة الحماية[2]؛ إلا أن ثمة جانبا من الفقه يرى ضرورة وجود نظام أمني[3].

وينطبق هذا التعريف على النظم المعلوماتية الخاصة بتدبير برامج الدعم الاجتماعي؛ حيث تناط بالوكالة الوطنية للسجلات (حسب البند 1 من المادة 25 من القانون 72.18 المتعلق بمنظومة استهداف المستفيدين من برامج الدعم الاجتماعي وبإحداث الوكالة الوطنية للسجلات[4]) السهر على ضمان حماية المعطيات الرقمية المضمنة في السجل الوطني للسكان والسجل الاجتماعي الموحد، لا سيما من خلال تدبير سلامة النظم المعلوماتية المتعلقة بها طبقا للنصوص التشريعية والتنظيمية الجاري بها العمل المتعلقة بأمن نظم المعلومات. وفي هذا الصدد يلزم القانون 05.20 المتعلق بالأمن السيبراني إدارات الدولة باحترام التوجيهات والقواعد والأنظمة والمراجع والتوصيات الصادرة عن السلطة الوطنية في هذا المجال؛ كما يفرض على الهيئات تنفيذ التدابير التقنية والتنظيمية لإدارة المخاطر السيبرانية وتجنب الحوادث التي قد تؤثر على نظم المعلومات والالتزام بإبلاغ السلطة الوطنية للأمن السيبراني بأي حادث يؤثر على أمن أو سير نظم المعلومات الخاصة بها؛ وذلك حتى يتسنى للسلطة الوطنية إيجاد الحلول الناجعة تجاوزا لهذا الحادث.

ثالثا: تعريف نظم الحماية الاجتماعية

أ- المقصود بالحماية الاجتماعية:

[1] القرار عدد 681 الصادر بتاريخ 3 غشت 2011 في الملف الجنحي عدد 2010/1/6/160806، قرار منشور بالموقع الرسمي لمحكمة النقض.

[2] تنص المادة 370 من قانون العقوبات القطري رقم 11 لسنة 2004 على أنه:" يقصد بنظام المعالجة الآلية للبيانات، كل مجموعة من واحدة أو أكثر من وحدات المعالجة، سواء تمثلت في ذاكرة الحاسب الآلي، أو برامجه، أو وحدات الإدخال أو الإخراج أو الاتصال التي تساهم في تحقيق نتيجة معينة".

[3] عبد المجيد كوزي، الحماية الجنائية للمعطيات في المجال المعلوماتي، المجلة المغربية للقانون الجنائي والعلوم الجنائية، العدد 3، 2016، الصفحة 111.

[4] ظهير شريف رقم 1.20.77 صادر في 18 من ذي الحجة 1441 (8 أغسطس 2020) بتنفيذ القانون رقم 72.18 المتعلق بمنظومة استهداف المستفيدين من برامج الدعم الاجتماعي وبإحداث الوكالة الوطنية للسجلات، الجريدة الرسمية عدد 6908-23 ذو الحجة 1441 (13 أغسطس 2020)، الصفحة 4360.

الحماية الاجتماعية تغطي كافة العمليات أو الآليات المؤسسة للرعاية الجماعية أو العامة أو الخاصة أو حتى المتعلقة بالتضامن الاجتماعي؛ مما يسمح للأفراد أو الأسر مواجهة التكاليف الناجمة عن ظهور عدد معين من المخاطر أو الاحتياجات الاجتماعية المحددة؛ والغرض من ذلك دعم الفئات المستهدفة، في حالة حدوث هذه المخاطر[1]؛ ذلك من خلال التغطية الصحية الإجبارية؛ عبر الصندوق الوطني للضمان الاجتماعي؛ التعويضات العائلية؛ الحماية من مخاطر الشيخوخة والحماية من مخاطر فقدان الشغل[2]؛ وكذا تعويضات جزافية للأسر التي لا تتوفر على أطفال أو يتجاوز سن هؤلاء 21 سنة؛ شريطة ألا تكون مستفيدة من تعويضات الحماية من المخاطر المرتبطة بالطفولة؛ وتهدف هذه التعويضات أساسا لدعم القدرة الشرائية لهذه الأسر والحد من الهشاشة[3].

ب- نظم الحماية الاجتماعية:

ثمة نوعان من نظم الحماية الاجتماعية يستهدفان تدبير أوراش هذه الحماية وهما:

ب-1: السجل الوطني للسكان

تنص المادة الرابعة من القانون 72.18 المشار إليه أعلاه على أنه يحدث سجل وطني رقمي يحمل اسم "السجل الوطني للسكان"، يتم في إطاره معالجة المعطيات ذات الطابع الشخصي المتعلقة بالأشخاص الذاتيين المغاربة والأجانب المقيمين بالتراب المغربي بطريقة إلكترونية، من خلال تجميعها وتسجيلها وحفظها وتحيينها، وتغييرها عند الاقتضاء. وذلك بهدف[4] تسيير الولوج إلى الخدمات التي تقدمها الإدارات العمومية والجماعات الترابية والهيئات العمومية والخاصة؛ كما يهدف إلى منح المعرف الرقمي المحدث بموجب المادة الثامنة من هذا القانون؛ علاوة على إتاحة إمكانية التعرف على الأشخاص الراغبين في التقييد في السجل الاجتماعي الموحد من أجل الاستفادة من برامج الدعم الاجتماعي التي تشرف عليها الإدارات العمومية، بما في ذلك التأكد من هويتهم والتثبت من صدقية المعلومات والمعطيات المتعلقة بهم بالإضافة إلى ذلك يروم السجل الوطني للسكان تقديم خدمات التحقق من صدقية المعطيات المدلى بها من قبل الأشخاص المذكورين أو توفير بعض المعطيات التكميلية، لفائدة الإدارات العمومية والجماعات الترابية والهيئات العمومية والخاصة، وذلك طبقا للشروط والكيفيات المحددة بموجب هذا القانون؛ فضلا عن الإسهام في تبسيط الإجراءات الإدارية المتعلقة بالخدمات المقدمة للمرتفقين.

ب-2: السجل الاجتماعي الموحد

[1] Emeric Jeansen, Droit de la protection social, LexisNexis, Paris, France, 2013, page 1.

[2] المادة 2 من القانون 09.21 المتعلق بالحماية الاجتماعية المشار إليه.

[3] المادة الرابعة من القانون 09.20 المشار إليه.

[4] انظر المادة الخامسة من القانون 72,18 المشار إليه أعلاه.

هو نظام معلوماتي وطني يتيح تسجيل الأسر التي ترغب في الاستفادة من برامج الدعم الاجتماعي واستهدافها بناء على مؤشر اجتماعي واقتصادي يعكس المستوى السوسيو اقتصادي لكل أسرة؛ فهو نظام مجاني ومفتوح أمام المواطنين المغاربة والأجانب المقيمين بالتراب المغربي.

رابعا: تمييز جريمة الإتلاف المعلوماتي عن بعض الجرائم المشابهة

تكاد تشتبه جريمة الإتلاف المعلوماتي مع بعض الجرائم كجريمتي التزوير الإلكتروني وإعاقة سير النظم المعلوماتية؛ بيد أنها تختلف معهما في نقاط متعددة؛ سنتولى تبيانها على النحو الذي سيأتي:

أ- تمييز جريمة الإتلاف المعلوماتي عن جريمة التزوير الإلكتروني

1- أوجه الشبه والتداخل بين الجريمتين:

- **كلاهما يقع على محرر**: يرتبط الحديث عن جريمة التزوير بمحل الجريمة المتمثل في "المحرر الإلكتروني"، كون هذه الجريمة – سواء في صورتها التقليدية أم الإلكترونية- تقوم على التغيير الحاصل في محرر، كما أن محل جريمة الإتلاف المعلوماتي يتسع ليشمل فضلا عن المحرر الإلكتروني، البرامج والبيانات والمعلومات.

- **كلاهما من الجرائم الضرر "النتيجة"**: كما تتطلب جريمة التزوير المعلوماتي لقيامها إحداث تغيير ناتج عن "التلاعب" في محرر "إلكتروني" أو ما في حكمه، فضلا عن الضرر الذي يصيب الغير جراء هذا التزوير –ماديا كان الضرر أم معنويا-، فإن جريمة الإتلاف أيضا لا تنهض ما لم يتم حصول النتيجة الإجرامية التي تتمثل في التغيير الواقع على "المال المعلوماتي" بمختلف صوره من برامج وبيانات ومعلومات ومحررات، وهذا التغيير قد يكون في صورة التدمير أو التخريب الذي يعدم صلاحية محل الجريمة، بما يسبب الضرر للغير.

- **كلاهما محكومان بنصوص قانونية متداخلة**: بعض التشريعات المتخصصة بالجرائم المعلوماتية كالقانون البحريني والسوداني والسعودي والأردني قد أوردت عبارات عامة تتداخل فيها جريمة الإتلاف المعلوماتي، كعبارات "تحريف" أو "تعديل" أو "تغيير"، فضلا عن عبارات "إلغاء" أو "حذف"، وكذا ما جاءت به توصية المجلس الأوربي بشأن جريمة التزوير، وهي تعبيرات تتضمن معنى (التلاعب) الذي يتحقق به السلوك الإجرامي للتزوير المعلوماتي والإتلاف المعلوماتي تارة أخرى.

- **كلاهما من الجرائم العمدية**: ومن ثم تتطلب لقيام كل منهما تحقق القصد الجرمي العام بعنصرية "العلم والإرادة"

2- أوجه الاختلاف بين الجريمتين

- **من حيث النتيجة الإجرامية**: مع أن كلا الجريمتين –الإتلاف المعلوماتي والتزوير المعلوماتي- من جرائم النتيجة التي تتطلب لقيامها حصول نتيجة جرمية كما سبق أن بينا، إلا أن النتيجة الإجرامية في جريمة التزوير تختلف عنها في جريمة الإتلاف، ففي الأولى تتجلى في التغيير الحاصل في "المحرر" أي إن نتيجة التلاعب المعلوماتي في مجال التزوير ستفضي إلى تغيير في حقيقة المحرر الإلكتروني

بخلاف النتيجة الإجرامية في الإتلاف المعلوماتي التي تتجلى في تخريب وتدمير الكيانات المنطقية "المعنوية" من برامج وبيانات ومعلومات ومحررات.

- **من حيث علة التجريم:** تتجلى علة تجريم أفعال التزوير –في صورتيه المعلوماتية أو التقليدية– في حفظ الثقة العامة التي يجب أن تتمتع بها المحررات، مما يؤمن اليقين والاستقرار في المعاملات وسائر مظاهر الحياة القانونية في المجتمع، كونها وسيلة للإثبات يعتمد عليها الأفراد في معاملاتهم والدولة في ممارس اختصاصاتها فضلا عن كونها وسيلة لحسم النزاعات أمام القضاء...، أما علة تجريم أفعال الإتلاف المعلوماتي فتتجلى في حفظ أموال الغير، سواء كانت أموالا خاصة أم عامة من أفعال التلاعب بها، بما يحول بينها وبين أفعال التدمير والتخريب والإتلاف والحيلولة دون إعدام صلاحيتها للعمل.

- **من حيث الحصول على المنفعة:** يرتبط بما تقدم، أن الجاني في التزوير حينما يقوم تغيير الحقيقة "التلاعب" في محرر، فإنه يهدف إلى الحصول على منفعة ومصلحة من وراء هذا السلوك، بخلاف الحال في جريمة الإتلاف المعلوماتي التي لا يهدف الجاني من ورائها الحصول على منفعة معينة – في الغالب – كونه يقوم بتدمير محل الجريمة من برامج وبيانات ومعلومات ومحررات، ومن ثم فلا يتصور عقلا الانتفاع منها لانعدامها، فيما خلا حالات نادرة تتجلى في كون الإتلاف قد حصل من جهة منافسة للمجنى عليه، كما في حالة قيام شركة معينة بإتلاف بيانات وبرامج ومحررات شركة أخرى في إطار من المنافسة غير المشروعة....

- **من حيث الدوافع الإجرامية:** يترتب على الاختلاف السابق، أن تتباين الدوافع الإجرامية بين مرتكبي جريمتي التزوير والإتلاف، ففي الأولى تتمثل دوافع الجناة في الحصول على منافع مادية كانت أم معنوية من خلال تغيير الحقائق، أما في الإتلاف فغالبا ما تكون الدوافع دوافع خبيثة تنطوي الرغبة في الإضرار بالغير من خلال أفعال التدمير والتخريب الواقعة على الأموال المنطقية "المعنوية" للغير[1].

ب– تمييز جريمة الإتلاف المعلوماتي عن جريمة إعاقة النظام المعلوماتي

1– أوجه الشبه والتداخل بين الجريمتين

- **من حيث الوسائل التي ترتكب بها كل من الجريمتين:** الوسائل الفنية المستخدمة في السلوك الإجرامي للإتلاف المعلوماتي –كالفايروسات الخبيثة وبرنامج الدودة والقنابل المنطقية وحصان طروادة–؛ هي ذاتها التي قد تستخدم في جريمة الإعاقة؛

- **من حيث المحل الذي تقع عليه الجريمتين:** تشترك كلا الجريمتين في المحل الذي تقع عليه كل منهما، وهي مفردات النظام المعلوماتي والكيانات المنطقية من برامج وبيانات ومعلومات، ولهذا فإن كليهما من الجرائم الواقعة على النظام المعلوماتي عند بحث موقعها من جرائم المعلوماتية؛

- **كلاهما من جرائم النتيجة الضرر:** كلا الجريمتين تتطلب للعقاب عليه أن تتحقق نتيجة جرمية؛ ففي الإتلاف تكون النتيجة في إعدام الفائدة من الكيان المنطقي محل الجريمة، وفي الإعاقة تكون النتيجة تعطيل وقتي أو إرباك أو إبطاء عمل النظام؛

[1] عمار عباس الحسيني، جريمة الإتلاف المعلوماتي–دراسة قانونية مقارنة، منشورات زين الحقوقية، بيروت–لبنان، الطبعة 2018، الصفحة 62 وما بعدها.

- **أفعال الإعاقة قد تؤدي إلى الإتلاف المعلوماتي والعكس صحيح:** نجد في كثير من الأحيان أن تفضي أفعال الإعاقة وإرباك النظام المعلوماتي وعرقلته وإبطاء عمله إلى التعطيل الدائم "الإتلاف والتخريب المعلوماتيين"؛ والعكس صحيح؛ ففي حال إتلاف جزء من معلومات النظام؛ فإن ذلك سيؤدي إلى إعاقة النظام المعلوماتي عن أداء عمله.

2- أوجه الاختلاف بين الجريمتين:

- **من حيث النتيجة الإجرامية:** تتمثل النتيجة الإجرامية في الإتلاف المعلوماتي في تخريب أو تدمير أو التعطيل الكلي أو الجزئي لنظم المعلومات "الكيانات المنطقية": بيانات- برامج-معلومات-محررات إلكترونية؛ بخلاف النتيجة في الإعاقة النظام المعلوماتي؛ حيث تقتصر النتيجة على وجوب حصول إرباك أو عرقلة لهذا النظام بما يحول بينه وبين أدائه لوظائفه على وجهها الصحيح.

- **من حيث القصد الجرمي:** يتجه القصد الجرمي للجاني في الإتلاف المعلوماتي إلى إعدام صلاحية الكيانات المنطقية بما يفقدها قابليتها للعمل المرجو منها، أما القصد الجرمي في جريمة الإعاقة فيتمثل في عرقلة أو إرباك أو تعييب وقتي للنظام المعلوماتي أو تباطؤ في عمله؛ وإن كانت كلا الجريمتين من الجرائم العمدية التي تتطلب القصد الجرمي بعنصريه "العلم والإرادة[1]"

الفقرة الثانية: خصائص جريمة إتلاف معطيات نظم الحماية الاجتماعية

تتميز جريمة إتلاف معطيات نظم الحماية الاجتماعية باعتبارها جريمة معلوماتية بعدة خصائص، وهي:

أولا: جريمة عابرة للحدود

تتمتع الحواسيب والشبكات المرتبطة بها بمقدرة في نقل كميات كبيرة من المعلومات وتبادلها بين أنظمة يفصل بينها آلاف الأميال، قد أدت إلى نتيجة مؤداها أن أماكن متعددة في دول مختلفة قد تتأثر بالجريمة المعلوماتية الواحدة في آن واحد؛ فالسهولة في حركة المعلومات عبر أنظمة التقنية الحديثة، جعل بالإمكان اقتراف جريمة الإتلاف المعلوماتي في دولة وقد تتحقق النتيجة في المغرب؛ وهو ما يثير عدة إشكاليات تتعلق بالقانون الواجب التطبيق؛ إضافة إلى إشكاليات مرتبطة بالإجراءات القانونية للمتابعة؛ علاوة على مشكل الاختصاص القضائي لهذه الجريمة[2].

ثانيا: صعوبة اكتشاف جريمة الإتلاف المعلوماتي

تتميز هذه الجريمة باعتبارها جريمة معلوماتية بصعوبة اكتشافها، ويرجع السبب في ذلك إلى عدم ترك هذه الجريمة لأي أثر خارجي بصورة مرئية، بحكم أن الفاعل يتولى تدمير الدليل بعد اقترافه الجريمة مباشرة.

[1] عمار عباس الحسيني، المرجع السابق.

[2] عبد الكريم عباد، الجريمة المعلوماتية، المجلة الوطنية للعلوم القانونية والقضائية، العدد الأول، 2016، مطبعة الأمنية، الرباط، الصفحة 43 وما بعدها.

ثالثا: صعوبة إثبات جريمة الإتلاف المعلوماتي

تتم هذه الجريمة خارج إطار الواقع المادي الملموس، لتقوم أركانها في بيئة الحاسوب والشبكات المرتبطة به، مما يجعل الأمور تزداد تعقيدا لإثباتها من قبل سلطات الأمن وأجهزة التحقيق، نظرا لأن البيانات والمعطيات الإلكترونية عبارة عن نبضات إلكترونية غير مرئية تنساب عبر النظام المعلوماتي، مما يجعل أمر طمس الدليل ومحوه كليا من قبل الفاعل أمرا في غاية السهولة، ويعزى ذلك إلى الخصائص التي يتسم بها الجاني؛ ذلك أن مرتكبي هذا النوع من الإجرام عادة ما يكون من ذوي الاختصاص والخبرة في مجال تقنية المعلوماتية، وعلى قدرة وكفاءة عاليتين في التعامل مع جهاز الحاسوب وشبكة والإنترنت؛ إضافة إلى توفره على مستوى علمي ومعرفي يؤهله من تحديد الهدف المقصود من اقترافه الجريمة؛ فضلا عن ذلك فإن جريمة الإتلاف المعلوماتي تتم عادة بتعاون أكثر من شخص، بشكل إيجابي أو سلبي، بحيث يكون هذا التعاون أو الاشتراك في الجريمة إيجابيا عندما تكون ثمة مساعدة فنية أو مادية من طرف شخص آخر؛ وجهة معينة...وقد يكتسي هذا التعاون شكلا سلبيا، وهو الذي يمكن ترجمته بالصمت من جانب من يعلم بوقوع الجريمة في محاولة منه لتسهيل إتمامها[1].

المطلب الثاني: رأي الفقه والتشريع في شأن جريمة إتلاف معطيات نظم الحماية الاجتماعية

تتجاذب جريمة الإتلاف المعلوماتي عدة آراء فقهية (الفقرة الأولى)؛ علاوة على ذلك فإن التشريعات الهادفة إلى مكافحة هذا النوع من الجرائم تختلف في تناول هذه الجريمة إما بمقتضى نصوص خاصة أو الإبقاء على القواعد العامة (الفقرة الثانية).

الفقرة الأولى: رأي الفقه بخصوص جريمة إتلاف معطيات نظم الحماية الاجتماعية

ثمة توجهان فقهيان يتجاذبان بخصوص جريمة الإتلاف التي تقع على النظم المعلوماتية:

الرأي الأول:

ذهب رأي إلى أنه لا يحول دون تطبيق النصوص التقليدية الخاصة بإتلاف المنقول المادي، على المعلومات والبرامج بالرغم من أنها أشياء معنوية[2]؛ إذ أن المشرع المصري مثلا لم يحدد طريقة بعينها لوقوع الجريمة ولم يحدد نتيجة واحدة لقيامها؛ فإنه من المتصور أن يتجه الجاني بنشاطه الإجرامي إلى البرنامج والدعامة المحمل عليها معا، أو إلى البرنامج فقط دون الدعامة، وقد تقع جريمة الإتلاف عن طريق الاتصال المباشر بالجهاز، كما تقع من خلال الاتصال عن بعد، كما أن المعلومات ذات قيمة اقتصادية، ويمكن نقلها –

[1] المرجع نفسه.

[2] محمود محمد جابر، الجرائم الناشئة عن استخدام الهواتف النقالة (جرائم نظم الاتصالات والمعلومات)، المكتب الجامعي الحديث، الإسكندرية، مصر، طبعة 2018، الصفحة 186.

رغم عدم رؤيتها- ويمكن تدميرها وإتلافها عن طريق التدخل في هذه البرامج وهي محملة على الجهاز، وإتلافها كليا أو جزئيا أو تشويهها؛ ومن ثم فإن هذه المعلومات تخضع للنصوص التقليدية المتعلقة بالإتلاف[1].

الرأي الثاني:

ذهب رأي آخر إلى أن المعلومات المبرمجة آليا هي بمثابة نبضات كهربائية تفتقر إلى الطبيعة المادية، كما أن مجرد التدخل في وظائف العناصر المادية التي يتكون منها النظام المعلوماتي، والتي يتم تسجيل هذه المعلومات عليها يعتبر إتلافا لها. ويؤيد هذا التوجه المشرع الفرنسي من خلال المادة 4/462 من القانون رقم 19 لسنة 1988 التي تجرم فعل الإتلاف الذي يكون محله عناصر غير مادية؛ حيث جاء فيها على أنه:" يعاقب بالحبس مدة تتراوح ما بين ثلاثة شهور إلى ثلاث سنوات وبغرامة تتراوح ما بين 2000 فرنك إلى 500000 فرنك أو بإحدى هاتين العقوبتين كل من أدخل عمدا وبدون مراعاة الحقوق الغير بطريق مباشر أو غير مباشر- بيانات في نظام المعالجة الآلية أو محا أو عدل في البيانات التي يحويها النظام أو طرق معالجتها أو نقلها[2]."

نتفق بدورنا مع الاتجاه الثاني؛ ومبررنا في ذلك أن المعلومات سواء كانت مخزنة في ذاكرة الحاسوب أو منفصلة عنه، شرط أن تكون على دعامة إلكترونية، يتعين ألا تخضع في حمايتها للمقتضيات العامة؛ لأن هذه الأخيرة إنما وجدت لحماية الأشياء المادية كالمكونات الملموسة لجهاز الحاسوب وما يرتبط به من أسلاك التوصيل؛ ومن ثم نرى ضرورة توسيع النصوص الخاصة لتشمل كافة الاعتداءات على الأشياء المعنوية (كالمعلومات...)؛ خاصة جريمة الائتلاف المعلوماتي.

الفقرة الثانية: رأي التشريع في شأن جريمة إتلاف معطيات نظم الحماية الاجتماعية

مما لا شك فيه أن الشق المادي للنظام المعلوماتي والمتجسد في أجهزة النظم المعلوماتية من حواسيب ومعدات مرتبطة بها؛ وشاشات العرض؛ والدعامات والأشرطة المغناطيسية والأقراص بكل أشكالها التي تخزن عليها المعلومات والكابلات وشبكات الربط وغير ذلك؛ هي مال مادي منقول له كيان خارجي ملموس؛ فنحن بصدد جريمة إتلاف بصورتها التقليدية؛ وبالتالي تخضع للنصوص

[1] انظر:
- علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب، دار الجامعة الجديدة، الإسكندرية، الطبعة الأولى، سنة 1997، الصفحتان 78 و79.
- غنام محمد غنام، عدم ملاءمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر، بحث مقدم إلى مؤتمر القانون والكمبيوتر والأنترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة- مايو 2000، المجلد الثاني، الطبعة الثالثة، سنة 2004، الصفحة 642.

[2] Art 462-4: « Quiconque aura, intentionnellement et au mépris des droits d'autrui, directement ou indirectement , introduit des données dans un système de traitement automatisé ou supprimé ou modifié les données qu'il contient ou leurs modes de traitement ou de transmission, sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 2000 F à 500 000 F ou de l'une de ces deux peines ».

التقليدية؛ وفي هذا السياق تناول المشرع الأردني بالتجريم فعل الإتلاف الذي يؤدي إلى إلحاق الضرر بالمال المنقول المملوك للغير؛ وذلك من خلال نص المادة 445 من قانون العقوبات التي ينص بندها الأول على أنه:" كل من ألحق باختياره ضررا بمال غيره المنقول، يعاقب بناء على شكوى المتضرر بالحبس مدة لا تتجاوز سنة أو بغرامة لا تتجاوز خمسين دينارا أو بكلتا العقوبتين."

وبالرجوع إلى مجموعة القانون الجنائي المغربي نجد أنها تجرم إتلاف –عمدا– أوراق أو سجلات أو صكوك أو سندات محفوظة في مضابط أو في كتابات الضبط أو مستودعات عامة أو مودعة لدى أمين عمومي بصفته هذه[1]؛ علاوة على ذلك تنص المادة 592 من مجموعة القانون المغربي على أنه:" في غير الحالات المشار إليها في الفصل 276 فإن من يحرق ويتلف عمدا بأي وسيلة كانت، سجلات أو أصول الوثائق المتعلقة بالسلطة العامة أو صورها الرسمية أو سندات أو حججا، أو سفتجة أو أوراقا تجارية أو بنكية متضمنة أو منشئة لالتزامات أو تصرفات أو إبراء، فإنه يعاقب بالسجن من خمس إلى عشر سنوات، إن كانت الأوراق المتلفة متعلقة بالسلطة العامة، أو أوراقا تجارية أو بنكية، وبالحبس من سنتين إلى خمس سنوات وغرامة من مائتين إلى خمسمائة درهم، إن كانت أوراقا أخرى."

باستقرائنا للمادتين أعلاه؛ نستشف أن المشرع المغربي لم يتطرق إلا إلى الوثائق والسجلات المتعلقة بالسلطة العامة ولم يتعرض إلى إتلاف الأجهزة المادية للنظم المعلوماتية؛ إلا أنه تدارك ذلك من خلال ما ورد في البند الأول من المادة 81 من القانون 24.96 المتعلق بالبريد والمواصلات؛ حيث يعاقب بغرامة من 1500 إلى 5000 درهم، كل من قام بعدم احتياط أو عن غير عمد:

- بارتكاب فعل مادي من شأنه عرقلة خدمات المواصلات؛
- بتغييب أو إتلاف الخطوط الهوائية أو المدفونة أو أجهزة المواصلات أو كل منشأة مواصلاتية بأية طريقة كانت."

وكما هو معلوم أن النظم المعلوماتية الخاصة بالحماية الاجتماعية لا يمكن تفعيلها إلا إذا كانت مرتبطة بشبكة المواصلات (الأنترنت) وأن أي مساس بالأجهزة المادية المرتبطة بهذه النظم تطالها المادة 81 المشار إليها.

بالإضافة إلى ما سلف؛ نستشف أن المشرع المغربي أفرد نصا خاصا يجرم إتلاف المكونات المادية للنظم المعلوماتية، كما هو الشأن في قانون العقوبات القطري رقم 11 لسنة 2004؛ حيث تنص المادة 374 منه على أنه:" يعاقب بالحبس مدة لا تتجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على عشرة آلاف ريال، كل من أتلف أو خرب عمدا وحدات الإدخال أو الإخراج أو شاشة حاسب آلي مملوك للغير أو الآلات أو الأدوات المكونة له."

[1] الفقرة الأولى من المادة 276 من مجموعة القانون الجنائي.

وتتضاعف العقوبة[1] إذا ارتكبت جريمة الإتلاف على جهاز حاسب آلي مملوك[2] للوزارات والأجهزة الحكومية الأخرى، وكذا الهيئات والمؤسسات العامة.

وبخصوص إتلاف المعطيات المعالجة عبر النظم المعلوماتية فقد أورد لها المشرع المغربي، نصا خاصا يتمثل في الفصل 607-6 من القانون 07.03 المشار إليه، إسوة بالتشريع الإماراتي[3] الذي يعاقب كل من تسبب عمدا في الإضرار أو تدمير أو إيقاف أو تعطيل موقع إلكتروني أو نظام معلوماتي إلكتروني أو شبكة معلومات أو وسيلة تقنية المعلومات، عائدة لمؤسسات الدولة أو احد المرافق الحيوية. فإذا وقعت الجريمة نتيجة لهجمة إلكترونية اعتبر ذلك ظرفا مشددا.

ما يمكن ملاحظته بخصوص قانون مكافحة الشائعات والجرائم الإلكترونية الإماراتي أنه ميز ما بين الاعتداء الواقع على الأنظمة المعلوماتية في حالتها العادية؛ أي النظم الإلكترونية الخاصة بجهات غير حكومية، أو جهة مصرفية أو إعلامية أو صحية أو علمية[4]، وما بين الإضرار بالأنظمة المعلوماتية لإحدى مؤسسات الدولة والمرافق الحيوية؛ كما ميز ما بين الاعتداء على البيانات والمعلومات الشخصية (إتلافها) بقاعدة قانونية خاصة[5]؛ وما بين الاعتداء على البيانات ولمعلومات الحكومية[6].

المبحث الثاني: الأحكام الخاصة بجريمة إتلاف معطيات نظم الحماية الاجتماعية

لقيام المسؤولية الجنائية عن ارتكاب جريمة إتلاف نظم الحماية الاجتماعية لا مناص من توافر الأركان التكوينية المتمثلة في الركنين المادي والمعنوي؛ فضلا عن توافر الركن الخاص المتجسد في محل الجريمة (المطلب الأول)؛ وبالتالي توقيع العقاب على الجناة (المطلب الثاني).

المطلب الأول: الأركان التكوينية لجريمة إتلاف معطيات نظم الحماية الاجتماعية

لقيام جريمة إتلاف المعطيات المعالجة من خلال النظم المعلوماتية المخصصة لتدبير أوراش الحماية الاجتماعية؛ لا مناص من توافر الأركان التكوينية المتمثلة في الركن المادي والركن المعنوي، فضلا عن الركن الخاص المتمثل في البرامج والمعلومات والمحررات الإلكترونية؛ وهو ما سنتطرق إليه في الفقرتين أدناه.

الفقرة الأولى: الركن المادي

[1] المادة 385 من قانون العقوبات القطري رقم 11 لسنة 2004.

[2] البندان 1 و2 من المادة الرابعة من قانون العقوبات القطري المشار إليه.

[3] المادة الخامسة من مرسوم بقانون اتحادي رقم 34 لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية.

[4] المادة الرابعة من مرسوم بقانون اتحادي رقم 34 لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية.

[5] المادة السادسة من قانون مكافحة الشائعات والجرائم الإلكترونية الإماراتي.

[6] المادة السابعة من مرسوم بقانون اتحادي رقم 34 لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية.

يتجلى الركن المادي لهذه الجريمة، باعتبارها من جرائم الضرر (النتيجة)، في العناصر الثلاثة المتجسدة في السلوك الإجرامي (أولا)؛ والنتيجة الجرمية (ثانيا)؛ والعلاقة السببية (ثالثا).

أولا: النشاط المجرم ووسائله

أ- السلوك الإجرامي في جريمة الإتلاف المعلوماتي

يتحقق السلوك الإجرامي بجميع الأفعال التي تؤدي إلى إتلاف النظم المعلوماتية؛ وفي هذا السياق جاءت التشريعات بتعبيرات متعددة دالة على قيام هذا النشاط؛ ومنها عبارة "الإتلاف" و"التدمير" و"التخريب" و"محو البرامج والبيانات" و"التشويه" و"مسح البرامج والبيانات" و"إيقاف" أو "حذف" أو أي سلوك آخر يجعل المحررات غير صالحة للاستعمال كليا أو جزئيا.

فالقانون المغربي جاء بتعبيرات "إدخال معطيات في نظام المعالجة الآلية للمعطيات أو أتلفها أو حذفها منه أو غير المعطيات المدرجة فيه، أو غير طريقة معالجتها أو طريق إرسالها عن طريق الاحتيال[1]؛ كما أن القانون الفرنسي أورد تعبيرات دالة على الإتلاف المعلوماتي؛ وذلك من خلال "الإدخال والمحو والتعديل". في حين نلاحظ باستقرائنا لقانون مكافحة الشائعات والجرائم الإلكترونية أن المشرع الإماراتي استعمل لفظتين؛ "تدمير" و"إتلاف"؛ فالأولى استعملها حين يتعلق الأمر بالإضرار بالأنظمة المعلوماتية، والثانية استخدمها متى تم الاعتداء على المعلومات والبيانات.

تأسيسا عليه؛ نرى على أنه يكفي لتحقق السلوك الإجرامي تحقق أحد الصور المشار إليها أعلاه، أي أن التدمير أو الإتلاف، أو الحذف وغيرها من الصور المذكورة تكفي لقيام جريمة الإتلاف المعلوماتي، وهو ما يستشف من لفظ "أو" الدالة على التخيير التي أوردتها جل التشريعات، كما نلاحظ أن المشرع المغربي أورد لفظ "أتلف" كسلوك قائم بذاته بالرغم من كون الألفاظ الأخرى الواردة في الفصل 607-6 تحقق جريمة الإتلاف المعلوماتي. وما نستشفه في هذا الصدد أن التعبيرات المشار إليها أعلاه يقصد منها النتيجة الجريمة في الإتلاف المعلوماتي أكثر مما كان يقصد بها النشاط الجرمي. كذلك؛ فإن السلوك الإجرامي قد يكون سلبيا يتجسد في إحجام شخص عن إتيان فعل إيجابي معين كان المشرع قد طلبه منه في ظروف معينة وأن يكون في استطاعة الفاعل "الممتنع" القيام بهذا الواجب، ومثال ذلك في إطار جريمة الإتلاف المعلوماتي[2]؛ ما ورد في الفقرة الأولى من المادة السابعة من القانون 05.20 المتعلق بالأمن السيبراني الناصة على أنه:" يجب على كل هيئة أن توفر الوسائل المناسبة لمراقبة ورصد الأحداث التي قد تمس بأمن نظم معلوماتها ويكون لها وقع بالغ على استمرارية الخدمات التي تقدمها." وهو الأمر الذي أدركته اتفاقية بودابست من خلال قولها:" يجب على كل الدول الأعضاء تبني إجراءات تشريعية أو اية إجراءات أخرى ترى أنها ضرورية لتجريم عمدا ودون وجه حق،

[1] الفصل 607-6 من القانون 07.03 المتعلق بنظم المعالجة الآلية للمعطيات.

[2] انظر: عمار عباس الحسيني، المرجع السابق، الصفحة 155.

التسبب في إحداث ضرر مالي للغير عن طريق: الإدخال، الإتلاف، المحو، الطمس لبيانات الحاسب"، ومعنى ذلك الامتناع عن هذا الواجب القانوني بما يحقق الإتلاف المعلوماتي سيشكل جريمة إتلاف بالامتناع.

وتجدر الإشارة في هذا المضمار أن الدخول غير المصرح به إلى النظم المعلوماتية يعد مقدمة لجريمة الإتلاف؛ بحيث تعتبر بعض التشريعات[1] أن تحقق جريمة الإتلاف يقتضي أن يكون الدخول إلى النظام المعلوماتي قد تم بشكل غير مشروع؛ كما جعل مسلك ثان[2] الإتلاف المعلوماتي ظرفا مشددا للدخول غير المشروع.

ب- وسائل الإتلاف المعلوماتي

غني عن البيان أن جل التشريعات لم تحدد طريقة وقوع جريمة الإتلاف؛ فقد تتم بواسطة برامج خبيثة كالفيروسات والقنابل المنطقية أو برامج الدودة أو أي وسيلة أخرى تحقق النتيجة ذاتها كتعديل شفرة الدخول أو تغييرها أو التلاعب بالبيانات أو محوها بشكل يدوي من خلال إيعازات الحاسب.

وهكذا؛ قد يتحقق الإتلاف المعلوماتي عن طريق إغراق ذاكرة الحاسب الآلي "الإغراق المعلوماتي"؛ وذلك من خلال بعث رسائل إلكترونية بغزارة من شأنه ملء ذاكرة الجهاز أو قد يصاحب تلك الرسائل فايروسات خبيثة، للعمل على تقليل أو إعدام مساحات ذاكرة النظام المعلوماتي بشكل يؤدي إلى فقدان المستخدم للمساحات الخاصة بالتخزين، ومن ثم يتم إعاقة استقبال بيانات ومعلومات أو تعطل الخدمة نتيجة لملء منافذ الاتصال، بما يؤدي إلى تدمير النظام المعلوماتي وتشتيت البيانات المخزنة[3].

وقد يتحقق الإتلاف المعلوماتي من خلال الفيروسات[4] التي تتكاثر بمعدل سريع لدرجة تصيب النظام المعلوماتي بالشكل التام[5]، وتتمتع الفيروسات بقدرة عالية جدا على مهاجمة النظم المعلوماتية، وتسفر عن تدمير البرامج والبيانات والمعلومات، كما تتمتع

---

[1] التشريع السعودي، المادة 5 من نظام مكافحة جرائم المعلوماتية السعودي لسنة 1428هـ.

[2] القانون الإماراتي: "1- كل فعل عمدي يتوصل فيه بغير وجه حق إلى الموقع أو نظام معلوماتي سواء بدخول الموقع أو النظام أو بتجاوز مدخل مصرح به، يعاقب عليه بالحبس وبالغرامة أو بإحدى هاتين العقوبتين. 2- فإذا ترتب على الفعل إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو إعادة نشر بيانات أو معلومات فيعاقب بالحبس مدة لا تقل عن ستة أشهر وبالغرامة أو بإحدى هاتين العقوبتين.

[3] عمار عباس الحسيني، المرجع السابق، الصفحتان 162 و163.

[4] الفيروسات عبارة عن برامج مشفرة مصممة بقدرة على التكاثر والانتشار من نظام إلى آخر، إما بواسطة قرص ممغنط أو عبر شبكة الاتصالات؛ بحيث يمكنه أن ينتقل عبر الحدود من أي مكان إلى آخر في العالم، وهو ما يسمى عادة باسم أول مكان اكتشف فيه، والبرامج الفيروسية لها قدرة على الاختفاء داخل برنامج سليم؛ حيث يصعب اكتشافها، كما أنها قد تكون مصممة لتدمير برامج أخرى أو تغيير معلومات ثم تقوم بتدمير نفسها ذاتيا دون أن تترك أثرا يدل عليها، وعلى الرغم من تدميرها للبرنامج والمعلومات إلا أنها لا تسبب عادة تدميرا لأي من المكونات المادية للنظام.

انظر: نهلا عبد القادر المومني، المرجع السابق، الصفحتان 125 و126.

[5] محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، الطبعة الأولى، سنة 1984، الصفحة 189.

بإنتاجها نسخا من نفسها، وقدرتها أثناء عملية الإنتاج الذاتي على التغيير والتطور والتكيف مع البرامج المتنوعة؛ مما يترتب عنه تدمير النظام المعلوماتي بأكمله[1].

ولعل ما يمكن أن يتسبب في خسائر مادية ناجمة عن إتلاف النظم المعلوماتية ما يعرف باستخدام برامج القنابل المنطقية، وهي عبارة عن برنامج أو جزء من برنامج ينفذ في لحظة محددة أو كل فترة زمنية منتظمة، ويتم وضعه في شبكة معلوماتية بهدف تحديد ظروف أو حالة مضمون النظام بغية تسهيل تنفيذ عمل أو غرض غير مشروع؛ حيث يمكن إدراج تعليمات في برنامج نظام التشغيل، وينصب البحث بعد ذلك على عمل معين يمكن أن يكون محلا للاعتداء، كأن تسعى قنبلة منطقية إلى البحث عن حرف معين (الألف مثلا) في أي سجل يتضمن أمرا بالدفع، وعندما تكتشفه؛ تحرك متتالية منطقية تعمل على إزالة هذا الحرف من السجل[2].

وعلى العكس القنبلة المنطقية؛ فثمة برنامج القنبلة الزمنية أو الموقوتة المصممة؛ بحيث تبقى ساكنة وغير فعالة؛ وغير مكتشفة؛ لمدد قد تصل إلى أشهر؛ بل وحتى أعوام؛ وهذه المدة يحددها عادة مؤشر زمني يحتويه البرنامج –كتاريخ معين– بحيث ينشط برنامج القنبلة عند حلوله ويؤدي مهامه التدميرية الهدامة؛ فهي مرتبطة دائما بعنصر الزمن؛ حيث يتم إدخالها في برنامج أو تنفذ في جزء من المللي ثانية أو في بضع أو دقائق وفقا للتحديد أو البرمجة اللازمة للانفجار[3].

كذلك؛ تعد الديدان من البرامج التي تتلف الكيان المعنوي للنظم المعلوماتية؛ فهي عبارة عن برنامج تستغل أي فجوات في نظم التشغيل كي تنتقل من جهاز إلى آخر، أو من شبكة إلى أخرى عبر الوصلات التي تربط بينها، وتتكاثر هذه البرامج إلى شغل أكبر حيز ممكن من سعة الشبكة؛ ومن ثم العمل على تقليل او خفض كفاءتها، وأحيانا تتعدى هذا الهدف لتبدأ بعد التكاثر والانتشار في التخريب الفعلي للملفات والبرامج ونظم التشغيل. وهي لا تحتاج لانتقالها إلى ملف أو غيره؛ بل تنقل نفسها بنفسها عن طريق البريد الإلكتروني مثلا، ولا تحتاج لتنفيذ حدث لتنشيطها[4].

مما سبق؛ نستنتج أن اساليب إتلاف النظم المعلوماتية متعددة ومتجددة؛ لذلك لم يحدد المشرع المغربي أيا من الآليات المشار إليها أعلاه؛ وهو ما يحسب للمشرع نظرا للتطور الذي يشهده وسيشهده المجال الرقمي؛ خاصة سبب الإتلاف المعلوماتي.

ثانيا: الضرر الناجم عن جريمة إتلاف معطيات نظم الحماية الاجتماعية

[1] محمد عبد الله أبو بكر سلامة، المرجع السابق، الصفحة 160.

[2] محمد عبد الله أبو بكر سلامة، المرجع السابق، الصفحة 153.

[3] محمد عبد الله أبو بكر سلامة، المرجع السابق، الصفحتان 154 و155.

[4] محمود محمد محمود جابر، المرجع السابق، الصفحتان 189 و190.

تعد جريمة الإتلاف المعلوماتي من جرائم الضرر؛ أي تلك التي تتطلب حصول نتيجة جرمية ناجمة عن قيام الجاني بمحو أو تدمير أو إتلاف أو تشويه أو إعطاب البرامج أو المعلومات أو البيانات؛ بحيث يحرم المالك من منفعة هذه الأخيرة بشكل كلي أو جزئي؛ ومن ثم فإن حدوث ضرر ولو جزئي تقام المسؤولية الجنائية المترتبة عن هذا الإتلاف؛ مادام تم التأثير في مادة الكيان المنطقي للنظم المعلوماتية؛ وهو من المسائل الموضوعية التي يختص بها قاضي الموضوع.

ثالثا: العلاقة السببية بين السلوك والنتيجة الجرمية

إن جريمة الإتلاف لا تقوم مالم تتحقق النتيجة الجرمية الناجمة عن السلوك الإجرامي المحدث من قبل الجاني، بمعنى وجوب تحقق العلاقة السببية بين السلوك الإجرامي والنتيجة الجرمي كي يسأل الفاعل عن سلوكه الإجرامي؛ وإلا فلا مجال لمساءلته. أما إذا تحقق السلوك دون النتيجة كان الفعل عندئذ شروعا في جريمة الإتلاف.

الفقرة الثانية: الركن المعنوي والركن الخاص

لقيام جريمة الإتلاف المعلوماتي لا يكفي تحقق الركن المادي بل لا مناص من تحقق الركن المعنوي لهذه الجريمة التي تعد من الجرائم العمدية (أولا) فصلا عن الركن الخاص المتمثل في محل الجريمة موضوع الدراسة.

أولا: الركن المعنوي

لقيام الركن المعنوي في جريمة الإتلاف المعلوماتي لمعطيات نظم الحماية الاجتماعية يقتضي تحقق القصدين العام (أ) والخاص (ب).

أ- القصد الجرمي العام في جريمة الإتلاف المعلوماتي

يتجسد القصد الجرمي العام في هذه الجريمة في عنصري العلم والإرادة؛ فبشأن العنصر الأول فيقصد به علم الجاني بقيامه بنشاط غير مشروع؛ وأنه يعتدي على مصلحة يحميها القانون؛ فينبغي أن يعلم الجاني وقت مقارفته للفعل الجرمي؛ أنه يعتدي على أموال معلوماتية مملوكة للغير تتمثل في المعطيات والمعلومات والبيانات والبرامج والمحررات المعلوماتية التي تتولى الوكالة المكلفة بتدبير ورش الحماية الاجتماعية معالجتها. كما يقتضي تحقق عنصر الإرادة اتجاه إرادة الفاعل إلى السلوك الإجرامي، وإحداث الضرر المتمثل في إتلاف الكيانات المنطقية للنظم المعلوماتية الخاصة بمعالجة بيانات الحماية الاجتماعية؛ وذلك من خلال قيامه بالتعديل غير المشروع، والتدمير والتخريب ومحو البرامج والبيانات أو التشويه أو المحو لهذه النظم الإلكترونية؛ بما يترتب على ذلك عطب المعلومات وإعدام قيمتها وتعطيل منفعتها أو تدميرها سواء تم ذلك بشكل جزئي أم كلي.

تجدر الإشارة في هذا الصدد إلى أنه لا يشترط في القصد الجرمي في جريمة الإتلاف المعلوماتي أن تتجه الإرادة إلى النتيجة المتحققة؛ بل يكفي أن يكون القصد الجرمي هنا غير مباشر أو ما يعرف بالقصد الاحتمالي الذي يعرف بأنه الحالة الذهنية للشخص الذي يدرك النتائج الإجرامية التي تترتب على سلوكه ويقبل بها (قبول النتيجة الجرمية)[1]

ب- القصد الخاص في جريمة الإتلاف المعلوماتي

باستقرائنا للعديد من التشريعات المقارنة نجد أن الغالب منها لم تتطلب قصدا خاصا يقوم به الركن المعنوي لجريمة الإتلاف المعلوماتي؛ لأن الأصل في هذه الجريمة تقوم على القصد العام بعنصريه "العلم والإرادة"؛ ويتجلى ذلك من خلال الصياغات القانونية التي جعلت من وقوع أفعال الإتلاف والتدمير والحذف...تارة ظرفا مشددا في حالة وقوعها؛ وذلك من خلال تجريم أفعال الدخول غير المصرح به مبدئيا؛ ومن ثم تشديد العقاب في حال ترتب على هذا الدخول حذف أو تدمير أو إتلاف أو تغيير أو إعادة نشر بيانات أو معلومات...وتارة جعلتها قصدا خاصا كصياغة القانون السعودي الذي جاء بصيغة الدخول غير المشروع لإلغاء بيانات خاصة أو حذفها أو تدميرها أو تسريبها، فحرف اللام في عبارة "لإلغاء" يفيد أن غاية الدخول هنا تكون في الإتلاف المعلوماتي[2].

ثانيا: الركن الخاص في جريمة الإتلاف المعلوماتي – محل الجريمة

لا بد من الإشارة إلى أن محل جريمة إتلاف معطيات نظم الحماية الاجتماعية يقتضي أن يكون ذا طبيعة معنوية "منطقية" وإلا باتت جريمة الإتلاف جريمة عادية تخضع إلى القواعد العامة وليس بجريمة معلوماتية؛ ومن ثم فإن صور محل الجريمة موضوع الدراسة تكون إما عبارة عن برامج إلكترونية "معلوماتية" أو ما تسمى ببرامج الحاسب الآلي أو معلومات او بيانات، فضلا عن المحرر الإلكتروني الذي يكتسي أهمية كبيرة في هذا المجال من خلال تطبيقاته؛ ومن ثم فإن أفعال الإتلاف المعلوماتي قد تقع عليه أيضا.

المطلب الثاني: العقوبات المقررة لجريمة إتلاف معطيات نظم الحماية الاجتماعية

سنعرض لصور العقاب عن جريمة الإتلاف المعلوماتي لمعطيات نظم الحماية الاجتماعية في ضوء بعض التشريعات الحديثة (الفقرة الأولى)؛ ثم نعرض لصور هذا العقاب في ظل التشريع المغربي.

الفقرة الأولى: عقوبة جريمة الإتلاف المعلوماتي في التشريع الفرنسي والإماراتي

سنتناول في خضم هذه الفقرة تجليات العقاب عن جريمة الإتلاف المعلوماتي في التشريع الفرنسي (أولا)، والإماراتي (ثانيا) على النحو الذي سيأتي:

[1] عمار عباس الحسيني، المرجع السابق، ص185 وما بعدها.

[2] المرجع نفسه.

أولا: في التشريع الفرنسي

في القانون الفرنسي الخاص بجرائم المعلوماتية رقم 19-88 والصادر في 22 دجنبر 1987 والنافذ في 5 يناير 1988 إلى العقاب بالحبس لمدة تتراوح بين ثلاثة شهور وثلاث سنوات وبغرامة تتراوح بين 2000 و500000 ألف فرنك أو بإحدى هاتين العقوبتين، كل من أدخل عمدا إلى نظام المعالجة الآلية للمعلومات بطريق مباشر أو غير مباشر وبدون مراعاة لحوق الغير، بيانات أو محا أو عدل في البيانات التي يحتويها أو في طرق معالجتها أو نقلها[1].

غير أن الانتقادات الفقهية التي وُجهت إلى بعض نصوص القانون ومنها النص المشار إليه أدت بالمشرع الفرنسي إلى تلافي هذه الانتقادات المتمثلة في العبارات "بطريق مباشر أو غير مباشر"، "بدون مراعاة حقوق الغير" و"طرق معالجتها ونقلها"؛ حيث تحفظ عليها الفقه وأعرض عنها، وفي قانون العقوبات الجديد الصادر سنة 1994 الذي أدمج نصوص قانون 1988 بين طياته في المواد (1/323 -7) والتي جاءت تحت عنوان "الاعتداءات علة نظام المعالجة الآلية للمعطيات" المضافة إلى قانون العقوبات الفرنسي الجديد والتي أضحت تمثل الفصل الثالث من الباب الثاني من القسم الثالث منه؛ حيث ذهب إلى "العقاب بالحبس لمدة خمس سنوات وغرامة قدرها خمسة وسبعين ألف يورو، كل من أدخل بيانات بطريقة غير مشروعة في نظام معالجة البيانات أو إلغاء أو تعديل البيانات التي يحتوي عليها النظام بطريقة غير مشروعة.

ثانيا: في التشريع الإماراتي

ميز المشرع الإماراتي، على النحو المبين أعلاه، بين الإضرار بالأنظمة المعلوماتية لإحدى مؤسسات الدولة والمرافق الحيوية؛ ففي حالة تدمير هذه النظم يعاقب الفاعل بالسجن المؤقت والغرامة التي لا تقل عن 500.000 درهم ولا تزيد على 3.000.000 درهم؛ وإذا وقعت الجريمة نتيجة لهجمة إلكترونية اعتبر ذلك ظرفا مشددا[2]؛ علاوة على ذلك تعاقب المادة السابعة من قانون مكافحة الشائعات والجرائم الإلكترونية على الاعتداءات على البيانات والمعلومات الحكومية في ثلاث وضعيات متدرجة؛ حيث يعاقب بالسجن المؤقت مدة لا تقل عن سبع سنوات والغرامة التي لا تقل عن 500.000 درهم ولا تزيد على 3.000.000 درهم كل من حصل أو استحوذ أو عدل أو أتلف أو أفشى أو سرب أو ألغى أو حذف أو نسخ أو نشر أو أعاد نشر بغير تصريح بيانات أو معلومات حكومية سرية[3].

نلاحظ مما سبق؛ أن المشرع الإماراتي لم يحدد مدة السجن المؤقت في حالة تدمير النظم المعلوماتية لإحدى مؤسسات الدولة والمرافق الحيوية؛ بيد أنه إذا أتلف الجاني البيانات والمعلومات الحكومية يعاقب بالسجن المؤقت مدة لا تنزل عن سبع سنوات؛ فضلا

[1] ينظر المادة 4/462 منه

[2] المادة الخامسة من قانون مكافحة الشائعات والجرائم الإلكترونية.

[3] البند الأول من المادة السابعة من قانون مكافحة الشائعات والجرائم الإلكترونية.

عن ذلك نلاحظ أنه عاقب بنفس الغرامة المالية في الواقعتين؛ إلا أنه تشدد في العقوبة البدنية والمالية إذا ترتب عن إتلاف المعلومات والبيانات الحكومية أضرارا للدولة، أو إذا ترتب عليها فقدان سرية عمل الأنظمة والبرمجيات الإلكترونية الخاصة بالمنشآت العسكرية والأمنية وما يتعلق بالاتصال ونقل المعلومات السرية؛ حيث تكون العقوبة السجن المؤقت مدة لا تقل عن 10 سنوات والغرامة لا تقل عن 500.000 درهم ولا تزيد على 5.000.000 درهم. في حين يعاقب ذات القانون المشار إليه بالسجن المؤقت كل من تلقى أي من البيانات والمعلومات المشار إليها في البند الأول من المادة السابعة، واحتفظ بها أو خزنها أو قبل التعامل بها أو استخدامها رغم علمه بعدم مشروعية الحصول عليها[1].

الفقرة الثانية: عقوبة الإتلاف المعلوماتي في ضوء التشريع المغربي

ميز المشرع المغربي في جريمة الرسوم الإلكتروني للحالة المدنية بين عقوبة أصلية وبديلة وإضافية[2]؛ وهو ما سنبرزه في ما يأتي:

أولا: العقوبات الأصلية

نص الفصل 607-6 من مجموعة القانون المغربي على معاقبة بالحبس من سنة إلى ثلاث سنوات وبالغرامة من 10000 إلى 200000 درهم أو بإحدى هاتين العقوبتين فقط كل من أدخل معطيات في نظام للمعالجة الآلية للمعطيات أو أتلفها أو حذفها منه أو غير المعطيات المدرجة فيه، أو غير طريقة معالجتها أو طريقة إرسالها عن طريق الاحتيال.

فضلا عن ذلك؛ فإن المشرع المغربي يعاقب على محاولة ارتكاب جنحة إتلاف نظم المعلومات المتعلقة بتدبير ورش الحماية الاجتماعية والبيانات المخزنة فيها بالعقوبة المطبقة على الجريمة التامة[3].

علاوة على ذلك فإن الفصل 607-9 يقضي بتطبيق عقوبة نفس الجريمة المرتكبة أو العقوبة المطبقة على الجريمة الأشد على كل من اشترك في عصابة أو اتفاق تم لأجل الإعداد لواحدة أو أكثر من الجرائم المنصوص عليها في هذا الباب، إذا تمثل الإعداد في فعل أو أكثر من الأفعال المادية." ومن ثم نرى على أن المشرع المغربي خص الجريمة موضوع الدراسة بخصوصية مفادها تطبيق نفس

[1] البند الثالث من المادة السابعة من القانون الإماراتي المشار إليه.

[2] ينص الفصل 14 من مجموعة القانون الجنائي على أنه:" تكون العقوبات إما أصلية أو بديلة أو إضافية.

تكون أصلية عندما يمكن الحكم بها وحدها دون أن تضاف إلى عقوبة أخرى.

وتكون بديلة عندما يمكن الحكم بها بديلا للعقوبة السالبة للحرية.

وتكون إضافية عندما لا يمكن الحكم بها وحدها، وتضاف إلى عقوبة أصلية أو بديلة، أو عندما تكون ناتجة عن الحكم بعقوبة أصلية."

[3] الفصل 607-8 من مجموعة القانون الجنائي المغربي.

العقوبة على الجريمة المقترفة حالة الاشتراك في عصابة أو اتفاق لأجل الإعداد لجريمة الإتلاف المعلوماتي؛ إلا أنه أحال ضمنيا على المشاركة في صورتها العادية على القواعد العامة[1].

أما بخصوص المساهمة فإن القانون 07.03 المتعلق بالمس بنظم المعالجة الآلية للمعطيات لم يتطرق إليها صراحة؛ ومن ثم نرى على أنه أحالها على القواعد العامة[2].

وتجدر الإشارة في هذا الصدد، أن المشرع المغربي شدد العقوبة في حالة ارتكاب جريمة الإتلاف المعلوماتي لنظم الحماية الاجتماعية؛ إذا كان الفاعل موظفا أو مستخدما أثناء مزاولة مهامه أو بسببها، سواء شخصيا أو سهل للغير القيام بها، وذلك بغية ضمان الثقة في النظم المعلوماتية موضوع الدراسة، وبالتالي تكون العقوبة المقررة لهذا الفعل هي الحبس من سنتين إلى خمس سنوات والغرامة من 100.000 إلى 200.000 درهم، مع مراعاة المقتضيات الجنائية الأشد.

بالإضافة إلى ذلك؛ شدد العقوبة على الجريمة الناص عليها الفصل 10-607 من مجموعة القانون الجنائي، الحبس من سنتين إلى خمس سنوات وبالغرامة من 50.000 إلى 2.000.000 درهم، من خلال تجريم مجموعة الأفعال التي تشكل الركن المادي لجريمة إتلاف النظم المعلوماتية محل التحليل والمناقشة، وتتجلى هذه الأفعال في صنع تجهيزات أو أدوات، أو إعداد برامج للمعلومات أو أية معطيات، أعدت أو اعتمدت خصيصا لأجل ارتكاب الجريمة محل الدراسة، أو تملكها أو حازها أو تخلى عنها للغير أو عرضها أو وضعها رهن إشارة الغير.

ومما تجب الإشارة إليه أن المشرع المغرب في القانون 07.03 المتعلق بالمس بنظم المعالجة الآلية للمعطيات؛ لم يتطرق إلى الشخص الاعتباري خلافا لما ذهب إليه المشرع القطري؛ حيث يعاقب الشخص المعنوي بالغرامة التي تزيد على 1000000 مليون ريال، إذا ارتكبت باسمه أو لحسابه إحدى الجرائم المنصوص عليها في القانون رقم 14 لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية، وذلك مع عدم الإخلال بالمسؤولية الجنائية للشخص الطبيعي التابع له[3]. والمشرع المصري من خلال القانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات الذي ينص في مادته 36 على أنه:" في الأحوال التي ترتكب فيها أي من الجرائم المنصوص عليها في هذا القانون باسم ولحساب الشخص الاعتباري، يعاقب المسؤول عن الإدارة الفعلية إذا ثبت علمه بالجريمة أو سهل ارتكابها تحقيقا لمصلحة له أو لغيره بذات عقوبة الفاعل الأصلي.

[1] انظر الفصل 129 من مجموعة القانون الجنائي المغربي.

[2] الفصل 128 من مجموعة القانون الجنائي المغربي.

[3] المادة 48 من قانون مكافحة الجرائم الإلكترونية القطري.

وللمحكمة أن تقضي بإيقاف ترخيص مزاولة الشخص الاعتباري للنشاط مدة لا تزيد على سنة، ولها في حالة العود أن تحكم بإلغاء الترخيص أو حل الشخص الاعتباري بحسب الأحوال، ويتم نشر الحكم في جريدتين يوميتين واسعتي الانتشار على نفقة الشخص الاعتباري."

ثانيا: العقوبات البديلة

عُرفت العقوبات البديلة، من خلال الفصل 1-35 من القانون رقم 43.22 المتعلق بالعقوبات البديلة[1]، بأنها العقوبات التي يحكم بها بديلا للعقوبات السالبة للحرية في الجنح التي لا تتجاوز العقوبة المحكوم بها من أجلها خمس سنوات حبسا نافذا. علاوة على ذلك؛ حدد الفصل 2-35 من القانون المذكور العقوبات البديلة في:

1- العمل لأجل المنفعة العامة؛

2- المراقبة الإلكترونية؛

3- تقييد بعض الحقوق أو فرض تدابير رقابية أو علاجية أو تأهيلية."

4- الغرامة المالية

علاوة على ذلك؛ حدد المشرع المغربي من خلال القانون المذكور، على سبيل الحصر، الجرائم التي لا يمكن العقاب عليها بمقتضى العقوبات البديلة وهي: الجرائم المتعلقة بأمن الدولة والإرهاب؛ الاختلاس أو الغدر أو الرشوة أو استغلال النفوذ أو تبديد الأموال العمومية؛ غسل الأموال؛ الجرائم العسكرية؛ الاتجار الدولي في المخدرات؛ الاتجار في المؤثرات العقلية؛ الاتجار في الأعضاء البشرية؛ والاستغلال الجنسي للقاصرين أو الأشخاص في وضعية إعاقة[2]. بالإضافة إلى ذلك لا يحكم بالعقوبات البديلة في حالة العود[3].

باستقرائنا للمقتضيات أعلاه؛ يتضح جليا أن جريمة الإتلاف المعلوماتي يسري عليها قانون العقوبات البديلة؛ حيث تعد وكما أسلفنا جنحة معاقب عليها من سنة إلى ثلاث سنوات وبالغرامة من 10000 إلى 200000 درهم أو بإحدى هاتين العقوبتين فقط. لكن إذا كان الغرض من الإتلاف هو إتيان أفعال ترقى إلى عمل إرهابي؛ فلا يمكن العقاب عليها بموجب العقوبات البديلة.

ثالثا: العقوبات الإضافية

[1] القانون رقم 43.22 المتعلق بالعقوبات البديلة الصادر بتنفيذه الظهير الشريف رقم 1.24.32 صادر في 18 من محرم 1446 (24 يوليو 2024)، الجريدة الرسمية عدد 7328 بتاريخ 17 صفر 1446 (22 أغسطس 2024)، الصفحة 5327.

يدخل هذا القانون حيز التنفيذ بصدور النصوص التنظيمية اللازمة لتطبيقه بالجريدة الرسمية في أجل أقصاه سنة.

[2] الفصل 3-35 من قانون العقوبات البديلة المشار إليه.

[3] الفقرة الثانية من الفصل 1-35 من قانون العقوبات البديلة المشار إليه.

نص المشرع المغربي على هذه العقوبات بمقتضى الفصل 11-607 من مجموعة القانون الجنائي الذي ورد فيه:" يجوز للمحكمة مع مراعاة حقوق الغير حسن النية أن تحكم بمصادرة الأدوات التي استعملت في ارتكاب الجرائم المنصوص عليها في هذا الباب والمتحصل عليه منها.

يمكن علاوة على ذلك، الحكم على الفاعل بالحرمان من ممارسة واحد أو أكثر من الحقوق المنصوص عليها في الفصل 40 من هذا القانون لمدة تتراوح بين سنتين وعشر سنوات.

يمكن أيضا الحكم بالحرمان من مزاولة جميع المهام والوظائف العمومية[1] لمدة تتراوح بين سنتين وعشر سنوات وبنشر أو بتعليق الحكم الصادر بالإدانة[2]."

تأسيسا عليه، يتضح أن المشرع المغربي وحماية للنظم المعلوماتية المتعلقة بتدبير ورش الحماية الاجتماعية من جريمة الإتلاف؛ قد نص على مصادرة الأدوات التي استعملت في ارتكاب الجريمة موضوع الدراسة، إلا أن الأمر يثير تساؤلا حول تفسير عبارة "الأدوات" هل تشمل البرامج التي استعملت في جريمة الإتلاف؛ حتى تسري عليها العقوبة الإضافية المتمثلة في المصادرة؟ فإذا كان المشرع المغربي لم يشر إلى مصادرة هذه البرامج؛ فإن قانون مكافحة الجرائم الإلكترونية الإماراتي كان أكثر توسعا في ما يخص المصادرة كعقوبة إضافية؛ وهو ما يستفاد من المادة 56 من هذا القانون الناص على أنه:" مع عدم الإخلال بحقوق الغير حسني النية، وفي حال الإدانة يحكم بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا المرسوم بقانون أو الأموال المتحصلة منها، وبحذف المعلومات أو البيانات."

وإذا كان الفصل 40 من مجموعة القانون الجنائي قد أجاز حرمان المحكوم عليه، في الحالات المحددة قانونا، من ممارسة حق أو عدة حقوق من الحقوق الوطنية أو المدنية أو العائلية المنصوص عليها في الفصل 26؛ وذلك لمدة تتراوح بين سنة وعشر سنوات؛ فإن الفصل 11-607 من مجموعة القانون الجنائي جعل هذه المدة تتراوح ما بين سنتين وعشر سنوات.

---

[1] عالج المشرع المغربي تدبير الحرمان من مزاولة جميع المهام والوظائف العمومية لمدة معينة بموجب الفصل 86 من مجموعة القانون الجنائي والذي جاء فيه:
" يجب على المحكمة أن تصرح بعدم الأهلية لمزاولة جميع الوظائف والخدمات العمومية في الأحوال التي نص فيها القانون على ذلك أو إذا تعلق الأمر بجريمة إرهابية.
ويجوز الحكم بهذا التدبير في غير الأحوال المشار إليها، عندما تلاحظ المحكمة وتصرح بمقتضى نص خاص بالحكم أن الجريمة المرتكبة لها علاقة مباشرة بمزاولة الوظيفة أو الخدمة وأنها تكشف عن وجود فساد في خلق مرتكبها لا يتلاءم ومزاولة الوظيفة أو الخدمة على الوجه المرضي.
ويحكم بعدم الأهلية لمدة لا يمكن أن تفوق عشر سنوات، ما لم ينص القانون على خلاف ذلك.
وتحسب هذه المدة من اليوم الذي ينتهي فيه تنفيذ العقوبة."

[2] تطرق المشرع المغربي إلى عقوبة النشر والتعليق ضمن الفصل 48 من مجموعة القانون الجنائي بالقول:
" للمحكمة، في الأحوال التي يحددها القانون، أن تأمر بنشر الحكم الصادر عنها بالإدانة كلا أو بعضا، في صحيفة أو عدة صحف تعينها، أو بتعليقه في أماكن تبينها.
والكل على نفقة المحكوم عليه من غير أن تتعدى صوائر النشر ما قدرته المحكمة لذلك ولا أن تتجاوز مدة التعليق شهرا واحدا."

بالإضافة إلى ما سلف ذكره؛ فإن المشرع المغربي لم يتعرض، في الفصل 11-607 من مجموعة القانون الجنائي، إلا لتدبير وقائي[1] واحد، يتمثل في الحرمان من مزاولة جميع المهام والوظائف العمومية لمدة تتراوح بين سنتين وعشر سنوات، في حين ثمة تدابير وقائية أخرى واردة في الفصل 61 من مجموعة القانون الجنائي. خلافا للمشرع الإماراتي الذي حدد ثلاثة تدابير وقائية للتصدي لجريمة إتلاف أو تدمير النظم الإلكترونية والمعلومات والبيانات الحكومية؛ من خلال قانون مكافحة الشائعات والجرائم الإلكترونية؛ حيث تنص مادته 59 من القانون المذكور على أنه:" يجوز للمحكمة عند الحكم بالإدانة في أي جريمة من الجرائم المنصوص عليها بهذا المرسوم بقانون أن تقضي بأي من التدابير الآتية:

1. الأمر بوضع المحكوم عليه تحت الإشراف أو المراقبة الإلكترونية أو حرمانه من استخدام أي شبكة معلوماتية، أو نظام المعلومات الإلكتروني، أو أي وسيلة تقنية معلومات أخرى، أو وضعه في مأوى علاجي أو مركز تأهيل للمدة التي تراها المحكمة مناسبة.

2. إغلاق الموقع المخالف إغلاقا كليا أو جزئيا متى أمكن ذلك فنيا.

3. حجب الموقع المخالف حجبا كليا أو جزئيا للمدة التي تقررها المحكمة.

يعاقب بالحبس مدة لا تزيد على سنة أو بغرامة لا تزيد على 5000 خمسة آلاف درهم، كل من خالف أي تدبير من التدابير المحكوم بها، وللمحكمة أن تأمر بإطالة التدبير مدة لا تزيد على نصف المدة المحكوم بها ولا تزيد في أية حال على 3 ثلاث سنوات أو أن تستبدل به تدبيرا آخر مما ذكر."

وبخصوص العقوبة الإضافية المتمثلة في نشر أو تعليق الحكم الصادر بالإدانة؛ فنلاحظ أن المشرع المغربي لم يحدد في الفصل 11-607 كيفية النشر أو التعليق ومدتها، بمعنى آخر هل تم ضمنيا الإحالة على ذلك في القواعد العامة الناص عليها الفصل 48 من مجموعة القانون الجنائي؛ الذي ينص على أنه:" للمحكمة، في الأحوال التي يحددها القانون، أن تأمر بنشر الحكم الصادر عنها بالإدانة كلا أو بعضا، في صحيفة أو عدة صحف تعينها، أو بتعليقه في أماكن تبينها. والكل على نفقة المحكوم عليه من غير أن تتعدى صوائر النشر ما قدرته المحكمة لذلك ولا أن تتجاوز مدة التعليق شهرا واحدا."

[1] راجع: عبد الواحد العلمي، شرح القانون الجنائي المغربي، القسم العام، مطبعة النجاح الجديدة، الدار البيضاء، الطبعة العاشرة 2022، الصفحة 462 وما بعدها.

الخاتمة:

مما سبق؛ نستنتج أن جريمة الإتلاف المعلوماتي تعد جريمة خطيرة لما لها من آثار على النظم المعلوماتية؛ فتدمير الوثائق والمعطيات المعلوماتية يشكل تحديا كبيرا للتشريع المغربي والأجنبي؛ وهو ما حث المشرع في هذه الدول إلى سن نصوص خاصة تتلاءم وخصوصية هذا النوع من الجرائم المستحدثة.

في هذا السياق نقترح ما يأتي:

- ضرورة تبسيط الإجراءات الإدارية للتسجيل في السجل الوطني خصوصا المعايير المحددة للمؤشر؛ تفاديا للتصريح المخالف للقانون؛
- تدقيق العبارات الواردة في القانون 03.07 المتعلق بالمس بنظم المعالجة الآلية للمعطيات؛
- تحديث مقتضيات المسطرة الجنائية؛ وذلك من خلال سن قواعد إجرائية تتلاءم وجريمة الإتلاف المعلوماتي باعتبارها جريمة إلكترونية؛
- توسيع إبرام اتفاقيات دولية؛ خاصة مع الدول الإفريقية في مجال الحماية الاجتماعية والأمن السيبراني؛
- تخصيص قضاء متخصص في الجرائم السيبرانية.

لائحة المراجع:

– عبد الكريم عباد، الجريمة المعلوماتية، المجلة الوطنية للعلوم القانونية والقضائية، العدد الأول، مطبعة الأمنية، الرباط، 2016.

– عبد المجيد كوزي، الحماية الجنائية للمعطيات في المجال المعلوماتي، المجلة المغربية للقانون الجنائي والعلوم الجنائية، العدد 3، 2016.

– عبد الواحد العلمي، شرح القانون الجنائي المغربي، القسم العام، مطبعة النجاح الجديدة، الدار البيضاء، الطبعة العاشرة 2022.

– علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب، دار الجامعة الجديدة، الإسكندرية، الطبعة الأولى، سنة 1997.

– عمار عباس الحسيني، جريمة الإتلاف المعلوماتي–دراسة قانونية مقارنة، منشورات زين الحقوقية، بيروت–لبنان، الطبعة 2018.

– غنام مُحَمَّد غنام، عدم ملاءمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر، بحث مقدم إلى مؤتمر القانون والكمبيوتر والأنترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة– مايو 2000، المجلد الثاني، الطبعة الثالثة، سنة 2004.

– مجاني الطلاب، دار المجاني ش.م.ل، بيروت، لبنان، الطبعة الثالثة، سنة 1996.

– مُحَمَّد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، الطبعة الأولى، سنة 1984.

– مُحَمَّد عبد الله أبو بكر سلامة، جرائم الكمبيوتر والأنترنت، دار النشر منشأة المعارف، الإسكندرية، مصر، سنة 2006.

– ممحمود مُحَمَّد محمود جابر، الجرائم الناشئة عن استخدام الهواتف النقالة (جرائم نظم الاتصالات والمعلومات)، المكتب الجامعي الحديث، الإسكندرية، مصر، طبعة 2018.

– نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، الأردن، السنة 2008.

– Emeric Jeansen, Droit de la protection social, LexisNexis, Paris, France, 2013.