مجلة الدراسات القانونية (صنف ج) - Journal OF LEGAL STUDIES (Class C)
مجلة علمية دولية سداسية محكمة صادرة عن مخبر السيادة والعولمة – جامعة يحيى فارس بالمدية (الجزائر)
ISSN 2437-0304
EISSN: 2602-5108
رقم الإيداع القانوني: 3039 -2015

المجلد: 09 العدد: 02 السنة: جوان 2023 م- ذو القعدة 1444 هـ ص: 178 - 198

الجرائم المعلوماتية في إطار التجارة الإلكترونية وسبل مكافحتها

Information crimes in the context of electronic commerce and ways to combat them.

موزالي نور الدين *
أستاذ محاضر ب
كلية الحقوق والعلوم السياسية
جامعة الجيلالي بونعامة، خميس مليانة (الجزائر)
n.mouzali@univ-dbkm.dz

تاريخ إرسال المقال: 2023-01-30 **تاريخ قبول المقال:** 2023-05-28 **تاريخ نشر المقال:**2023-06-10

الملخص: شكلت ظاهرة الجريمة المعلوماتية أبرز التحديات التي تواجهها الأنشطة التجارية، بوجه عام، والتجارة الإلكترونية، بوجه خاص، وهذا لحداثة هذا النوع من الأنشطة وتطور المعلومات التكنولوجية التي سهلت عملية الاعتداء عليها رغم تكريس وسائل متعددة لمحاربتها والتقليل من خطورتها على الدول والأفراد والمؤسسات المتضررة منها.

في هذا الإطار، ومن أجل حماية المتعامل الإلكتروني، وحماية المواقع والنظم المعلوماتية، عملت المنظمات التي تهتم بمحاربة هذه الظاهرة على إيجاد آليات قانونية وتقنية للتصدي لهذه الجرائم وسن قوانين تتعلق بالتجارة الإلكترونية، كما بذلت دول العالم جهود معتبرة وجسدتها في الميدان من خلال وضع تشريعات داخلية تدعم المعاملات في إطار التجارة الإلكترونية والتقليل من مخاطرها على المتعاملين فيها.

الكلمات المفتاحية: الجريمة، المعلوماتية، المعاملات، التجارية، التجارة، الإلكترونية، الآليات، القانونية.

Abstract: The phenomenon of cybercrime is considered one of the most significant challenge facing business activities in general and electronic commerce in particular. This is due to the modernization of this type of activity, and the development of technological information that has facilitated the process of assault, despite the fact that multiple means have been devoted to combating it, and reducing its risk to the affected States, individuals and institutions.

In this framework, and in order to protect the electronic user and protect the websites and information systems through which these transactions are made legal and technical mechanisms to combat these crimes and to enact laws on electronic commerce. The world countries have also made significant efforts in the field through the development of domestic legislation that supports e-commerce transactions and reduces their risks to their clients.

KEY WORDS: INFORMATION, CRIME, COMMERCIAL, TRANSACTIONS, ELECTRONIC, TRADE, LEGAL, MECHANISMS.

***المؤلف المرسل**

مجلة الدراسات القانونية (صنف ج) - Journal OF LEGAL STUDIES (Class C)
مجلة علمية دولية سداسية محكمة صادرة عن مخبر السيادة والعولمة – جامعة يحيى فارس بالمدية (الجزائر)
ISSN 2437-0304
EISSN: 2602-5108
رقم الإيداع القانوني: 3039 -2015
المجلد: 09 العدد: 02 السنة: جوان 2023 م- ذو القعدة 1444 هـ ص: 178 - 198

المقدمة:

يشهد العالم في الوقت الحالي عدة تطورات في مجال تقنية المعلومات وتكنولوجيا الاتصالات، وهذه التطورات أثرت بدورها على مختلف القطاعات والمجالات من بينها قطاع التجارة، حيث أصبح اليوم بالإمكان الاعتماد على هذه التقنيات الحديثة في المبادلات التجارية، التي يطلق على تسميتها بالمعاملات التجارية الإلكترونية.

على الرغم من المزايا التي حققتها هذه الوسائط الإلكترونية في تطوير المبادلات التجارية وتعزيز ودعم قطاع التجارة برمته، إلا أنها سهلت في، نفس الوقت، عملية الاعتداء على هذه المعاملات، نظرا لكونها تتم عبر وسائل لا تعترف بالحدود الجغرافية، فهي عبارة عن وسائل مفتوحة للجميع وتسمح بالولوج إليها في أي وقت ومن أي مكان في العالم.

يكون الاعتداء على المعاملات التجارية الإلكترونية عن طريق الاعتداء على البيانات والمعلومات المتعلقة بالعملية التعاقدية أو بالأشخاص المتعاقدين، وقد أطلق على هذه الاعتداءات بما يعرف بالجريمة الإلكترونية أو الجريمة المعلوماتية.

تتطور الجريمة الإلكترونية بتطور التقنيات الحديثة، فكلما تطورت الوسائط الإلكترونية المعتمد عليها في المبادلات التجارية تتطور معها طرق ووسائل الاعتداء عليها، لذلك ظهرت الحاجة الملحة لوضع آليات لمكافحتها والحد منها، فإلى جانب الآليات التقنية المستحدثة لحماية التجارة الإلكترونية من الاعتداءات التي تعرقلها، وجدت آليات قانونية، منها ما هي وقائية، ومنها ما هي ردعية، والهدف من وراء إقرارها، هو الحد من الاعتداءات وتقرير الحماية اللازمة للمعاملات التجارية الإلكترونية، بصفة خاصة، والتجارة الإلكترونية، بصفة عامة.

تكمن أهمية البحث في موضوع الجرائم المعلوماتية في إطار التجارة الإلكترونية وسبل مكافحتها، كون الجرائم المعلوماتية من أكبر التحديات التي تعرفها اليوم المبادلات والمعاملات في مجال التجارة الإلكترونية، التي تتم عبر وسائل التكنولوجيا الحديثة والشبكة الدولية للاتصالات، خاصة مع التطور المسجل في مجال التقنيات والتكنولوجيا، وظهور برامج معلوماتية متطورة تسمح باختراق أي نظام معلوماتي أو قاعدة بيانات خاصة بالمؤسسات والشركات التجارية.

مجلة الدراسات القانونية (صنف ج) - Journal OF LEGAL STUDIES (Class C)
مجلة علمية دولية سداسية محكمة صادرة عن مخبر السيادة والعولمة – جامعة يحيى فارس بالمدية (الجزائر)
ISSN 2437-0304
EISSN: 2602-5108
رقم الإيداع القانوني: 3039 -2015
المجلد: 09 العدد: 02 السنة: جوان 2023 م- ذو القعدة 1444 هـ ص: 178 - 198

تستوجب دراسة هذا الموضوع، اعتماد كل من المنهج الوصفي بهدف تحديد مفهوم الجرائم المعلوماتية المتعلقة بالمعاملات التجارية الإلكترونية والمنهج التحليلي بهدف تحليل ونقد النصوص القانونية المتعلقة بهذا البحث، لأن هذه الدراسة هي عبارة عن مقاربة قانونية بالدرجة الأولى، كما يمكن الاستعانة أحيانا بالمنهج المقارن للمقارنة بين الأحكام والقواعد القانونية التي أصدرتها بعض الدول في سبيل مكافحة الجرائم الإلكترونية للتعرف عليها، من جهة، والاستفادة من تجربتها في هذا المجال، من جهة أخرى.

وعلى ضوء ما سبق، يمكن طرح الإشكالية التالية:

- ما هي الجرائم المعلوماتية المتعلقة بالمعاملات التجارية الإلكترونية؟ وما مدى تفعيل الآليات القانونية والتقنية في مكافحتها؟

للإجابة على هذه الإشكالية تم تقسيم البحث إلى محورين:

المبحث الأول: الجرائم المعلوماتية في إطار التجارة الإلكترونية

المبحث الثاني: دور التشريعات في محاربة الجرائم الإلكترونية

المبحث الأول: الجرائم المعلوماتية في إطار التجارة الإلكترونية

من أهم مزايا التجارة الإلكترونية هو توفير الوقت والتقليل من مشقة الانتقال، وحتى وإن كان المستهلك الجزائري لا يقبل بصفة مستمرة التعامل عبر الوسائط الإلكترونية لكي يقتني حاجياته، إلا أنه وفي بعض الحالات يفضل أن يبتاع حاجياته اليومية من خلال الدعائم التكنولوجية، وهذا ما هو معمول به في المحلات التجارية الكبرى، بصفة خاصة، أين يتم التعامل مع الزبائن بواسطة الدعائم الإلكترونية المتاحة.

يحتاج المتعامل عبر الوسائط الإلكترونية إلى حماية من الناحية التقنية وحماية قانونية حتى يضمن تعاملاته وعلاقاته مع المتعاقد معه ومع الغير، ومن أجل حماية المستهلك الإلكتروني وحماية تعاملاته الإلكترونية، يجب في، نفس الوقت، حماية المواقع والنظم المعلوماتية التي يتم من خلالها إجراء هذه المعاملات[1].

[1]- ناصر حمودي، الحماية الجنائية الموضوعية والإجرائية الخاصة المقررة للمستهلك الإلكتروني في التشريع الجزائري، مداخلة ضمن الملتقى الوطني الثالث حول المستهلك والاقتصاد الرقمي: ضرورة الانتقال وتحديات الحماية، 23-24 أفريل 2018، المركز الجامعي عبد الحفيظ بوالصوف، ميلة، ص 8؛ المداخلة منشورة في الموقع الإلكتروني التالي: http://dspace.centre-univ-mila.dz/jspui/handle.

مجلة الدراسات القانونية (صنف ج) - Journal OF LEGAL STUDIES (Class C)
مجلة علمية دولية سداسية محكمة صادرة عن مخبر السيادة والعولمة – جامعة يحيى فارس بالمدية (الجزائر)
ISSN 2437-0304
EISSN: 2602-5108
رقم الإيداع القانوني: 3039 -2015
المجلد: 09 العدد: 02 السنة: جوان 2023 م- ذو القعدة 1444 هـ ص: 178 - 198

تقتضي دراسة هذا المبحث، تحديد مفهوم الجريمة المعلوماتية في مجال التجارة الإلكترونية (المطلب الأول)، ثم تطبيقات الجريمة المعلوماتية في نطاق التجارة الإلكترونية (المطلب الثاني).

المطلب الأول: مفهوم الجريمة المعلوماتية في مجال التجارة الإلكترونية

تعتبر الجريمة الالكترونية من أخطر الجرائم غير التقليدية المرتكبة من طرف الإنسان في عالمنا المعاصر، وهي ظاهرة بدأت تنمو تدريجيا بنمو وتطور عصابات الجريمة المنظمة وجرائم المعلوماتية والانترنيت.

في البداية، يجب إعطاء تعريف لكل من التجارة الإلكترونية والجريمة المعلوماتية (الفرع الأول)، ثم السياق العام لظهور وتطور الجريمة الإلكترونية (الفرع الثاني).

الفرع الأول: تعريف كل من التجارة الإلكترونية والجريمة المعلوماتية

توجد العديد من التعاريف المتعلقة بهذين المصطلحين، باعتبارهما من المفاهيم الحديثة المترتبة عن الثورة المعلوماتية ووسائل الاتصال الحديثة وما نتج عنها من تغيرات التي مست مختلف المجالات، بما فيها مجال المعاملات التجارية.

أولا: تعريف التجارة الإلكترونية

عرفتها منظمة التعاون الاقتصادي والتنمية OCDE لسنة 2009، بأنها بيع أو شراء السلع أو الخدمات التي تقوم بها المؤسسات أو الأفراد، ويتم ذلك عن طريق الشبكة الإلكترونية[2].

كما عرفتها منظمة التجارة العالمية OMC في إطار الإعلان العالمي للتجارة الإلكترونية لسنة 1998، بأن مصطلح التجارة الإلكترونية يقصد به إنتاج أو توزيع أو تسويق أو بيع المنتجات (السلع والخدمات) عن طريق الوسائط الإلكترونية[3].

[2]- راجع موقع منظمة التعاون الاقتصادي والتنمية حسب تعريفها لسنة 2009 التالي: https://www.ocde.org

[3]- راجع الإعلان العالمي للتجارة الإلكترونية لسنة 1998 المنشور في موقع منظمة التجارة العالمية:www.wto.org

مجلة الدراسات القانونية (صنف ج) - Journal OF LEGAL STUDIES (Class C)
مجلة علمية دولية سداسية محكمة صادرة عن مخبر السيادة والعولمة – جامعة يحيى فارس بالمدية (الجزائر)
ISSN 2437-0304
EISSN: 2602-5108
رقم الإيداع القانوني: 3039 -2015
المجلد: 09 العدد: 02 السنة: جوان 2023 م- ذو القعدة 1444 هـ ص: 178 - 198

من جهته، عرف المشرع الجزائري التجارة الإلكترونية في المادة 6 الفقرة 1 من القانون رقم 18-05، المتعلق بالتجارة الإلكترونية[4] كما يلي: " يقصد في مفهوم هذا القانون بما يأتي: التجارة الإلكترونية: النشاط الذي يقوم بموجبه مورد إلكتروني باقتراح أو ضمان توفير سلع وخدمات عن بعد لمستهلك إلكتروني، عن الاتصالات الإلكترونية.

من خلال هذه التعاريف، يتبين بأن التجارة الإلكترونية تشمل عمليات بيع وتسويق وحتى ترويج منتجات من سلع وخدمات بالاعتماد على دعائم ووسائط الكترونية.

ثانيا: تعريف الجريمة المعلوماتية

على المستوى القانوني، لم يقدم المشرع الجزائري أي تعريف للجريمة المعلوماتية، حيث فضل السكوت وترك هذا المجال للفقه والمختصين. سواء في قانون العقوبات أو في القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004[5]، يعدل ويتمم الأمر رقم 66-156 المؤرخ في 8 جوان 1966 والمتضمن قانون العقوبات، وكذا القانون رقم 09-04 المؤرخ في 05 أوت 2009[6]، يتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الذي اكتفى في المادة الثانية (2) منه بشرح وتحديد بعض المصطلحات الواردة في هذا النص.

يستخلص مما سبق، بأن الجريمة المعلوماتية أو الإلكترونية هي عبارة عن تلك الجرائم الناتجة عن استخدام المعلوماتية والتقنية الحديثة، المتمثلة في الكمبيوتر والانترنيت في أعمال غير مشروعة، عادة ما ترتكب بهدف تحقيق عوائد مالية ضخمة جراء أعمال غير شرعية يعاد ضخها في الاقتصاد الدولي عبر شبكة الانترنيت.

[4]- القانون رقم 18-05 المؤرخ في 10 ماي سنة 2018، الجريدة الرسمية عدد 28 الصادرة بتاريخ 16 ماي 2018، ص 4.

[5]- القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، المعدل والمتمم، للأمر رقم 66-156 المؤرخ في 8 جوان 1966 المتضمن قانون العقوبات، الجريدة الرسمية عدد 71 بتاريخ 10 نوفمبر 2004، ص8.

[6]- القانون رقم 09-04 المؤرخ في 5 أوت 2009، المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية عدد 47 بتاريخ 16 أوت 2009، ص5.

مجلة الدراسات القانونية (صنف ج) - Journal OF LEGAL STUDIES (Class C)
مجلة علمية دولية سداسية محكمة صادرة عن مخبر السيادة والعولمة – جامعة يحيى فارس بالمدية (الجزائر)
ISSN 2437-0304
EISSN: 2602-5108
رقم الإيداع القانوني: 3039 -2015
المجلد: 09 العدد: 02 السنة: جوان 2023 م- ذو القعدة 1444 هـ ص: 178 - 198

من بين أهم الجرائم الواقعة على التجارة الإلكترونية، توجد جريمة اختراق مواقع التجارة الإلكترونية، جريمة الاتجار بمعطيات غير مشروعة، قرصنة البيانات والمعلومات من خلال اعتراض البيانات وسرقتها بغرض الاستفادة منها، لاسيما سرقة أرقام البطاقة الائتمانية وأرقام الحسابات وكلمات الدخول وكلمات السر، والاحتيال المالي بالبطاقات من خلال الاستعمال غير القانوني لبطاقات التسوق، وجرائم الاعتداء على الأموال، مثل المؤسسات المصرفية والمالية والبنوك ومواقع التجارة الإلكترونية.

الفرع الثاني: السياق العام لظهور وتطور الجريمة الإلكترونية

ظهرت الجريمة الالكترونية وتزايدت، شيئا فشيئا، في ظل الانفتاح العالمي وارتباط الأسواق الدولية بعضها ببعض، فهي تعبر عن نشاط تعاوني بشكل إجرامي تتلاقى من خلالها أيادي خبراء المال والبنوك مع جهود الاقتصاديين والمجرمين وبعض القانونيين لتتجاوز عملياتها ونطاقها الحدود الإقليمية للدول، لتضفي على الجريمة في نهاية الأمر سمة العالمية، وصفة العولمة على تبعاتها، وتجعلها جريمة منظمة بمعنى الكلمة.

تعتمد التجارة كما هو متعارف عليه على مبدأ الثقة والأمان في المعاملات، ونتيجة إرساء هذا المبدأ في المعاملات التجارية، فإنه يستوجب في المقابل تحقيق الحماية اللازمة التي تضمن مصلحة المتعاقدين في المعاملات الإلكترونية مثلها في المعاملات التقليدية، ولا يكون ذلك إلا بضمان عدم حدوث أي اعتداء على الأشخاص المتعاقدة والعملية التعاقدية بحد ذاتها في إطار هذا النوع من المعاملات.

والجرائم الإلكترونية لا تمس مصلحة البائع والمشتري فقط أو المنتج والمورد والمستهلك، بل تتعدى ذلك، بحيث أصبحت أضرارها تخرج من نطاق المصالح الخاصة أو الشخصية وتمتد إلى المصلحة العامة، مثل التزوير المعلوماتي للمحررات والتوقيعات الإلكترونية[7]، وجريمة الدخول غير المشروع لنظم المعالجة الآلية للمعطيات، وهي جريمة أسفرت عنها التطورات التكنولوجية الحديثة[8]، وغيرها من الجرائم المعلوماتية الأخرى.

[7]- عبد الفتاح بيومي حجازي، الحكومة الإلكترونية بين الواقع والطموح، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، مصر، 2008، ص 516.

[8]- ناصر حمودي، المرجع السابق، ص 9.

مجلة الدراسات القانونية (صنف ج) - Journal OF LEGAL STUDIES (Class C)
مجلة علمية دولية سداسية محكمة صادرة عن مخبر السيادة والعولمة – جامعة يحيى فارس بالمدية (الجزائر)
ISSN 2437-0304
EISSN: 2602-5108
رقم الإيداع القانوني: 3039 -2015
المجلد: 09 العدد: 02 السنة: جوان 2023 م- ذو القعدة 1444 هـ ص: 178 - 198

لقد أطلق على المعتدي في الجرائم الإلكترونية في الاصطلاح القانوني "بالمجرم المعلوماتي"، أما في الاصطلاح الإلكتروني، فقد أطلق عليه خبراء أمن المعلوماتية باسم "هاكر hacker"[9]، وهو مصطلح مقتبس من اللغة الإنجليزية، ومعناه باللغة العربية القرصان وجمعه القراصنة.

كما أصبحت الأعمال التي تصدر عن هذا الأخير، من خلال الاعتداءات على المعلومات التي ترتكز عليها المعاملة التجارية، والاعتداء على الأنظمة المعلوماتية وقواعد البيانات، من أهم الإشكالات التي تواجه التجارة الإلكترونية، بصفة عامة، والمعاملات التجارية، بصفة خاصة، وأكبر عائق يعرقل تطورها ونموها.

في السياق ذاته، وبسبب هذه الأعمال والمخاطر المذكورة، أصبح المتعامل في هذا المجال، لا يثق في البيئة الافتراضية باعتبارها وسط غير آمن يشكل مخاطر على المتعاقدين، من جهة، وعلى العملية التعاقدية بحد ذاتها، من جهة أخرى، لاسيما أن الجريمة المعلوماتية تتطور بسرعة نتيجة ما تقدمه الوسائل التكنولوجية من تسهيلات كبرى للأنشطة الإجرامية، على عكس القوانين والتشريعات، التي تتميز بالبطء نسبيا وتتأخر عن مواكبة التغيرات التي تطرأ في مجال التقنيات والتكنولوجيا الحديثة[10]، كما أصبح العدد الهائل من البيانات التي يجري تداولها في الأنظمة المعلوماتية من بين أحد أهم الصعوبات التي تعيق التحقيق في الجرائم المعلوماتية[11].

المطلب الثاني: تطبيقات الجريمة المعلوماتية في نطاق التجارة الإلكترونية

تتعدد تطبيقات الجريمة الإلكترونية في نطاق التجارة الإلكترونية، والمهم في هذا الصدد هي الاعتداءات الواقعة على المعاملات التجارية الإلكترونية، مثل الاعتداء على نظام معلوماتي معين، كاستحداث برامج للحاسب الآلي بهدف تقليد التوقيعات الرقمية، الاعتداء على البيانات الشخصية المتعلقة بالمتعاقدين في إطار عقود التجارة

[9]- عائشة بوخبزة، الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري، مذكرة ماجستير في القانون الجنائي، كلية الحقوق، جامعة وهران، 2012-2013، ص 25.

[10]- كمال حطاب، الحماية الجزائية للتجارة الإلكترونية، أطروحة دكتوراه في العلوم، كلية الحقوق والعلوم السياسية، جامعة جيلالي اليابس، سيدي بلعباس، 2015-2016، ص 174.

[11]- عائشة بوخبزة، المرجع السابق، ص 36.

مجلة الدراسات القانونية (صنف ج) - Journal OF LEGAL STUDIES (Class C)
مجلة علمية دولية سداسية محكمة صادرة عن مخبر السيادة والعولمة – جامعة يحيى فارس بالمدية (الجزائر)
ISSN 2437-0304
EISSN: 2602-5108
رقم الإيداع القانوني: 3039 -2015
المجلد: 09 العدد: 02 السنة: جوان 2023 م- ذو القعدة 1444 هـ ص: 178 - 198

الإلكترونية، فإحاطة البيانات الشخصية بسرية هو أمر يساعد على نمو وازدهار التجارة الإلكترونية، سواء تعلق الأمر بالبائع أو بالمستهلك[12].

على العموم، تتمثل أهم الجرائم الإلكترونية وأخطرها في إطار المعاملات التجارية الإلكترونية في اختراق مواقع التجارة الإلكترونية (الفرع الأول)، ثم الاعتداء على البطاقات البنكية (الفرع الثاني) وفي الأخير الاعتداء على التوقيع الإلكتروني (الفرع الثالث).

الفرع الأول:اختراق مواقع التجارة الإلكترونية

يتمثل الاعتداء على مواقع التجارة الإلكترونية من خلال توقيف نظام المعالجة، أو بالحد من سرعته المطلوبة، أو من خلال الاعتداء على بيانات مواقع التجارة الإلكترونية، كإدخال بيانات جديدة ضمن هذه المواقع أو تعديلها أو محوها[13].

كما يمكن أن يكون اختراق المواقع التجارية بالاعتداء على سرية البيانات والمعلومات في البيئة الافتراضية، بحيث يتمكن القراصنة Hackers في هذه الحالة من الوصول إلى المعلومات المالية والشخصية للأشخاص والمؤسسات، أو بإتلاف المواقع الإلكترونية وتدميرها عن طريق الفيروس المعلوماتي[14]... الخ.

الفرع الثاني: الاعتداء على البطاقات البنكية

تعتبر البطاقات البنكية وسيلة من وسائل الدفع الإلكتروني التي فرضتها تطورات التقنية الحديثة، ومن جانبه عرف القانون رقم 18-05 المتعلق بالتجارة الإلكترونية المذكور أعلاه، بأنها: " كل وسيلة دفع مرخص بها طبقا للتشريع المعمول به تمكن صاحبها من القيام بالدفع عن قرب أو عن بعد، عبر منظومة إلكترونية.

---

[12]- عبد الفتاح بيومي حجازي، المرجع السابق، ص ص 516-521.

[13]- عزوز سعيدي، التجارة الإلكترونية وتحديات الجريمة المعلوماتية، مقال منشور في مجلة الدراسات والبحوث القانونية، المجلد 04، العدد 01، كلية الحقوق والعلوم السياسية، جامعة لونيسي علي، البليدة 2، الجزائر، 2019، ص ص 218-232، ص 229؛ المقال مشور في الموقع الإلكتروني التالي: https://www.asjp.cerist.dz.

[14]- عبد الفتاح بيومي حجازي، المرجع السابق، ص 452-453.

مجلة الدراسات القانونية (صنف ج) - Journal OF LEGAL STUDIES (Class C)
مجلة علمية دولية سداسية محكمة صادرة عن مخبر السيادة والعولمة – جامعة يحيى فارس بالمدية (الجزائر)
ISSN 2437-0304
EISSN: 2602-5108
رقم الإيداع القانوني: 3039 -2015
المجلد: 09 العدد: 02 السنة: جوان 2023 م- ذو القعدة 1444 هـ ص: 178 - 198

إن البطاقات البنكية بما فيها بطاقة الائتمان ليست آمنة دائما، فحتى وإن كانت لها مزايا من خلال وظائفها المتعددة التي تحققها للعملاء وللتجارة بحد ذاتها، من حيث ربح الوقت وضمان السرعة في إبرام وتنفيذ المعاملات التجارية، إلآ أنها لا تخلو من سلبيات تهدد تطور التجارة الإلكترونية، حيث ساعد ظهور هذه البطاقات وانتشارها على شيوع الجريمة بمختلف أشكالها، وانعكس ذلك بدوره على تطور أساليب ارتكاب الجرائم المعلوماتية[15].

إن خير مثال على ما سبق، هو حصول شخص على بطاقة ائتمان استنادا على مستندات مزورة، بحيث يصبح منتحلا صفة الغير أو أن المستندات تتضمن بيانات غير صحيحة، ويصدر البنك بطاقة الائتمان بالاعتماد على تلك البيانات الغير صحيحة أو المزورة، ويقوم حامل البطاقة باستعمال هذه البطاقة في المبادلات التجارية التي يجريها مع الغير، ولا يتمكن البنك حينها من استرداد قيمتها بعد ذلك، إما بسبب أن صاحب البطاقة لا يمكن الاستدلال عنه أو أن الضمانات المقدمة من طرفه لا تكفي[16].

بوجه عام، يكون الاعتداء على البطاقات البنكية، إما من قبل حامل البطاقة (أ)، أو من قبل الغير(ب).

أ-الاعتداء على البطاقة البنكية من قبل حامل البطاقة

يكون الاعتداء على البطاقة البنكية من قبل حاملها عندما يقوم هذا الأخير في بعض الحالات باستخدام البطاقة البنكية رغم إلغاءها من قبل الجهة المصدرة لها (1)، أو باستخدامها رغم انتهاء مدة صلاحيتها(2).

1- استخدام البطاقة رغم إلغائها من طرف الجهة المصدرة لها

تكون حالة استخدام البطاقة رغم إلغائها من طرف الجهة المصدرة لها، عندما تقوم هذه الأخيرة بإلغاء البطاقة لأي سبب من الأسباب، كأن يكون الحامل قد أساء استخدامها، أو تم إلغاءها بسبب المركز المالي للحامل[17] أو تم إلغاءها لسبب آخر، ورغم ذلك يبقى حامل البطاقة يستعملها ويعتمد عليها في المبادلات التجارية التي يجريها مع الغير.

[15]- كمال حطاب، المرجع السابق، ص 174.
[16]- عبد الفتاح بيومي حجازي، المرجع السابق، ص 496.
[17]- كمال حطاب، المرجع السابق، ص 174.

مجلة الدراسات القانونية (صنف ج) - Journal OF LEGAL STUDIES (Class C)
مجلة علمية دولية سداسية محكمة صادرة عن مخبر السيادة والعولمة – جامعة يحيى فارس بالمدية (الجزائر)
ISSN 2437-0304
EISSN: 2602-5108
رقم الإيداع القانوني: 3039 -2015
المجلد: 09 العدد: 02 السنة: جوان 2023 م- ذو القعدة 1444 هـ ص: 178 - 198

2- استخدام البطاقة بعد انتهاء مدة صلاحيتها

تكون البطاقة البنكية الصادرة من قبل البنك محددة المدة بموجب علاقة تعاقدية بين البنك والعميل، وعند انتهاء هذه المدة تصبح البطاقة غير صالحة للاستعمال، وفي حالة استعملها الحامل بعد انقضاء هذه المدة، فإن ذلك يشكل تعدي على بطاقة الائتمان وهذا التعدي يعتبر بمثابة جريمة إلكترونية، لأن العقد المبرم بين البنك والعميل يستوجب على هذا الأخير إعادة البطاقة عند انتهاء مدتها إلى البنك الذي أصدرها.

3-إساءة استعمال البطاقة من قبل الغير

يقصد بالغير هنا، أي شخص غير التاجر الذي يتعامل معه حامل البطاقة، أو موظفي البنك مصدر البطاقة، ويمكن للغير أن يعتدي على بطاقة الائتمان في حالة ضياع أو سرقة البطاقة، أو ضياع أو سرقة الرقم السري الخاص بها[18]، وفي هذه الحالة يقوم الغير باستخدام البطاقة البنكية في المبادلات التجارية دون أن يكون له الحق في استعمالها، وهذا يشكل تعديا على بطاقة الائتمان وعلى أطراف العلاقة وهما، حامل البطاقة والبنك الذي أصدرها.

الفرع الثالث: الاعتداء على التوقيع الإلكتروني

بوجه عام، يعرف التوقيع الإلكتروني بأنه عبارة عن مجموعة من البيانات يتم إدراجها على شكل رسالة إلكترونية، بحيث تسمح من خلالها بالتعرف على صاحب التوقيع الإلكتروني.

في هذا الإطار، عرفه القانون النموذجي للجنة القانون التجاري الدولي التابعة لمنظمة الأمم المتحدة من خلال المادة 2 الفقرة أ، بأنه عبارة عن بيانات في شكل إلكتروني مدرجة في رسالة بيانات، أو مضافة إليها أو مرتبطة بها منطقيا، يجوز أن تستخدم لتعيين هوية الموقع بالنسبة إلى رسالة البيانات، ولبيان موافقة الموقع عل المعلومات الواردة في رسالة البيانات، وهذا التعريف تبنته مختلف التشريعات المقارنة.

على مستوى التشريع الجزائر، عرفه القانون رقم 15-04، المتعلق بالتوقيع والتصديق الإلكترونيين السابق الذكر في المادة 2 منه، بأنه عبارة عن بيانات في شكل إلكتروني، مرفقة أو مرتبطة منطقيا ببيانات إلكترونية أخرى تستعمل كوسيلة توثيق.

[18]- عبد الفتاح بيومي حجازي، المرجع السابق، ص 551.

مجلة الدراسات القانونية (صنف ج) - Journal OF LEGAL STUDIES (Class C)
مجلة علمية دولية سداسية محكمة صادرة عن مخبر السيادة والعولمة – جامعة يحيى فارس بالمدية (الجزائر)
ISSN 2437-0304
EISSN: 2602-5108
رقم الإيداع القانوني: 3039 -2015
المجلد: 09 العدد: 02 السنة: جوان 2023 م- ذو القعدة 1444 هـ ص: 178 - 198

في نفس السياق، من أجل منح المصداقية للتوقيع الإلكتروني، يجب تصديقه أو توثيقه من طرف جهة محايدة تدعى بمؤدي خدمات التصديق الإلكتروني، إذ أن عملية التصديق هذه تضفي على التوقيع الإلكتروني الحجية الكافية واللازمة حتى يمكن الاعتماد عليه كدليل إثبات، مثله في ذلك مثل التوقيع العادي أو التوقيع التقليدي المتعارف عليه، وبعث الثقة والأمان فيما بين المتعاملين أو المتعاقدين، خاصة وأن الهدف من وراء التوقيع الإلكتروني هو رفع مستوى الأمن والخصوصية بالنسبة للمتعاملين عبر شبكة الانترنيت، والحفاظ على سرية المعلومات وتحديد هوية المرسل والمستقبل في التعاقد الإلكتروني[19].

يكون الاعتداء على التوقيع الإلكتروني بعدة صور، فقد يكون الاعتداء من طرف مؤدي خدمات التصديق من خلال كشف البيانات السرية المتعلقة بالتوقيع الإلكتروني، ويمكن أن يكون الاعتداء من قبل الغير كأن يقوم هذا الأخير بتقليد التوقيع الإلكتروني، أو بالاعتداء على سرية البيانات الشخصية للموقع.

أما على مستوى حماية التوقيع الإلكتروني من الناحية التقنية، فيكون بواسطة عدة آليات تقنية أيضا، ومن أهمها عملية التشفير، وتتمثل عملية التشفير في تحويل البيانات والنصوص إلى رموز، وبالتالي تصبح هذه البيانات عبارة عن نص مشفر، ويتم التحكم في عملية التشفير من خلال مفتاح يمكن تحريكه لوضع معاكس، بحيث يسمح للرموز حل الشفرة المقابلة أن تعيد العملية باستخدام المفتاح المناسب.

أما بالنسبة للشفرات المتماثلة، فيتم استخدام نفس المفتاح لحل شفرة الرسالة كما سبق استخدامه في تشفيرها، وفي هذه الحالة، يجب أن يظل هذا المفتاح سريا غير معروف،[20]وهذا ما يحقق الحماية من الناحية التقنية للتوقيعات الإلكترونية، غير أن ذلك لا يغني عن وجود حماية قانونية لهذا النوع من التوقيعات.

المبحث الثاني: دور التشريعات في محاربة الجرائم الإلكترونية

إن حماية التجارة الإلكترونية تكون بآليات فنية حمائية، مثل التشفير، برامج الحماية، البصمة الإلكترونية ... وغيرها من التقنيات، التي يمكن من خلالها حماية

[19]- عبد الصمد حوالف، الحماية القانونية للمستهلك في عقود التجارة الإلكترونية، مقال منشور في مجلة الأكاديمية للدراسات الاجتماعية والإنسانية، المجلد 08، العدد 1، كلية الحقوق والعلوم السياسية، جامعة حسيبة بن بوعلي، الشلف، الجزائر، 2016، ص ص 124-130، ص128؛ المقال منشور في الموقع الإلكتروني التالي:https://www.asjp.cerist.dz .

[20]- عبد الفتاح بيومي حجازي، المرجع السابق، ص 516.

ISSN 2437-0304
EISSN: 2602-5108
رقم الإيداع القانوني: 3039 -2015
المجلد: 09 العدد: 02 السنة: جوان 2023 م- ذو القعدة 1444 هـ ص: 178 - 198

البيانات والمعطيات والأنظمة المعلوماتية المتعلقة بأي معاملة تجارية تتم عبر البيئة الافتراضية، غير أن الحماية التقنية لا تكفي لوحدها، بل تحتاج إلى تدعيمها بآليات قانونية من شأنها العمل على الحد من الجرائم المعلوماتية.

في هذا المجال، وبالنظر للتطور السريع للمعاملات التي تتم عبر الوسائط الإلكترونية الحديثة، وإزاء سهولة التعدي على وسائل الدفع الإلكتروني وعلى التوقيع الإلكتروني وعلى الأنظمة المعلوماتية والبيانات الشخصية للأشخاص والمؤسسات والشركات التجارية، لجأت مختلف الأجهزة الدولية إلى سن القوانين المتعلقة بالتجارة الإلكترونية، وسلكت الدول نفس المنهج من خلال وضع تشريعات داخلية تدعم المعاملات في إطار التجارة الإلكترونية، من جهة، وحمايتها من الاعتداءات التي يمكن أن تعرقلها وتعيق تطورها، من جهة أخرى.

يتناول هذا المحور الجهود المبذولة ضد الجرائم المعلوماتية على مستوى التشريعات المقارنة (المطلب الأول)، ثم على مستوى التشريع الجزائري (المطلب الثاني).

المطلب الأول: الجهود المبذولة على مستوى التشريعات المقارنة

أمام الصعوبات والتحديات التي تواجهها الدول في مكافحة الجرائم المعلوماتية بمختلف أصنافها ضمن قوانينها وتشريعاتها، لاسيما كونها جريمة تتعدى الحدود الجغرافية والإقليمية، فقد عملت الدول على تكثيف جهودها بالتعاون فيما بينها في مواجهة هذا النوع الجديد من الجرائم.

يقصد بالتشريعات المقارنة المبذولة في سبيل مكافحة الجريمة الإلكترونية في ميدان المعاملات التجارية بالنصوص والتشريعات التي تصدرها المنظمات الدولية والأجهزة الدولية من جهة (أولا)، وفي القوانين والتشريعات الداخلية المبذولة من هذه الدول، سواء كان ذلك عن طريق إصدار مجموعة من القوانين لمحاربة هذا النوع من الجرائم المعلوماتية أو بتعديل وتكييف تشريعاتها مع التطورات التكنولوجية الحديثة، من جهة أخرى (ثانيا).

أولا- التشريعات الدولية في مجال مكافحة الجريمة الإلكترونية

أقرت الأجهزة والهيئات الدولية والإقليمية في إطار محاربة الجريمة المعلوماتية مجموعة من الآليات التقنية والقانونية، من بين هذه الهيئات توجد منظمة الأمم

مجلة الدراسات القانونية (صنف ج) - Journal OF LEGAL STUDIES (Class C)
مجلة علمية دولية سداسية محكمة صادرة عن مخبر السيادة والعولمة – جامعة يحيى فارس بالمدية (الجزائر)
ISSN 2437-0304
EISSN: 2602-5108
رقم الإيداع القانوني: 3039 -2015
المجلد: 09 العدد: 02 السنة: جوان 2023 م- ذو القعدة 1444 هـ ص: 178 - 198

المتحدة باعتبارها منظمة ذات بعد عالمي(1)، ثم الاتحاد الأوربي كونه منظمة إقليمية (2) وأخيرا اللجنة الاقتصادية والاجتماعية لغربي آسيا الإسكوا (3).

1- منظمة الأمم المتحدة

لعبت المنظمات الدولية وعلى رأسها منظمة الأمم المتحدة دورا مهما في الحفاظ على الأمن والاستقرار في مجال مواجهة الجريمة المعلوماتية، من خلال إقرار العديد من الاتفاقيات، مثل اتفاقية الأمم المتحدة لمكافحة الجريمة عبر الوطنية التي اعتمدت وعرضت للتوقيع والتصديق والانضمام بموجب قرار الجمعية العامة للأمم المتحدة 25 الدورة 55 المؤرخ في 15 نوفمبر سنة 2000[21]، كما عقدت العديد من المؤتمرات المتعلقة بهذا المجال.

في نفس الوقت، تمكنت منظمة الأمم المتحدة من تأسيس وكالات متخصصة لهذا الغرض، مثل المنظمة العالمية للملكية الفكرية WIPO، بالإضافة إلى جهود الأمم المتحدة من خلال منظمة اليونسكو، كونها منظمة تابعة لها، ومن بين أهم الاتفاقيات المنبثقة عنها، توجد الاتفاقية العالمية لحق المؤلف.

تعززت الجهود المبذولة من طرف الأمم المتحدة لتطوير التجارة الإلكترونية، عن طريق لجنة القانون التجاري الدولي من إقرار قانونين نموذجيين، يتعلق الأول بالقانون النموذجي للتجارة الإلكترونية، ويتعلق الثاني بالقانون النموذجي للتوقيع الإلكتروني.

وجدير بالذكر أن القانون النموذجي المتعلق بالتجارة الإلكترونية، هو عبارة عن نموذج تتخذه التشريعات الداخلية للدول أثناء سن قوانينها المتعلقة بالتجارة الإلكترونية، وكذا تسهيل المبادلات الداخلية للرسائل الإلكترونية المعتمد عليها في مجال التعاقد.

تلحق الجريمة المعلوماتية في ميدان المعاملات التجارية الإلكترونية الضرر بأطراف عديدة، فهي تصيب مصلحة كل من البائع والمشتري والمورد أو المنتج والمستهلك، وهو الأمر الذي حاول واضعو القانون النموذجي للتجارة الإلكترونية للجنة القانون التجاري الدولي التابعة لمنظمة الأمم المتحدة في سنة 1996 التنبيه والتنويه له،

[21]- قرار الجمعية العامة للأمم المتحدة رقم 25 الدورة 55 المؤرخ في 15 نوفمبر سنة 2000، راجع الموقع التالي:www.unodc.org

مجلة الدراسات القانونية (صنف ج) - Journal OF LEGAL STUDIES (Class C)
مجلة علمية دولية سداسية محكمة صادرة عن مخبر السيادة والعولمة – جامعة يحيى فارس بالمدية (الجزائر)
ISSN 2437-0304
EISSN: 2602-5108
رقم الإيداع القانوني: 3039 -2015
المجلد: 09 العدد: 02 السنة: جوان 2023 م- ذو القعدة 1444 هـ ص: 178 - 198

باعتبار أن المساس بالمصلحة في إطار التجارة الإلكترونية يتحقق بمجرد الاعتداء على الأنشطة التي تتعلق بهذا النوع من التجارة[22].

كما اعتمدت عليه مختلف الدول في وضع قوانينها الداخلية، منها كولومبيا، كوريا الجنوبية، سنغافورة، سلوفينيا... وغيرها من الدول. من جهتهما، تضمن كل من القانون الموحد الكندي المتعلق بالتجارة الإلكترونية لسنة 1999، والقانون الموحد للولايات المتحدة الأمريكية UETA-Uniform Electronic Transations d'Etats لسنة 1999 نفس الأحكام قياسا على القانون النموذجي المذكور، كما تم تبني أحكامه ضمن القانون التوجيهي الأوربي المتعلق بالتجارة الإلكترونية.

2- جهود الاتحاد الأوربي من خلال الاتفاقية الأروبية لمكافحة الإجرام المعلوماتي والمسـماة (بودابست) لعام 2001

من جانبه، أعلن المجلس الأوربي في 27 أبريل سنة 2000 عن مشروع اتفاقية لمواجهة الاعتداءات الحديثة على مواقع الانترنيت التجارية، مثل موقع "أمازون"، حيث أشار إلى المخاطر التي تواجهها الأعمال التي تتم في البيئة الافتراضية، وهي اتفاقية أوربية لمواجهة الاعتداءات على المواقع التجارية الإلكترونية نتيجة المخاطر التي تواجهها شبكة المعلومات، التي دخلت حيز التنفيذ في سنة 2001، وقد تضمنت هذه الاتفاقية توجيها للدول الأعضاء نحو تجريم أفعال الاعتداء على سرية البيانات للجهاز وأنظمته والاتصال بها[23]. كما لجأت معظم دول العالم إلى الدخول في هذا السياق والشروع في تنقيح وتعديل قوانينها الداخلية حتى تتلاءم مع قواعد وأحكام هذه الاتفاقية السابقة الذكر.

3- الإرشاد الصادر عن اللجنة الاقتصادية والاجتماعية لغربي آسيا الإسكوا (الإرشاد الخامس "الجرائم السيبرانية")

تناول القانون الإرشادي المتعلق بالجرائم السيبرانية الصادر عن اللجنة الاقتصادية والاجتماعية لدول غربي آسيا "الإسكوا" مختلف الجرائم المعلوماتية. من بين هذه الجرائم التي لها علاقة بالمعاملات التجارية الإلكترونية، "جرائم التعدي على

[22]- عبد الفتاح بيومي حجازي، نفس المرجع، ص 525.
[23]- عبد الفتاح بيومي حجازي، نفس المرجع، ص231.

مجلة الدراسات القانونية (صنف ج) - Journal OF LEGAL STUDIES (Class C)
مجلة علمية دولية سداسية محكمة صادرة عن مخبر السيادة والعولمة – جامعة يحيى فارس بالمدية (الجزائر)
ISSN 2437-0304
EISSN: 2602-5108
رقم الإيداع القانوني: 3039 -2015
المجلد: 09 العدد: 02 السنة: جوان 2023 م- ذو القعدة 1444 هـ ص: 178 - 198

البيانات المعلوماتية"، جرائم التعدي على الأنظمة المعلوماتية كجريمة الولوج غير المشروع إلى نظام معلوماتي أو المكوث فيه وإعاقة عمل نظام معلوماتي، وجرائم التعدي على الأموال والمعاملات، جرائم التعدي على الملكية الفكرية للأعمال الرقمية، جرائم البطاقات المصرفية والنقود... الخ.

ثانيا- عرض تجارب بعض التشريعات الداخلية للدول

سنت مختلف دول العالم تشريعات داخلية تسمح لها بتحقيق الحماية اللازمة من الجرائم المعلوماتية في ميدان التجارة الإلكترونية، وفي هذا الإطار يمكن التعرف على بعض تجارب تشريعات الدول المقارنة في هذا المجال، منها على سبيل المثال ما يلي:

1- الولايات المتحدة الأمريكية

أصدرت الولايات المتحدة الأمريكية في مجال محاربة الجرائم الإلكترونية ما يعرف بقانون مقاومة قرصنة الفضاء الخارجي (ACPA-PiracyAct) سنة 1999.

2- فرنسا

تم إحداث عدة وحدات ومراكز متخصصة من أجل مكافحة الجرائم المعلوماتية في فرنسا، مثل خلية استقبال وتحليل الانترنيت في سنة 1998 من قبل المديرية العامة للجمارك، كما تم إحداث على مستوى الشرطة القسم الوطني لقمع جرائم المساس بالأموال والأشخاص الذي بدأ مهامه في سنة 1997، والمركز الوطني لمكافحة جرائم تكنولوجيا المعلومات والاتصالات بموجب المرسوم التنفيذي رقم 2000-405 المؤرخ في 15 ماي 2000 على مستوى المديرية المركزية للشرطة القضائية التابعة لوزارة الداخلية، ولهذا المركز اختصاص وطني في مكافحة الجرائم الإلكترونية، كما توجد على مستوى الدرك الوطني مراكز ذات اختصاص وطني وأخرى ذات اختصاص إقليمي[24].

بالإضافة إلى الآليات التقنية والفنية التي وضعتها فرنسا من أجل محاربة الجريمة الإلكترونية، مثل الإستراتيجية الوطنية للأمن الرقمي لسنة 2015، قامت هذه الأخيرة أيضا بعدة مبادرات تهدف إلى محاربة الجريمة الإلكترونية، مثل إصدار القانون رقم 88-19 المؤرخ في 5 يناير 1988، المتعلق بجرائم الغش المعلوماتي، كما تدخل المشرع

[24]- صالح شنين، الحماية الجنائية للتجارة الإلكترونية (دراسة مقارنة)، رسالة دكتوراه في القانون، كلية الحقوق، جامعة أبو بكر بلقايد، تلمسان، الجزائر، 2012- 2013، ص ص 218-220.

مجلة الدراسات القانونية (صنف ج) - Journal OF LEGAL STUDIES (Class C)
مجلة علمية دولية سداسية محكمة صادرة عن مخبر السيادة والعولمة – جامعة يحيى فارس بالمدية (الجزائر)
ISSN 2437-0304
EISSN: 2602-5108
رقم الإيداع القانوني: 3039 -2015
المجلد: 09 العدد: 02 السنة: جوان 2023 م- ذو القعدة 1444 هـ ص: 178 - 198

الفرنسي في سنة 2012 من أجل تعديل قانون العقوبات الصادر في سنة 1992 وعدلت من خلاله العقوبات المتعلقة بالجرائم الإلكترونية.

3- دولة الإمارات العربية المتحدة

من أهم القوانين التي أصدرتها الإمارات العربية المتحدة بهدف حماية المعاملات الإلكترونية من القرصنة الخارجية، يوجد القانون الاتحادي رقم 2 لسنة 2006، المتعلق بمكافحة جرائم تقنية المعلومات، حيث تعد دولة الإمارات العربية المتحدة أول دولة عربية تتمكن من إصدار قانون مختص في مكافحة جرائم المعلومات بشكل مستقل[25]، يتضمن 29 مادة، إذ تناول من خلالها بعض أنواع الجرائم المعلوماتية وتقرير العقاب في حالة ارتكابها.

كما تمكنت الإمارات العربية المتحدة من تطبيق ما يعرف بنظام الرقيب proxy بغرض إحكام الرقابة على شبكة الانترنيت[26]، إصدار القانون الاتحادي رقم 5 لسنة 2012، يتعلق بمكافحة جرائم تقنية المعلومات، المعدل بالقانون الاتحادي رقم 5 لسنة 2016.

4- دولة الكويت

من جانبه، تدخل المشرع في دولة الكويت على سن قانون رقم 30 لسنة 2010، يتعلق بجرائم أنظمة المعلومات، حيث تناول البعض من الجرائم المعلوماتية التي تعيق المعاملات الإلكترونية، مثل الدخول القصدي إلى موقع إلكتروني أو نظام معلومات بأي وسيلة دون تصريح أو بما يخالف التصريح أو يتجاوزه، كل من أدخل أو نشر أو استخدم قصدا برنامجا عن طريق الشبكة المعلوماتية أو باستخدام نظام معلوماتي بهدف التلاعب بالبيانات أو المعلومات كحذفها أو تغييرها والاطلاع عليها، أو تغيير موقع إلكتروني أو إلغائه، أو إتلافه أو تغيير محتوياته ... إلخ. كما أصدر القانون رقم 63 لسنة 2015، المتعلق بمكافحة جرائم تقنية المعلومات الصادر في7 جويلية 2015.

[25]- حسين بن سعيد الغافري، وضع التشريعات السيبرانية في سلطنة عمان، دولة الإمارات العربية المتحدة، دولة قطر، بيروت، اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا)، إدارة تكنولوجيا المعلومات والاتصالات، 2010، ص 51؛ المقال منشور على الموقع الإلكتروني التالي: https://www.unescwa.org.تاريخ الاطلاع يوم 13 فيفري 2019 على الساعة 14:00.

[26]- صالح شنين، المرجع السابق، ص 19.

مجلة الدراسات القانونية (صنف ج) - Journal OF LEGAL STUDIES (Class C)
مجلة علمية دولية سداسية محكمة صادرة عن مخبر السيادة والعولمة – جامعة يحيى فارس بالمدية (الجزائر)
ISSN 2437-0304
EISSN: 2602-5108
رقم الإيداع القانوني: 3039 -2015
المجلد: 09 العدد: 02 السنة: جوان 2023 م- ذو القعدة 1444 هـ ص: 178 - 198

5- قطر

من جانبها، لم تتأخر دولة قطر، هي الأخرى، في محاربة هذه الظاهرة، يتبين ذلك من خلال إصدار قانون مكافحة الجرائم الالكترونية رقم 14 لسنة 2014، حيث كان له دور بالغ الأهمية في محاربة الجرائم المعلوماتية بما فيها الاعتداءات التي تمس بالمعاملات الإلكترونية.

المطلب الثاني: محاربة الجريمة المعلوماتية في التشريع الجزائري

لقد كللت جهود السلطات العمومية في محاربة هذه الظاهرة من خلال إصدار مجموعة من النصوص القانونية قصد مكافحة الجريمة الإلكترونية في ميدان التجارة الإلكترونية، يتعلق الأمر بالقانون رقم 04-15 المؤرخ في 10 نوفمبر سنة 2004، المعدل والمتمم للأمر رقم 66-156 والمتضمن قانون العقوبات (الفرع الأول)، ثم القانون رقم 09-04 المؤرخ في 5 أوت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها (الفرع الثاني).

الفرع الأول: القانون رقم 04-15 المؤرخ في 10 نوفمبر2004، المعدل والمتمم للأمر رقم 66-156 والمتضمن قانون العقوبات

لقد أدخل هذا القانون المذكور في المادة (12) منه تعديل على بعض أحكام وقواعد الأمر رقم 66-156، يتمثل في إتمام للفصل الثالث من الباب الثاني من الكتاب الثالث بقسم سابع مكرر، عنوانه، "المساس بأنظمة المعالجة الآلية للمعطيات" والذي يشمل المواد من 394 مكرر إلى 394 مكرر7.

بقراءة في أحكام هذه المواد، يتبين أن المشرع حدد العديد من أنواع الجرائم المحتملة الوقوع والمتصلة بأنظمة المعالجة الآلية للمعطيات، كما بين العقوبة المقررة لكل العناصر المشكلة للجرائم المذكورة، محددا بذلك الحد الأدنى والأقصى لعقوبة الحبس والغرامة المالية لكل نوع من هذه الجرائم المرتكبة.

من جهة أخرى، يلاحظ أن المشرع ضاعف وشدد العقوبات في حالة استهداف هذه الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام. كما نص على عقوبات مالية مشددة في حالة ارتكاب هذه الجرائم من قبل الشخص المعنوي تعادل خمس(5) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي.

وعلاوة على العقوبات السابقة الذكر، نص القانون على عقوبات أخرى، تتمثل في مصادرة الأجهزة والبرامج والوسائل المستعملة مع إغلاق المواقع التي تكون محلا

ISSN 2437-0304
EISSN: 2602-5108
رقم الإيداع القانوني: 3039 -2015
المجلد: 09 العدد: 02 السنة: جوان 2023 م- ذو القعدة 1444 هـ ص: 178 - 198

لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم، وإغلاق المحل أو مكان الاستغلال في حال ما إذا كانت الجريمة قد ارتكبت بعلم مالكها.

على العموم، لقد حاول المشرع إحاطة جميع الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، مقررا لها بذلك عقوبات من طبيعة مختلفة مالية وسالبة للحرية ومادية، تهدف في النهاية إلى ردع المخالفين على ارتكاب لمثل هذه الجرائم وتقرير الحماية اللازمة لأنظمة المعالجة الآلية للمعطيات.

الفرع الثاني: القانون رقم 09-04 المؤرخ في 5 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

يعكس صدور هذا القانون رغبة وسعي السلطات العمومية على مواجهة الجرائم ذات العلاقة بتكنولوجيات الإعلام والاتصال وسبل مكافحتها، التي أصبحت تهدد بشكل متزايد وملحوظ الأنظمة المعلوماتية وقواعد البيانات للشركات والمؤسسات وتشكل خطرا كبيرا على أمن واستقرار الاقتصاد الوطني.

احتوى القانون المذكور على (18) مادة موزعة على ست فصول تتناول العديد من المحاور الأساسية في هذا القانون.

جاء في بداية الأحكام المتعلقة بهذا القانون بقواعد عامة تتمثل في تحديد الهدف من هذا القانون، وشرح لبعض المصطلحات الواردة في النص وحدد مجال تطبيقه.

خصص الفصل الثاني من القانون لمراقبة الاتصالات الإلكترونية والحالات التي تسمح باللجوء إلى المراقبة الإلكترونية، أما الفصل الثالث من النص، فبين القواعد الإجرائية المتعلقة بتفتيش المنظومات المعلوماتية وكذا حجز المعطيات المعلوماتية والحجز عن طريق منع الوصول إلى المعطيات، وبين المعطيات المحجوزة ذات المحتوى المجرم وحدود استعمال المعطيات المتحصل عليها.

بدوره، عالج الفصل الرابع التزامات مقدمي الخدمة، من خلال تقديم المساعدة للسلطات العمومية المكلفة بالتحريات القضائية وحفظ المعطيات المتعلقة بحركة السير، وكذا العقوبات المقررة في حالة عدم احترام مقدمي الخدمات لالتزاماتهم.

من جهة أخرى، تنبأ القانون بإنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته وحدد مهامها، وهذا طبقا أحكام المادتين 13 و14 من الفصل الخامس من القانون.

أما على مستوى الفصل السادس والأخير من هذا القانون، فقد تناول موضوع التعاون والمساعدة القضائية الدولية والاختصاص القضائي، مثل المساعدة القضائية

ISSN 2437-0304
EISSN: 2602-5108
رقم الإيداع القانوني: 3039 -2015
المجلد: 09 العدد: 02 السنة: جوان 2023 م- ذو القعدة 1444 هـ ص: 178 - 198

الدولية المتبادلة وتبادل المعلومات واتخاذ الإجراءات التحفظية، وفي الأخير القيود الواردة على طلبات المساعدة القضائية الدولية.

مما سبق يمكن القول أن الجزائر حاولت كغيرها من بلدان العالم، الاعتماد على بعض الحلول التقنية والحلول القانونية في سبيل مكافحة الجريمة الإلكترونية بشتى أنواعها، التي أضحت حقيقة واضحة تزداد يوما بعد يوم نظرا للاعتداءات المتواصلة والمتزايدة على الأنظمة المعلوماتية وقواعد البيانات لمختلف الشركات والمؤسسات، كما أن لها آثار خطيرة على الأنظمة المعلوماتية وعلى البيانات الشخصية للمتعاملين الاقتصاديين، خاصة وأنها تتطور بصفة مستمرة وبشكل متزامن مع التطورات التكنولوجية الحديثة.

الخاتمة

أصبحت الجرائم الالكترونية ظاهرة تؤرق دول العالم بأكمله، لما لها من آثار اقتصادية واجتماعية خطيرة، ونظرا لكونها كذلك فقد اهتمت المنظمات العالمية الدولية وكذا الدول بسن تشريعات داخلية بغرض مكافحة هذا النوع من الجرائم، من خلال نصوص قانونية تتضمن قواعد تعمل على منع وقوع الجريمة الالكترونية من جهة، ومن جهة أخرى، تقرير المسؤولية الجنائية عند قيامها، وردع مرتكبيها وغيرها من الأحكام التي تعمل على الحد من هذه الجريمة والتقليل من مخاطرها.

غير أن وجود الآليات التقنية لما لها من دور فعال في محاربة الجريمة المعلوماتية كونها أدوات وقائية وردعية، إلا أن الحلول التقنية لا تكفي لوحدها، بل يتطلب الأمر وجود آليات قانونية التي يمكن من خلالها الحد من حدوث هذا النوع من الجرائم، وهذا الذي عملت به مختلف التشريعات الدولية والداخلية المقارنة على غرار المشرع الجزائري.

ومن أجل دعم المعاملات التجارية وتعزيز قطاع التجارة الإلكترونية أكثر، يستلزم الأمر وضع إجراءات وتدابير تسمح بحماية أكثر فعالية ضد الاعتداءات التي تمس الوسط الافتراضي، لذلك يجب على الدول ومن بينها الجزائر العمل على:

- استحداث نصوص قانونية تتلاءم مع التقدم التكنولوجي في مجال الوسائط الإلكترونية، بحيث يجب أن تساير النصوص القانونية مع الجرائم الإلكترونية التي تتطور بتطور التقنيات الحديثة.
- توفير بيئة آمنة يتم من خلالها إتمام العمليات التجارية الإلكترونية.

ISSN 2437-0304
EISSN: 2602-5108
رقم الإيداع القانوني: 3039 -2015
المجلد: 09 العدد: 02 السنة: جوان 2023 م- ذو القعدة 1444 هـ ص: 178 - 198

- تفعيل آليات قانونية وآليات تقنية أكثر صرامة وأكثر وقائية وردعية في، نفس الوقت، تسمح بتحقيق حماية كاملة وشاملة للمبادلات التجارية التي تتم عبر الوسائط الإلكترونية.

- تعزيز التعاون الدولي بين الدول في مجال مكافحة الجرائم المعلوماتية التي تعرقل تطور التجارة الإلكترونية.

- في الجزائر، يجب عليها أن تستمر في وضع مختلف الأدوات والوسائل التي تمكنها من محاربة هذه الظاهرة، وأن تعمل مع شركائها الدوليين قصد الاستفادة من تجاربها في مجال مكافحة الجرائم المعلوماتية التي تعد كعائق للمعاملات التجارية الإلكترونية.

- تطوير برامج وتطبيقات حمائية تتحقق من خلالها حماية أكثر للرسائل الإلكترونية المعتمد عليها في العقود الإلكترونية...الخ.

- الدفع والتحسيس بأهمية وخطورة هذه الجرائم على المعاملات التجارية والاقتصاد الوطني بوجه عام.

المراجع:

أولا- باللغة العربية

- القوانين

1- القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، المعدل والمتمم للأمر رقم 66-156 المؤرخ في 8 جوان 1966 المتضمن قانون العقوبات، الجريدة الرسمية عدد 71 بتاريخ 10 نوفمبر 2004، ص.8

2- القانون رقم 09-04 المؤرخ في 5 أوت 2009، المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية عدد 47 بتاريخ 16 أوت 2009، ص.5

3- القانون رقم 18-05، المؤرخ في 10 ماي 2018، المتعلق بالتجارة الإلكترونية، الجريدة الرسمية، العدد 28، الصادر بتاريخ 16 ماي 2018، ص 4.

- قرارات

1- قرار الجمعية العامة للأمم المتحدة رقم 25 الدورة 55 المؤرخ في 15 نوفمبر سنة 2000، راجع الموقع التالي:www.unodc.or

- الكتب

1- حسين بن سعيد الغافري، وضع التشريعات السيبرانية في سلطنة عمان، دولة الإمارات العربية المتحدة، دولة قطر، بيروت، اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا)، إدارة تكنولوجيا المعلومات والاتصالات، سلطنة عمان، 2010، ص 51؛ الكتاب منشور على الموقع الإلكتروني التالي: https://www.unescwa.org..

2- عبد الفتاح بيومي حجازي، الحكومة الإلكترونية بين الواقع والطموح، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، مصر، 2008.

- الرسائل والمذكرات

1- صالح شنين، الحماية الجنائية للتجارة الإلكترونية (دراسة مقارنة)، رسالة دكتوراه في القانون، كلية الحقوق، جامعة أبو بكر بلقايد تلمسان، الجزائر، 2012-.2013
2- عائشة بوخبزة، الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري، مذكرة ماجستير في القانون الجنائي، كلية الحقوق، جامعة وهران، الجزائر، 2012-.2013
3- كمال حطاب، الحماية الجزائية للتجارة الإلكترونية، أطروحة دكتوراه في العلوم، كلية الحقوق والعلوم السياسية، جامعة جيلالي اليابس، سيدي بلعباس، الجزائر، 2015-.2016
4- نورة طرشي، مكافحة الجريمة المعلوماتية، مذكرة ماجستير في القانون الجنائي، جامعة الجزائر1، 2012.

- المقالات

1- جنان الخوري، الحوسبة السحابية في الدول العربية: الجوانب القانونية والتشريعية، واقع وآفاق، مقال ضمن تقرير الاتحاد الدولي للاتصالات المؤرخ في 30 ديسمبر 2015، بيروت، ص ص 1-70 ؛ المقال منشور في الموقع الإلكتروني التالي: https://www.itu.int.
2- عبد الصمد حوالف، الحماية القانونية للمستهلك في عقود التجارة الإلكترونية، مقال منشور في مجلة الأكاديمية للدراسات الاجتماعية والإنسانية، المجلد 08، العدد 1، جامعة حسيبة بن بوعلي، الشلف، الجزائر، 2016، ص ص 124-130؛ المقال مشور في الموقع الإلكتروني التالي: https://www.asjp.cerist.dz.
3- عزوز سعيدي، التجارة الإلكترونية وتحديات الجريمة المعلوماتية، مقال منشور في مجلة الدراسات والبحوث القانونية، المجلد 04، العدد 01، كلية الحقوق والعلوم السياسية، جامعة لونيسي علي، البليدة 2، الجزائر، 2019، ص ص 218-232؛ المقال منشور في الموقع الإلكتروني التالي: https://www.asjp.cerist.dz.

- أشغال الملتقيات

1- ناصر حمودي، الحماية الجنائية الموضوعية والإجرائية الخاصة المقررة للمستهلك الإلكتروني في التشريع الجزائري، مداخلة ضمن الملتقى الوطني الثالث حول المستهلك والاقتصاد الرقمي: ضرورة الانتقال وتحديات الحماية، المركز الجامعي عبد الحفيظ بوالصوف، ميلة، 23-24 أفريل 2018، ص ص 1-20؛ المداخلة منشورة في الموقع الإلكتروني التالي: http://dspace.centre-univ-mila.dz/jspui/handle.

ثانيا-المراجع باللغة الفرنسية:

- Articles:

1-Josef DEXEL, Mondialisation et société de l'information-le commerce électronique et la protection des consommateurs, Article, Revue international de droit, 2022, p p 405-444 ; disponible sur le site : https://www.cairn.info/revue-internationale-de-droit-economique-2002.