•• مجلة الاجتهاد القضائي •• المجلد 15 •• العدد 01•• (العدد التسلسلي 31) •• مارس 2023 (ص ص: 257 – 272)••
مخبر أثر الاجتهاد القضائي على حركة التشريع ••• جامعة محمد خيضر بسكرة

الجريمة السيبرانية في الجزائر والعقوبات المقرّرة لها

Cybercrime in Algeria and the penalties prescribed for it

الدكتورة نادية لاكلي [1]

مخبر فلسفة، علوم وتنمية بالجزائر (جامعة وهران 2)

جامعة بلحاج بوشعيب - عين تموشنت (الجزائر)

nadia.lakli@univ-temouchent.edu.dz

تاريخ الارسال:	تاريخ القبول:	تاريخ النشر
15 نوفمبر 2022	13 مارس 2023	30 مارس 2023

الملخص:

أدّى انتشار تكنلوجيا المعلومات ووسائل الإتصال في عصرنا الحالي إلى ظهور نوع جديد من الجرائم تختلف تماما عن الجرائم التقليدية من حيث طبيعتها، خصائصها، أنواعها ووسائل تنفيذها، ويطلق عليها تسمية "الجرائم الإلكترونية" نظرا لتنفيذها عبر الشبكات الحاسوبية وعلى المال المعلوماتي. وتعتمد هذه الجرائم على اختراق أمن المعلومات الإلكترونية وتدميرها بهدف الحصول على معلومات سريّة لأهداف مادية أو معنوية. وتختلف أسباب ظهور الجريمة الالكترونية باختلاف أنواعها، ولقد رصد المشرّع الجزائري للجريمة المعلوماتية بشتى أنواعها عقوبات ردعية لها. وسنتعرّف في دراستنا على مفهوم وأنواع الجرائم الالكترونية مع تحديد العقوبات المطبقة عليها في التشريع الجزائري.

الكلمات المفتاحية: جريمة إلكترونية – النظام المعلوماتي – عقوبات – أصلية – تكميلية

Abstract:

The spread of information technology and means of communication in our time has led to the emergence of a new type of crime that is completely different from traditional crimes in terms of their nature, characteristics, types and means of implementation. It is called "electronic crimes" due to its implementation through computer networks and information money. These crimes depend on penetrating and destroying the security of electronic information in order to obtain confidential information for material or intangible purposes. The reasons for the emergence of cybercrime differ in all its types, and the Algerian legislator for information crime of all kinds has set deterrent penalties for it. In our study, we will get acquainted with the concept and types of cybercrime, along with defining the penalties applied to it in Algerian legislation.

key words:

Electronic crime – information system - sanctions - original - complementary

[1] **المؤلف المرسل: د. نادية لاكلي** ——— ***Email: lakli.nadia@gmail.com***

مقدمة:

أدّى التطور التكنولوجي في عصرنا الحالي إلى استحداث نوع جديد من الجرائم تختلف تماما عن الجرائم التقليدية والمعروفة بـ "الجرائم الإلكترونية" أو "الجرائم السيبرانية" أو "جرائم الفضاء الإلكتروني"، ومهما اختلفت تسميات هذا النوع من الجرائم إلا أنّ مرتكبها يستخدم نفس الوسيلة والمتمثلة في الحاسوب تُنفّذ هذه الجرائم عبر الشبكات الحاسوبية.

وتعتمد هذه الجرائم على اختراق أمن المعلومات الإلكترونية وتدميرها بهدف الحصول على معلومات سريّة لأهداف مادية أو معنوية. ويطلق على الأشخاص مرتكبي الجرائم الإلكترونية مسمّى "القراصنة الفضوليون" عندما يتعلق الأمر بدخول نظام معلوماتي من باب الفضول والهواية دون تعديل المعلومات أو العبث فيها، أو "القراصنة المحترفون" عندما يتعلق الأمر بالعبث في المعلومات من أجل ارتكاب جريمة كالسرقة أو التزوير.

وتتميّز الجرائم الإلكترونية عن باقي الجرائم التقليدية بسهولة وقوع الضحيّة في فخها من جهة وصعوبة إثباتها من جهة أخرى، وأصبحت هذه الجريمة شائعة في وقتنا الراهن نظرا للتطور التكنولوجي ممّا دفع بمختلف التشريعات إلى توقيع عقوبات صارمة على مرتكبيها نظرا لخطورتها نتيجة تعدّد أنواعها.

ولقد حاول المشرّع الجزائري مواكبة التطور التكنولوجي في مجال مكافحة الإجرام المعلوماتي وذلك من خلال تعديل قانون العقوبات بموجب القانون رقم 04-15[1]، حيث خصّص القسم السابع مكرر منه للجرائم المعلوماتية تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات".

وتتجلى أهمية هذه الدراسة في حداثة وانتشار هذا النوع من الجرائم، واختلافها عن الجرائم التقليدية نظرا للخصائص التي تتميّز بها وصعوبة اكتاشفها.

وتهدف هذه الدراسة إلى تحديد مفهوم الجريمة الالكترونية وتبيان أنواعها، وتسليط الضوء على دور التشريع الجزائري في ردع هذه الجرائم من خلال توقيع العقوبات اللازمة على مرتكبيها.

وتأسيسا لما سبق نطرح الإشكالية التالية: مامدى فعالية القواعد القانونية في التشريع الجزائري في ردع الجرائم الالكترونية؟

وللإجابة على هذه الإشكالية سنعتمد في دراستنا على المنهج الوصفي والتحليلي والذي سنتناول من خلاله في المبحث الأول إلى الطبيعة القانونية للجريمة الإلكترونية من خلال التعرّف على مفهومها وخصائصها، بينما سنتطرق في المبحث الثاني إلى أنواع الجرائم الإلكترونية والعقوبات الردعية لها.

المبحث الأول: الطبيعة القانونية للجريمة الإلكترونية

سنتعرّف على مفهوم الجريمة الإلكترونية والخصائص التي تميّزها عن باقي الجرائم التقليدية.

المطلب الأول: مفهوم الجريمة الإلكترونية

تعتبر الجريمة الإلكترونية من الجرائم التي تنوعت تسمياتها، فهناك من يسميها بجريمة الكمبيوتر نسبة للأداة المُستعملة فيها، وهناك من يسميها بالجريمة المعلوماتية باعتبارها تمس بمعلومات سريّة، وهناك من يسمّيها بجريمة الإنترنت باعتبارها قائمة على شبكة الانترنت، أو جريمة التقنية العالية، غير أن التّسمية الراجحة في الوقت الراهن هي الجريمة الإلكترونية. ولم تبيّن النصوص القانونية مفهوم هذه الجريمة بل استندت إلى أركانها ووسائل ارتكابها.

ويقصد بالجريمة الإلكترونية مجموعة من الأفعال غير القانونية المُرتكبة عبر أجهزة إلكترونية وشبكات الإنترنيت والتي تهدف إلى الإضرار بالأفراد أو المؤسسات من خلال الولوج إلى النظم المعلوماتية الخاصة بهم.

ويعرّفها البعض[2] بأنها: " فعل إجرامي يُستخدم الحاسب في ارتكابه كأداة رئيسيّة"، ويعرّفها البعض الآخر[3] بأنها: " تشمل كل أشكال السلوك غير المشروع الذي يُرتكب باستخدام الحاسب". كما يعرّفها آخرون بأنها: " كل فعل إيجابي أو سلبي عمدي يهدف إلى الإعتداء على تقنية المعلوماتية مهما كان غرض الجاني".[4]

وعليه، تتمثّل الجريمة الإلكترونية في استخدام الأجهزة التقنية الحديثة كالحاسوب أو الهواتف النقّالة في تنفيذ أغراض غير مشروعة بهدف الإضرار بالمجتمع.[5]

أمّا المشرع الجزائري فلم يتطرّق إلى مفهوم الجريمة الإلكترونية وإنّما استعمل مصطلح "المساس بأنظمة المعالجة الآلية للمعطيات" في المواد من 394 مكرر إلى 394 مكرر 7 من قانون العقوبات، وعرّفها في القانون رقم 09-04 المتضمن للقواعد الخاصة بالوقاية المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها[6] في المادية الثانية منه بأنّها جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأيّ جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للإتصالات الالكترونية.

وعليه، يعتبر المشرع الجزائري النظام المعلوماتي والمعطيات التي تدخل في الحاسب الآلي جوهر الجريمة الإلكترونية.، ويتضمّن نظام المعالجة الآلية للمعطيات على عناصر مادية كاجهزة الربط ومعنوية كالبرامج.

ولقد عرّف مجلس الأمة الفرنسي نظام المعالجة الآلية للمعطيات بأنّه "مجموعة منسجمة تتكوّن من وحدة أو عدة وحدات معالجة، ذاكرة، برامج، معطيات، وحدات إدخال وإخراج، واتصال بين هذه الوحدات التي تؤدّي إلى إعطاء نتيجة معينة، وتكون هذه المجموعة محمية تقنيا من خلال أية وسيلة إئتمان"[7].

بينما عرّف المشرّع الجزائري نظام المعالجة الآلية للمعطيات في المادة الثانية من القانون رقم 09-04 المتضمن للقواعد الخاصة بالوقاية المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها بأنّه:" كل نظام أو مجموعة من الانظمة منفصلة كانت أم متصلة بعضها البعض أو المرتبطة والتي يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معيّن".

نلاحظ مما سبق تقارب التعريفات بين التشريع الفرنسي والجزائري غير أنّ هذا الأخير لم يشترط أن تكون هذه المجموعة محميّة تقنيا غلى عكس المشرّع الجزائري، وحسن مافعل المشرّع بتعريفه لنظام المعالجة الآلية للمعطيات بشكل عام دون اشتراط الحماية التقنيّة، وذلك من أجل توسيع الحماية القانونية وردع جميع الجرائم الالكترونية حتى في حالة مساسها بمعطيات غير محمية.

ونشير إلى أنّه لا يقصد بنظام المعالجة الآلية للمعطيات الحاسوب فقط بل كل نظام من شأنه القيام بهذه المعالجة الآلية، وعليه تعتبر شبكة الانترنت نظام معالجة آلية للمعطيات بالاضافة إلى البريد الإلكتروني ومواقع الانترنت والبطاقات الإلكترونية كالبطاقات الإلكترونية البنكية، وكذلك الأقراص المرنة والاقراص النقالة والاقراص المضغوطة الخاصة بتخزين المعلومات[8].

وتتعدّد أسباب قيام الجريمة المعلوماتية بل تختلف أنواعها باختلاف شخصيات مرتكبيها وظروفهم النفسية والاجتماعية، فقد يكون السبب مجرد فضول من قبل مرتكب هذه الجريمة ونيّة الإضرار بصاحبها، كما قد يكون السبب اجتماعي إذ قد تدفع حاجة الشخص ورغبته في الحصول على المال إلى ارتكاب هذا النوع من الجرائم للكسب السريع والسهل من خلال الإبتزاز مقابل مبالغ مالية.

كما قد يكون السبب الشخصي بهدف الانتقام كالجريمة التي يرتكبها موظف ازاء مديره في الشركة بعد فصله من العمل، وقد يكون الدافع سياسيا يهدف إلى اختراق شبكات حكومية للتجسّس.

لكن أحيانا يكون الدافع من هذه الجريمة مجرد اللهو فقط كإنشاء بعض الألعاب التي يحمّلها الأشخاص على هواتفهم والتي تحمل في الحقيقة فيروسات تعطّل أو تدمّر معطيات

جهازهم، أو من خلال الألعاب التي قد تؤدي بحياة الأطفال مثلما حدث مؤخرا في لعبة "الحوت الأزرق" والتي أودت بحياة العديد من الأطفال.

المطلب الثاني: خصائص الجريمة الإلكترونية

إنّ الطابع المُستحدث للجريمة الإلكترونية يميّزها عن باقي الجرائم التقليدية إذ أصبح بإمكان الشخص ارتكاب الجريمة دون التنقل وبمجرد استخدامه لحاسوبه، ولعلّ من أهم الخصائص التي تميّز الجريمة الإلكترونية عن باقي الجرائم تتمثّل في:

– ارتكاب الجريمة عبر شبكة الإنترنيت مما يجعلها عابرة للحدود ولا تقتصر على إقليم معيّن، فقد يكون الجاني في بلد والمجني عليه في بلد آخر وقد يكون الضرر المُحتمل في بلد ثالث، وتشكّل هذه الخاصيّة أكبر عائقا أمام الجهات القضائية نظرا لصعوبة تحديد الجهة القضائية المختصة في الفصل في النزاع وكذا القانون الواجب تطبيقه.[9]

وتعد قضية "مرض نقص المناعة المكتسبة" لسنة 1989 أبرز مثال يجسّد لنا هذه الخاصيّة، إذ قام شخص يدعى " جوزيف بيب" بتوزيع عدد من النسخ الخاصة ببرنامج يهدف إلى إعطاء بعض المعلومات والنصائح عن مرض نقص المناعة المكتسبة "الإيدز"، غير أن هذا البرنامج كان يحتوي على فيروس يهدف إلى تعطيل حاسوب الشخص المتطلّع على البرنامج ثم يقوم بإرسال رسالة يطلب فيها من صاحب الحاسوب إرسال مبلغ مالي من أجل الحصول على مضاد الفيروس، لكن تم القبض على المتهم "جوزيف بيب" في الولايات المتحدة الأمريكية وطالبت المملكة المتحدة بتسليمه لها لمحاكمته باعتباره مواطن انجليزي غير أن الولايات المتّحدة الأمريكية رفضت تسليمه بحجة أن الجريمة ارتكبت في اقليمها وعلى أحد مواطنيها، لكن لم تستمر إجراءات المحاكمة نظرا لحالته العقلية.

ولقد كان القضاء الجنائي الفرنسي لفترة طويلة يرفض البت في القضايا المتعلقة بالجرائم الإلكترونية وكان يحيلها إلى القضاء المدني لعدم تخصّصه في هذا المجال، حيث أكّدت محكمة النقض الفرنسية في إحدى القضايا المرفوعة أمامها والتي تتلخص في استعمال أحد الاشخاص لبطاقته الإئتمانية بصورة احتيالية مكّنته من الحصول على مبلغ يفوق المبلغ المحدّد في رصيده فقام البنك برفع دعوى ضدّه، لكن اعتبرت محكمة النقض بأنّه لا يشكّل هذا التصرف جريمة وبالتالي يجب عرض النزاع على القاضي المدني، ثمّ تراجع القضاء الفرنسي عن موقفه ازاء الجرائم المعلوماتية لاسيما مع التطور التكنولوجي الذي شهده العالم[10].

– صعوبة أو استحالة إثبات الجريمة الإلكترونية لعدم ترك أيّ أثر للجريمة بعد ارتكابها، إذ يمكن للجاني أن يحذف المعلومات والمعطيات المتعلّقة به مباشرة بعد ارتكاب الجريمة

مما يستحيل إثباتها، فالجريمة الإلكترونية لا تترك أدلّة ملموسة يُستند إليها لاسيما عندما ترتكب الجريمة في دولة معيّنة لكن تنتج آثارها في دولة أخرى.

ورغم الجهودات المبذولة من قبل التشريعات في تعزيز الإجراءات لكشف الجرائم المعلوماتية من خلال تعين هيئات مختصة في هذا المجال، إلا أنّ صعوبة إثباتها مازات قائمة.

- الخبرة التقنية والفنيّة لمرتكب الجريمة الإلكترونية مما يؤدي إلى سهولة وقوع الضحية في فخّه، وصعوبة قيام رجال التحقيق بمهامهم في البحث والتحرّي، لذلك يُفضّل أن يستعان بمحقّق خبير في الجرائم المعلوماتية وهذا هو المعمول به حاليا في الولايات المتحدة الأمريكية.[11]

- قلة الإبلاغ عن الجريمة الإلكترونية من قِبل الضحية لعدم القدرة على إثباتها، إضافة إلى حرص الضحية على الحفاظ على سمعته. ونشير إلى قلة الإجتهادات القضائية المتعلّقة بهذه الجرائم سواء في التشريع الجزائري أو التشريعات المقارنة نظرا لندرتها.

- قيام الجريمة من خلال الحاسب الآلي وشبكة الانترنيت، إذ يشكّل كل منهما الأداة الرئيسية في ارتكاب الجريمة.

- شخصيّة الجاني في حد ذاته إذ يُطلق على مرتكبي الجرائم الإلكترونية " المجرمون المعلوماتيون" لتمييزهم عن المجرمين التقليديّين، كما يطلق عليهم كذلك تسمية "القراصنة"، ونفرّق بين القراصنة الفضوليون الذين يجتاحون المعلومات السرّية للغير من باب الهواية والفضول كاختراق حساب شخصي للإطلاع على الصور، وبين القراصنة المحترفون الذين يرتكبون جرائم معلوماتية خطيرة تلحق أضرارا وخسائر كبيرة للضحية لاسيما عندما يتعلق الأمر باختلاس أموال مؤسسات مالية، أو ابتزاز بعض الشخصيات السياسية بهدف الحصول على المال. بل قد يصل الأمر إلى ارتكاب جرائم إرهابية من خلال تجهيز جماعات متطرفة.

المبحث الثاني: أنواع الجرائم الإلكترونية والعقوبات الردعية لها

سنتعرّف على أنواع الجرائم الإلكترونية، ثم سنتناول العقوبات المقرّرة لها.

المطلب الأول: أنواع الجرائم الإلكترونية

يصعب تعداد جميع أصناف الجرائم الإلكترونية باعتبارها تستند إلى تقنيات حديثة، غير أنه يمكن تقسيمه إلى نوعين: الجرائم الإلكترونية المرتكبة بواسطة النظام المعلوماتي، وتلك المرتكبة على النظام المعلوماتي.

الفرع الأول: الجرائم الإلكترونية المرتكبة بواسطة النظام المعلوماتي

ونفرّق في هذا المجال بين الجرائم الإلكترونية المُرتكبة ضد الأشخاص الطبيعية، وتلك المُرتكبة ضد الأشخاص المعنويّة.

أوّلا- الجرائم الإلكترونية المُرتكبة ضدّ الأشخاص الطبيعية:

وتسمى كذلك بجرائم الإنترنيت الشخصية كونها تمس بالأفراد من خلال الوصول إلى هويّتهم الشخصية عن طريق قرصنة حساباتهم الشخصية وانتحال شخصيتهم أو الإطّلاع على صورهم الشخصية لاستعمال غير مشروع، كابتزازهم بها بهدف كسب المال.

وعليه، يعدّ استخدام النظام المعلوماتي في الإعتداء على حرمة الأفراد جريمة يعاقب عليها القانون. وتتمثّل الجرائم الإلكترونية ضد الأفراد الأكثر شيوعا في انتحال شخصيات فنيّة أو سياسيّة والتشهير بها عبر المواقع الإلكترونية من خلال الولوج إلى النظام المعلوماتي الخاص بالضحايا واستخدام معلوماتهم وصورهم الشخصية التي تم سرقتها من حساباتهم الخاصة، وتهديدهم بها مقابل الحصول على المال.

كما يمكن للمجرم اختراق النظام المعلوماتي للشخص للإعتداء على حقوقه الفكرية والأدبية والفنيّة من خلال سرقة بعض المعلومات العلمية مثلا ونسبها إليه، أو الإعتداء على براءة الإختراع إذ تعتتبر كلها حقوقا معنوية شخصية محمية قانونا.[12] وغالبا ما تتمّ الجرائم الإلكترونية ضدّ الأفراد من خلال الولوج إلى بريدهم الإلكتروني للحصول على هويتهم الشخصية.

ونشير إلى أنّ المشرّع الجزائري قد كرّس مجموعة من الآليات لحماية الأشخاص في العالم الافتراضي لاسيما مع تعدّد مواقع التواصل الاجتماعي وخطورتها وذلك بموجب القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي[13]، حيث أكدت المادة الثانية منه على ضرورة معالجة المعطيات ذات الطابع الشخصي في إطار احترام الكرامة الإنسانية والحياة الخاصة والحريات العامة، كم استحدث هذا القانون سلطة وطنية لحماية المعطيات ذات الطابع الشخصي والتي تتخذ إجراءات غدارية في حالة خرق أحكام هذا القانون من طرف المسؤول عن المعالجة، كما يمكنها القيام بالتحريات اللازمة ومعاينة المحلات التي تتم فيها المعالجة ماعدا محلات السكن، كما يمكنها الولوج على المعطيات المعالجة وجميع المعلومات والوثائق أيا كانت دعامتها[14].

ونظرا للتطور التكنولوجي في المجال التجاري والذّي أدّى إلى ظهور التجارة الالكترونية، كرّس المشرّع الجزائري حماية للمستهلك الالكتروني من خلال حماية بياناته الالكترونية لاسيما تلك المتعلقة ببطاقة الدفع في حالة استعمالها لاقتناء منتوجاته، فنجد أنّ القانون رقم 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين[15] خصّص إجراءات تقنية معيّنة لحماية وسائل الدفع الالكتروني من الهجمات السيبرانية تتمثّل في التوقيع والتصديق، إذ يخضع التوقيع الالكتروني إلى تقنية التشفير والمتمثّلة في تحويل البيانات

المتعلّقة ببطاقة الدفع الإلكتروني إلى رموز مبهمة لا يمكن للغير الاطلاع عليه أو فهمها إلا من خلال استخدام المفتاح السري لها لفك هذه الشفرة[16] فنظرا لحساسية التوقيع الإلكتروني والمعاملات الإلكترونية يشترط ان تصدر تقنية التشفير من جهة مختصة بذلك، ولقد خوّل المشرّع الجزائري بموجب المادة 14 من القانون رقم 15-04 هذا الاختصاص إلى الهيئة الوطنية المكلّفة باعتماد آليات إنشاء التوقيع الإلكتروني والتحقّق منه، فلا يحق حيازة أو إفشاء أو استعمال بيانات إنشاء توقيع إلكتروني من طرف الغير، ويعتبر هذا التصرّف غير مشروع ومعاقب عليه بمقتضى المادة 68 من القانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين، إذ تتمثّل العقوبة بالنسبة للشخص الطبيعي في الحبس من 03 أشهر إلى 03 سنوات وغرامة مالية من 1000.000دج إلى 5000.000دج أو بإحدى هاتين العقوبتين.

أمّا بالنسبة للتصديق الالكتروني فلقد أنشأ المشرّع الجزائري بموجب القانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين في الباب الثالث منه ثلاث سلطات للتصديق الإلكتروني:

- السلطة الوطنية تهتم بإعداد سياسة التصديق الإلكتروني والسهر على تطبيقها، والموافقة على سياسات التصديق الصادرة عن السلطتين الحكومية والاقتصادية.

- السلطة الحكومية والتي يكمن دورها في متابعة ومراقبة التصديق الإلكتروني، بالإضافة إلى إعداد القواعد والإجراءات التنظيمية والتقنية الخاصة بالتوقيع والتصديق الإلكترونيّين والسهر على تطبيقهما بعد الحصول على موافقة السلطة الوطنية وهذا ما أقرّته المادة 28 من القانون رقم 15-04.

- السلطة الاقتصادية والتي خوّلها المشرّع بموجب المادة 30 من القانون رقم 15-04 مجموعة من السلطات منها سلطة منح التراخيص لمؤدّي خدمات التصديق الإلكتروني والموافقة على سياسات التصديق الصادرة عنهم والسهر على تطبيقها، واتخاذ التدابير اللازمة لضمان استمرارية هذه الخدمات في حالة عجز مؤدي خدمات التصديق الإلكتروني عن تقديمها. كما يمكن أن تلعب السلطة الاقتصادية دور التحكيم في النزاعات القائمة بين مؤديي خدمات التصديق الإلكتروني فيما بينهم أو مع المستعملين.

وتسند لمؤدّي خدمات التصديق الالكتروني عملية التصديق لضمان صحة البيانات الالكترونية، ثم يقوم مؤدّي خدمات التصديق الإلكتروني بإصدار شهادة تثبت بأنّ التوقيع الإلكتروني صحيحا وصادرا عن صاحبه الحقيقي وأنّ البيانات كلّها صحيحة لا احتيال فيها، وأنّه يستوفي جميع الشروط القانونية المطلوبة، وتسمّى هذه الشهادة بشهادة التصديق الإلكتروني[17].

كما أكّد المشرّع على ضرورة إنشاء واستغلال منصات الدفع الإلكتروني حصريّا من طرف البنوك المعتمدة من قبل بنك الجزائر وبريد الجزائر وهذا ما نصت عليه المادة 27 من القانون رقم 18-05 المتعلق بالتجارة الالكترونية[18] في فقرتها الثانية، وتخضع منصات الدفع الإلكتروني لرقابة بنك الجزائر لضمان استجابتها لسرية البيانات وسلامتها وأمن تبادلها، وهذا ما جاء في نص المادة 29 من القانون رقم 18-05 المتعلق بالتجارة الإلكترونية.

ثانيا- الجرائم الإلكترونية ضد الأشخاص المعنوية:

هي جرائم تستهدف المؤسسات بشتّى أنواعها، يقوم الجاني من خلالها بإتلاف الوثائق المهمة للمؤسسة أو برامجها الخاصة، أو استعمال بيانات غير مسموح بها من أجل اختلاس المال من المؤسسات المالية.

ومن بين الجرائم الإلكترونية الشائعة في هذا المجال السرقة الواقعة على المؤسّسات المالية لاسيما في المجتمعات المتقدّمة، إذ يقوم الجاني باختلاس البيانات الخاصة بزبائن البنك والمحفوظة في برنامج خاص ويستخدم شخصية الضحية لتحويل المال لحسابه الخاص. أو يقوم الجاني بإنشاء صفحة انترنيت مطابقة لصفحة أحد البنوك الكبرى ويطلب من العميل إدخال بياناته الخاصة من أجل استخدامها في سرقة المال.

ولا يقتصر الأمر على الأشخاص الطبيعية والمعنوية فحسب، بل قد تمتد الجريمة الإلكترونية إلى المساس بأمن الدولة من خلال اختراق الجاني للمواقع الخاصة بالدولة كالمواقع العسكرية، ونشر المعلومات السريّة بهدف المساس بأمن الدولة بواسطة برامج متخصصة في فك أو سرقة كلمة السر.

الفرع الثاني: الجرائم الإلكترونية المرتكبة على النظام المعلوماتي

بالإضافة إلى الجريمة الإلكترونية التي تُرتكب بواسطة النظام المعلوماتي، توجد جرائم إلكترونية يكون النظام المعلوماتي في حد ذاته محلّ الجريمة، وتستهدف هذه الجرائم إمّا المكونات المادية أو المنطقيّة (برامج) للنظام المعلوماتي أو المعلومات المُدرجة في النظام المعلوماتي.

أوّلا- الجرائم الواقعة على المكوّنات المادية للنظام المعلوماتي:

ويقصد بها تلك الجرائم التي تستهدف الأجهزة والمعدّات المُلحقة التي تستخدم في تشغيل النظام المعلوماتي كالأسطوانات مثلا وذلك من خلال سرقتها أو إتلافها عمدا، إذ تكمن القيمة الحقيقية للمعدات فيما تحتويه من معلومات.[19]

ثانيا- الجرائم الواقعة على برامج النظام المعلوماتي:

يتميّز مرتكب هذه الجريمة بمعرفة تقنية عالية في المجال المعلوماتي، وتتمثل هذه الجرائم في الدخول إلى النظام المعلوماتي للشخص والبقاء فيه لتعديل أو حذف بياناته أو

الإستيلاء على البيانات الشخصية لاستعمالها لأغراض غير مشروعة، كسرقة المال وغالبا ما تكون في مجال المؤسسات المالية، كما تتجلى هذه الجريمة من خلال التلاعب في البرامج بزرع برنامج فرعي في البرنامج الأصلي يسمح بالولوج في أي نظام معلوماتي. وتعدّ جريمة البقاء في النظام المعلوماتي جريمة مستمرة لأنها مقترنة بفترة زمنية تستمر فيها الجريمة.

كما يمكن تزويد البرنامج بمجموعة تعليمات إضافية يسهل الوصول إليها بواسطة شفرة تسمح الحصول على جميع المعطيات التي يتضمنها النظام المعلوماتي.[20] وتعتبر المعلومة المعاجة آليا أساس عمل النظام المعلوماتي، لذلك قد تكون محل الجريمة الإلكترونية من خلال تعديل المعلومات الموجودة داخل النظام أو إتلافها من خلال الإستعانة ببعض البرامج الفيروسية، ويعد برنامج حصان طراودة (*Le cheval de troie*) من أشهر هذه البرامج وهو نوع من الفيروسات الضارّة يظهر في شكل برنامج مفيد لخداع الضحيّة لكنّه يحتوي على فيروس يسمح للشّخص بالتجسّس على الآخرين وسرقة بياناتهم بكل سهولة.

كما توجد انواع أخرى من الفيروسات الضارة كفيروس "الدودة" (*Le vers*) وهو عبارة عن برنامج ينتشر في شبكات المعلوماتية بصورة أوتوماتيكية، وتتمثل وظيفته في التكاثر بشكل يؤدي إلى تعطيل الشبكات المعلوامتية لتسهيل تسرّب مختلف الفيروسات[21].

ويوجد أيضا فيروس القنبلة المنطقيّة (*La bombe logique*) وهو عبارة عن برنامج يتم تنفيذه في فترة زمنية معينة، ويقوم هذا الفيروس بتسهيل تنفيذ العمليات غير المشروعة من قِبل الجاني وتدمير النظام المعلوماتي[22].

ونشير إلى أنّه مجرد استعمال الفيروس المعلوماتي يدل على وجود فعل مجرّم قانونا، وقد اعتبر القضاء الفرنسي في إحدى القضايا المعروضة أمامه في هذا المجال بأنّه تعتبر شركة الصيانة في مجال المعلوماتية مسؤولة عن الضرر اللاحق بالنظام المعلوماتي المملوك للغير نظرا للإستعمال غير المشروع لفيروس القنبلة الذي أدّى إلى تدمير النظام المعلوماتي، واعتبر القاضي في هذه القضيّة مسيّر الشركة فاعلا أصليا للجريمة بينما اعتبر باقي العمال شركاء له فيها[23]. لذلك ينصح دائما بتحميل البرامج المضادة للفيروسات المعلوماتية بهدف حماية النظام المعلوماتي منها.

وعليه، يمكن أن تتجلى جريمة الاعتداء على النظام المعلوماتي من خلال الدخول والبقاء فيه بشكل غير مشروع، أي استمرارية التواجد داخل نظام المعالجة دون إذن من صاحبه[24]، ولا يشكّل الدخول في النظام المعلوماتي تصرف محظور في حدّ ذاته وإنّما عدم الترخيص بهذا الدخول يشكّل جريمة.[25] ويعتبر الدخول في النظام المعلوماتي جريمة شكلية لا تتطلب الركن المادي لتحقق نتيجتها الإجرامية، إذ يشكل تصرّفا محظورا مجرد الدخول في كل او جزء من

النظام المعلواتي دون علم أو إذن صاحبه وهذا ما يفهم من نصّ المادة 394 مكرر من قانون العقوبات"...كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك...". وجاءت صيغة المادة بشكل عام إذ لم يشترط أن يكون النظام المعلوماتي محمي فنيا لحظر الدخول، بل يجرّم الدخول في النظام المعلوماتي حتى في حالة عدم حمايته شريطة عدم الحصول على ترخيص.

وبالتالي تعتبر جريمة الدخول الإحتيالي إلى النظام المعلوماتي إذ لا يشكّل الدخول الخطأ تصرفا يعاقب عليه القانون نظرا لحسن النيّة، ولكن يصعب إثبات نيّة الجاني في هذا النوع من الجرائم.

ويعاقب القانون جريمة الدخول إلى النظام المعلوماتي مهما كانت الوسيلة المستعملة، ونفرّق في هذا المجال بين الإتّصال المادي المباشر بالنظام المعلوماتي وبين الإتّصال المعنوي عن بعد بالنظام المعلوماتي.

ويقصد بالإتّصال المادي المباشر بالنظام المعلوماتي الدخول عليه دون الحاجة إلى وسيلة إلكترونية كشبكة الأنترنت، إذ يكون الجاني في نفس مكان تواجد النظام المعلوماتي ويقوم بعمليات مادية كالتلاعب بمعطيات النظام وتعديلها أو نقلها إلى قرص مضغوط مثلا من أجل استخدامها لأغراض شخصية، كالجرائم التي يقوم بها موظفو الشركات الكبرى أو البنوك، أو تلك التي يقوم بها الشخص المكلّف بصيانة الجهاز.

أمّا الإتصال المعنوي عن بعد بالنظام المعلوماتي فيقصد به الدخول إلى النظام المعلوماتي عن بعد من خلال استعمال شبكة الانترنت، إذ يمكن للجاني في هذه الحالة إرتكاب الجريمة وهو في مكانه دون الحاجة إلى التنقّل إلى المكان المعني.

وفي كلتا الحالتين يجب توافر العنصر المعنوي للجريمة أي يجب أن يقوم الجاني بالدخول إلى النظام المعلوماتي بإرادته وليس عن طريق الصدفة أو الخطأ، فلا يعاقب القانون الدخول غير المقصود إلى النظام المعلوماتي.[26]

كما تتجلى الجريمة المعلوماتية من خلال البقاء في النظام المعلوماتي أي الاستمرار في التواجد فيه دون ترخيص من صاحبه، إذ يكمن الركن المادي لهذه الجريمة في البقاء في المنظومة دون إذن صاحبها. وقد يحدث ان يدخل شخص في نظام معلوماتي بالخطأ دون قصد الإضرار بصاحبه فيجيب عليه في هذه الحالة الخروج فورا من النظام وعدم البقاء فيه.

يعتبر البقاء الإحتيالي في النظام المعلوماتي المرحلة الموالية للدخول فيه، وقد يكون هذا البقاء ناتجا عن دخول مشروع أي عن طريق الخطأ أو الصدفة، كما قد يكون ناتجا عن دخول احتيالي بهدف الإضرار بالنظام المعلوماتي. ويعرّف البعض[27] البقاء الإحتيالي في النظام

المعلوماتي بأنّه اتّصال غير عادي بالنظام المعلوماتي عن طريق الشبكة المعلوماتية والنظر في المعطيات التي يتضمّنها هذا النظام دون علم صاحبها.

المطلب الثاني: العقوبات الرّدعية للجرائم الإلكترونية

بالرجوع إلى المواد 394 مكرر إلى 394 مكرر 7 من قانون العقوبات نجد أنّ المشرّع الجزائري يوقّع عقوبات على الأشخاص الذين يعتدون على الأنظمة المعلوماتية للغير من خلال الدخول والبقاء فيها بشكل غير مشروع بهدف تعطيلها أو تعديل بياناتها أو مسحها أو إفشاء أسرار الغير. فقد تتجلى الجريمة من خلال حذف معطيات معلوماتية بشكل احتيالي بغض النظر عن طبيعة أو قيمة هذه المعطيات، كما قد تتجلّى الجريمة من خلال تعديل المعطيات المعلوماتية وتغييرها عن الحالة التي كانت عليها في الأصل، بغض النظر عن الطريقة التي تم بها تعديل هذه المعطيات.

كما قد يتجلى السلوك المحظور من خلال إدخال معطيات معلوماتية على النظام دون علم صاحبه كإدخال فيروسات[28] أو بيانات إضافية أو برامج، ويعاقب القانون كذلك على جريمة تصميم معطيات معلوماتية مقرصنة كإعداد برامج قرصنة بهدف قرصنة أنظمة معلوماتية دون علم أصحابها ثم نشرها.

وتُضاعف العقوبة في حالة المساس بالنظام المعلوماتي الخاص بالدفاع الوطني أو المؤسّسات الخاضعة للقانون العام، غير أنّ هذه العقوبات تفتقد للطابع الرّدعي نظرا لعدم تناسبها مع الضرر المادي والمعنوي الذي قد يلحق بالضحيّة بسبب الجريمة المعلوماتية. ونفرّق في هذا السياق بين العقوبات الأصلية والعقوبات التكميلية.

الفرع الأوّل: العقوبات الأصلية

ينصّ المشرّع الجزائري في المادة 394 مكرر من قانون العقوبات على عقوبة الحبس من ثلاثة أشهر إلى سنة، وبغرامة مالية من 50.000 دج إلى 200.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك. ونشير إلى أنّه تضاعف هذه العقوبة في حالة حذف أو تغيير معطيات المنظومة أو في حالة تخريب نظام اشتغال المنظومة وهذا ما نصت عليه صراحة نفس المادة في فقرتيها الثانية والأخيرة.

بينما يعاقب الشخص المعنوي بغرامة تعادل خمس مرات الحد الأقصى للغرامة المقرّرة للشخص الطبيعي، وهذا ما نصّت عليه صراحة المادة 394 مكرر 4 من قانون العقوبات.

كما جاء القانون 18-07 سالف الذكر بعقوبة الحبس من سنتين إلى خمس سنوات وبغرامة من 200.000 إلى 500.000 دج كل شخص يخالف أحكام المادة الثانية من هذا

القانون[29]. أما بالنسبة للشخص المعنوي الذي يرتكب الجرائم المنصوص عليها في هذا القانون فتطبّق عليه أحكام قانون العقوبات[30].

الفرع الثاني: العقوبات التكميلية

بالإضافة إلى العقوبات الأصلية المقرّرة على مرتكبي الجريمة المعلوماتية، ينصّ المشرّع على عقوبات تكميلية للتشديد من ردع هذه الجرائم. وتتمثل هذه العقوبات في مصادرة الأجهزة والبرامج والوسائل المستخدمة، مع إغلاق المواقع محل الجريمة وكذلك إغلاق محل أو مكان الإستغلال في حالة ارتكاب الجريمة بعلم المالك وهذا ما أقرّته صراحة المادة 394 مكرر 6 من قانون العقوبات، كغلق مقهى إلكتروني ارتكبت فيه الجريمة المعلوماتية بعلم مالكه.

كما نصّت المادة 18 مكرر من قانون العقوبات على عقوبات تكميلية للشخص المعنوي تتمثّل في الآتي:

- حل الشخص المعنوي
- غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز خمس سنوات
- الإقصاء من الصفقات العمومية لمة لا تتجاوز خمس سنوات
- المنع من مزاولة نشاط أو عدة أنشطة مهنية أو اجتماعية بشكل مباشر أو غير مباشر نهائيا، أو مؤقتا لمدة لا تتجاوز خمس سنوات
- مصادرة الشيء الذي استعمل في ارتكاب الجريمة أو نتج عنها
- نشر وتعليق حكم الإدانة
- الوضع تحت الحراسة القضائية لمدة لا تتجاوز خمس سنوات، وتنصب الحراسة على ممارسة النشاط الذي أدى إلى الجريمة أو الذي ارتكبت الجريمة بمناسبته.

ونشير إلى أنّ المشرّع الجزائري قد جاء ببعض التدابير الوقائية التي تتخذ مسبقا من طرف المصالح المعنية لتفادي أو الكشف عن الجرائم الالكترونية وذلك بموجب القانون رقم 09-04 السالف الذكر والمتضمن للقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، إذ تنص المادة الثالثة منه على أنّه: "مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والإتّصالات، يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الإتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية".

وتعدّ مراقبة الإتصالات الإلكترونية إجراء مهمّا، ولقدّ حدّدت المادة الرابعة من القانون رقم 09-04 الحالات التي يسمح فيها باللجوء إلى المراقبة الإلكترونية وتتمثّل في:

"- الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة،
- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدّد النظام العام أو الدفاع الوطني أو مؤسسات الدولة او الإقتصاد الوطني،
- لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية،
- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة...".

غير أنّه لا يجوز القيام بإجراء المراقبة الإلكترونية إلا بإذن مكتوب من السلطة القضائية المختصة.

ولقد أجازت المادة الخامسة من نفس القانون للسلطات القضائية المختصة وضباط الشرطة القضائية بالدخول إلى المنظومة المعلوماتية في الحالات المذكورة آنفا بهدف التفتيش، بينما أجازت المادّة السادسة بحجز المعطيات التي تراها السلطة التي تباشر التفتيش مفيدة للكشف عن الجريمة أو مرتكبها.

كذلك تم إقحام مزوّدي خدمات الإتّصالات الإلكترونية في مسار الوقاية من الجرائم الالكترونية وذلك من خلال فرض عليهم بعض الالتزامات كالإلتزام بالتعاون مع مصالح الأمن والإلتزام بحفظ المعطيات، والإلتزام بالسحب الفوري للمحتويات التي يمكن الاطلاع عليها من قبل الغير، والإلتزام بوضع ترتيبات تقنية للحد من إمكانية الدخول إلى الموزعات التي تتضمن معلومات متنافية مع النظام العام والآداب العامة.[31]

وحسن ما فعل المشرّع الجزائري عندما ألزم مزودو الخدمات الإلكترونية بمساهمتها في الوقاية من الجرائم المعلوماتية باعتبارهم حلقة بين الجاني والجريمة، فقد يتعمّد الجاني اللجوء إلى استخدام حاسوب في مركز الخدمات المعلواتية بدلا من حاسوبه الشخصي لارتكاب الجريمة لتظليل الهيئات القضائية، لذلك يسمح هذا الإجراء بتسهيل عملية الوصول إلى هوية الجاني.

خاتمة:

تعرّفنا من خلال هذه الدراسة على ظاهرة إجرامية حديثة متفشيّة في مختلف دول العالم، ولاحظنا تعدّد تسميات هذه الجريمة لكن هدفها واحد وهو القيام بفعل غير مشروع عبر الحاسوب وشبكة الانترنت.

ولقد كرّس المشرّع الجزائري آليات في مختلف القوانين لمكافحة الجريمة السيبرانية، كما وقّع عقوبات ضد مرتكبي هذه الجريمة غير أنها تبقى عقوبات لا تصل إلى درجة الردع مقارنة بخطورة هذه الجرائم وانتشارها السريع إذ تشير الاحصائيات إلى تسجيل 4600 جريمة

سيبرانية خلال سنة 2022 بعدما كان يصل عددها إلى 2838 خلال سنة 2021، شملت اختراق مواقع مؤسسات وشركات عمومية وخاصة وكذا الجرائم المالية والاقتصادية، خاصة العابرة للحدود وتلك المستحدثة، إلى جانب الابتزاز، التهديد والتشهير، المساس بالحريات الشخصية والحياة الخاصة عبر شبكات التواصل الاجتماعي، إلى جانب نشر المعلومات الزائفة والمضللة، القرصنة والتحرش الإلكتروني[32].

وعليه نقترح التوصيات التالية:

- يجب على الدول اتخاذ التدابير الصارمة لمواجهة هذه الجرائم وذلك من خلال توقيع عقوبات ردعية ضد مرتكبيها، إذ لا تتناسب العقوبات الموقّعة على المجرمين الإلكترونيّين مع خطورة هذه الجريمة التي تتعلّق بأسرار الشخص.

- كما يتوجب القيام باتفاقيات دولية متعدّدة حول كيفيات مكافحة الجريمة الالكترونية باعتبارها جريمة عابرة للحدود، إذ يلعب التعاون الدولي دورا فعالا في مكافحة هذه الجرائم.

- إضافة إلى ضرورة الإعتماد على الوسائل التقنية الحديثة في إجراءات التحقيق والتحرّي من خلال تدريب رجال الضبطية القضائية على كيفية التعامل مع هذا النوع من الجرائم، وتكوين فِرق متخصصة في التحقيق الإلكتروني.

- كما يستحسن توعية الأفراد بخطورة الجريمة الإلكترونية، وحثّهم على تجنب تخزين صورهم الشخصية عبر مواقع التواصل الإجتماعي وأجهزة الحاسوب أو الأجهزة واللوحات الذكيّة، وعدم تنزيل أي برنامج من مصدر غير معروف.

الهوامش:

[1] – المؤرخ في 10 نوفمبر 2004، ج. ر. الصادرة في 10 نوفمبر 2004، ع. 71.

[2]- *Guillaume CHAMPY, Essai de définition de la fraude informatique, Dalloz, France, 1988, p.24.*

[3]- *Klaus TIEDEMANN, Fraude et autres délits d'affaires commis à l'aide d'ordinateurs électroniques, Dalloz, France, 1993, p.61.*

[4] – أمير فرج يوسف، الجرائم المعلوماتية على شبكة الانترنت، دار المطبوعات الجامعية، الاسكندرية، مصر، 2009، ص. 106.

[5] – زبيخة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، الجزائر، 2011، ص. 42.

[6] – المؤرخ في 05 غشت 2009، ج. ر. الصادرة في 16 غشت 2009، ع. 47.

[7]- *Alain HOLLANDE, Xavier LINANT, Pratique du droit de l'informatique, éd. Delmas, France, 2002, p. 250.*

[8]- *André LUCAS, Jean DEVREZE, Jean FRAYSSINET, Droit de l'informatique et de l'internet, Dalloz, France, 2001, p. 690.*

[9] – باطلي غنية، الجريمة الالكترونية "دراسة مقارنة"، الدار الجزائرية للنشر والتوزيع، الجزائر، 2015، ص. 15.

[10]- *André LUCAS, Jean DEVREZE, Jean FRAYSSINET, op.cit., p. 680.*

[11] – م. نشناش مداخلة حول الركن المفترض في الجريمة المعلوماتية، كلية الحقوق والعلوم السياسية، جامعة بسكرة، الجزائر، 2015-2016، ص.05

[12] – ع. بن يونس، الجرائم الناشئة عن استخدام الانترنيت، دار النهضة العربية، القاهرة، مصر، 2004، ص. 21.

[13] – المؤرخ في 10 يونيو 2018، ج. ر. الصادرة في 10 يونيو 2018، ع. 34.

[14] – أنظر المادة 49 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[15] – المؤرخ في 01 فبراير 2015، ج. ر. الصادرة في 10 فبراير 2015، ع. 06.

[16] – العزيز سمير حامد، التعاقد عبر تقنيات الاتصال الحديثة (دراسة مقارنة)، دار النهضة العربية، 2001، ص. 62.

[17] – انظر المادة 44 من القانون رقم 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين.

[18] – المؤرخ في 10 مايو 2018، ج. ر. الصادرة في 16 مايو 2018، ع. 28.

[19] – أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، القاهرة، مصر، 2006، ص. 14.

[20] – أحمد خليفة الملط، نفس المرجع، ص. 44.

[21]- *André LUCAS, Jean DEVREZE, Jean FRAYSSINET, op.cit., p. 689.*

[22]- *André LUCAS, Jean DEVREZE, Jean FRAYSSINET, op.cit., p. 690.*

[23]- *Alain HOLLANDE, Xavier LINANT, op. cit., p. 250*

[24] – جمال براهيمي، مكافحة الجرائم الإلكترونية في التشريع الجزائري، المجلة النقدية للقانون والعلوم السياسية، جامعة مولود معمري تيزي وزو، الجزائر، المجلد 11، العدد 02، ص.128.

[25] – أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2007، ص. 102.

[26]- *Bensoussan ALAIN, Internet: aspect juridique, éd. Hermès, France, 1996, P. 110.*

[27]- *Bensoussan ALAIN, op. cit., p. 113.*

[28] – تعتبر الفيروسات المعلوماتية تعليمات طفيلية خبيثة تختفي بسهولة في النظام المعلوماتي، تظهر في شكل برامج صغيرة تنتشر في الجهاز وتؤثر سلبا على النظام المعلوماتي للجهاز، ولها قدرة فائقة على المكونات المعنوية للجهاز والشبكات المعلوماتية وهذا ما يسهّل انتشاره وتنفيذ أهدافه. أنظر: محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، مصر، 1993، ص. 189.

[29] – المادة 54 من القانون 18-07 السابق ذكره.

[30] – المادة 70 من القانون 18-07 السابق ذكره.

[31] – أنظر الفصل الرابع من القانون رقم 09-04 المتعلّق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتّصال ومكافحتها.

[32] – باشوش نوارة، الجريمة السيبرانية: أسلحة الجناة الجديدة لضرب الأشخاص والاقتصاد، مقال منشور في 15 فيفري 2023، تاريخ الاطلاع: 2023/03/10 على الساعة 15.30. *https://www.echoroukonline.com*