حماية المستهلك الإلكتروني في ظل الجرائم السيبرانية

Electronic consumer protection in light of cybercrime.

ط. د/ عز الدين غبش *

جامعة الشهيد حمة لخضر الوادي

gh.ezza07@gmail.com

تاريخ الاستلام:2021/11/17 تاريخ القبول للنشر: 2021/12/17 تاريخ النشر: 2022/04/30

ملخص: تهدف هذه الدراسة إلى تسليط الضوء على كيفية حماية المستهلك الإلكتروني من المخاطر في ظل المعاملات الإلكترونية التي أصبحت عرضة إلى الجرائم السيبرانية باعتبارها أكبر المشكلات المعاصرة من خلال عدة أساليب قمعية كالغش والاحتيال والنصب والتزوير...الخ. وقد خلصت هذه الدراسة إلى عدة آليات ووسائل لحماية المستهلك منها الإدارية والتقنية وكذا القانونية، ومن جهة أخرى طرحت الدراسة العديد من التوصيات والاقتراحات والتي قد تشكل جدار حماية من شأنه أن يحمي المستهلك كتفعيل نوع من الرقابة على مختلف العمليات والاتفاقيات الإلكترونية لحماية المستهلك وكذا سن القوانين والتشريعات التي تنظم نشاط التجارة والمعاملات الإلكترونية على المستوى الدولي، وأمن المعاملات التجارية والمدفوعات بما يعزز من حماية المستهلك الإلكتروني من مختلف أنماط الاحتيال والاختراق والغش الإلكتروني.

الكلمات المفتاحية: مستهلك إلكتروني، جرائم سيبرانية، معاملات إلكترونية، غش إلكتروني.

Abstract: *This study aims to highlight how to protect the electronic consumer from risks in light of electronic transactions that have become vulnerable to cybercrimes considered as the biggest contemporary problems through several repressive methods such as trickery, fraud, forgery...etc. This study concluded that several mechanisms and means of consumer's protection exist including administrative, technical, as well as legal. On the other hand, the study put forward many recommendations and suggestions, which may constitute a firewall that would protect the consumer, such as activating a kind of control over various electronic processes and conventions for consumer's, as well as enacting laws and legislations which regulates the activity of electronic commerce and transactions at the international level, and the security of commercial transactions and payments in a way that enhances the protection of the electronic consumer from various types of hacking and electronic fraud.*

Key Words: *Electronic Consumer, Cybercrimes, Electronic Transactions, Electronic Fraud*

* المؤلف المراسل

مقدّمة:

في ظل التحولات الكبرى التي يعيشها العالم اليوم في جميع المجالات خاصة منها ثورة تكنولوجيا المعلومات والاتصالات، وظهور العديد من الوسائل التكنولوجية الحديثة التي اختزلت الوقت والمسافة وساعدت على تحويل العالم إلى قرية صغيرة يتلاشى فيها أثر الحدود الجغرافية والسياسية. وفي خضم جملة التحولات التي مست بيئة الأعمال التقليدية، ونقلت المعاملات التجارية إلى عام افتراضي يفصل فيه بين البائع والمستهلك شاشة ونقرة زر، أين يتم انتقاء السلع والخدمات وتسديد أثمانها من خلال الحواسيب والأجهزة الذكية وبطاقات وأجهزة الدفع الإلكتروني. لتساهم هذه الوسائط متحدة في استحداث نمط إدارة المعاملات الإلكترونية عبر الأنترنيت، وابتكار طرق جديدة لعرض المنتج والخدمة وتسديد أثمانها، وإلغاء عائق البعد الزماني والمكاني بين البائع والمستهلك.

غير أنه ورغم المزايا العديدة للمعاملات الإلكترونية توجد العديد من المعوقات التي قد تجعلها بديلا مكلفا عن المعاملات التقليدية خاصة بالنسبة للمستهلك، الذي قد يتعرض لبعض المخاطر والجرائم الإلكترونية أو السيبرانية كالتزوير، النصب، الاحتيال والغش. فلقد اكتسب موضوع حماية المستهلك أهمية كبيرة في السنوات الأخيرة، وبرزت قضية حماية المستهلك كقضية هامة ضمن قضايا المسؤولية الاجتماعية الواجب على المنظمات أخذها في الحسبان عند وضع الخطط واتخاذ القرارات، كما مكانا بارزا بين القضايا السياسية والاجتماعية والاقتصادية المطروحة في المؤتمرات والندوات وحازت على اهتمام العديد من الكتاب والباحثين، إذ بدأ مفهوم الحماية الإلكترونية في التبلور خاصة بعد اتساع مستخدمي الأنترنيت في العالم، وهو ما يعني الحفاظ على حقوق المستهلك

وحمايته من الغش أو الاحتيال أو شراء بضائع مغشوشة باستخدام أدوات الويب التي تستطيع الوصول لكل مكان وتمارس تأثيرا يتجاوز أحيانا الأدوات التقليدية.

إشكالية الدراسة:

على ضوء ما سبق فإن إشكالية الدراسة تتمحور حول التساؤل التالي:

كيف يمكن حماية المستهلك الإلكتروني في ظل الجرائم السيبرانية؟

وتنبثق من الإشكالية الرئيسية التساؤلات الفرعية التالية:

- ما المقصود بالجرائم السيبرانية؟ وما مفهوم الحماية الإلكترونية للمستهلك؟
- ما مبررات حماية المستهلك الإلكتروني؟
- ما هي أهم الوسائل لحماية المستهلك الإلكتروني من المخاطر التي يتعرض لها في ظل الجرائم السيبرانية؟

أهمية الدراسة:

تستمد هذه الدراسة أهميتها من أهمية المستهلك باعتباره أساس وجوهر أي معاملة إلكترونية وباعتباره الطرف الضعيف في العملية التعاقدية الأمر الذي يستدعي البحث عن أهم المخاطر التي يمكن أن يتعرض لها في ظل الجرائم السيبرانية وكذا أهمية توفير الحماية له في ظل هذه المعاملات، وأهمية وجود مجموعة قواعد من شأنها أن توفر الحماية لكل طرف من أطراف المعاملة الإلكترونية سواء كان داخل حدود الدولة أو خارجها.

أهداف الدراسة:

تهدف هذه الدراسة إلى:

- تقديم إطار نظري يوضح مفهوم الجرائم السيبرانية باعتبارها من المواضيع الحديثة في العالم الافتراضي، وكذا مفهوم حماية المستهلك الإلكتروني في ظل هذه الجرائم؛

- تحديد أهم المخاطر التي يتعرض لها حماية المستهلك الإلكتروني في ظل الجرائم السيبرانية؛
- التوصل إلى أهم الوسائل التي تساهم في حماية المستهلك الإلكتروني من الجرائم السيبرانية.

منهج الدراسة:

من أجل الإجابة على الإشكالية المطروحة والإلمام بمحاور الدراسة تم الاعتماد على المنهج الوصفي والتحليلي لملائمته لطبيعة الموضوع.

هيكل الدراسة

بهدف الإلمام بأدبيات الدراسة من مختلف الجوانب ومحاولة الإجابة على إشكالية الدراسة فقد تم تقسيمها إلى المحاور التالية:

أولا: الإطار المفاهيمي للجرائم السيبرانية؛

ثانيا: الإطار العام للمستهلك الإلكتروني

ثالثا: المخاطر التي يتعرض لها المستهلك الالكتروني في ظل الجرائم السيبرانية ووسائل حمايته منها؛

أولا: الإطار المفاهيمي للجرائم السيبرانية

تشكل الجرائم السيبرانية تحديا كبيرا للبيئة التي ترتكب فيها، إذ يمكن لمجرمي الأنترنيت العمل من أي مكان في العالم، واستهداف أعداد كبيرة من الناس أو الشركات عبر الحدود الدولية، وتزداد التحديات التي تفرضها استنادا إلى نطاق وحجم الجرائم، والتعقيد التقني لتحديد هوية الجناة وكذلك ضرورة العمل على الصعيد الدولي لتقديمهم إلى

العدالة، فالأنترنيت تفتح فرصا جديدة لمجرميها، على أساس الاعتقاد بأن إنقاذ القانون لا يعمل في عالم الأنترنيت.

1- تعريف الجريمة السيبرانية:

تعددت تسميات المفكرين والباحثين في هذا المجال ولا يوجد إجماع على تعريف الجريمة السيبرانية من حيث كيف تعرف وما هي الجرائم التي تتضمنها الجريمة السيبرانية وفي أغلب الأحيان هناك من يسميها: جريمة العصر، الجريمة الإلكترونية، استخدام نظم المعلومات.[1] فهي تمثل مختلف السلوكات التي ترتكب ضد الأفراد بدافع إلحاق الضرر بالطرف الآخر باستخدام الحاسوب وشبكات الاتصال المختلفة، فالجرائم السيبرانية بشكل عام هي جميع أشكال الجريمة التي تلعب فيها تكنولوجيات المعلومات والاتصال دورا أساسيا وتتكون الجريمة السيبرانية من كلمتين هما: الجريمة Crime والسيبرانية Cyber وهو مصطلح مشتق من المصطلح الإغريقي Kubernan الذي يعني التسيير والقيادة، مع الإشارة إلى أن الجريمة السيبرانية لم يبث في تعريفها من طرف رجال القانون باستثناء ما نصت عليه إجراءات الاتحاد الأوروبي الخاصة بمذكرة التوقيف، وقد عرفت هيئة الأمم المتحدة الجريمة السيبرانية على أنها: "جميع السلوكات غير القانونية التي تستخدم عمليات إلكترونية تستهدف أمن النظام المعلوماتي والمعطيات التي يعالجها".[2]

ومنهم من عرف الجرائم السيبرانية بأنها: "هي التي تتم بواسطة الكمبيوتر أو أحد وسائل التقنية الحديثة على كمبيوتر آخر أو أحد وسائل التقنية الحديثة، مع ضرورة توفر شبكة اتصال فيما بينها".[3]

والبعض الآخر عرفها بأنها: "نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود".[4]

وقد عرف اتفاق منظمة شنغهاي للتعاون الجرائم السيبرانية على أنها: "استخدام موارد المعلومات والتأثير عليها في المجال المعلوماتي لأغراض غير مشروعة".[5]

ومن خلال ما سبق يمكن أن نعرف الجريمة السيبرانية بأنها: "كل فعل أو امتناع يقوم به الشخص بصفة عمدية يتمثل في فعل الاستخدام غير المشروع لتقنية المعلومات بحيث يهدف من خلاله إلى تحقيق مصالح شخصية تتمثل في الاعتداء على الأموال المادية أو المعنوية، كما قد ينصب موضوعها أيضا في الاعتداء على خصوصية الأفراد والمؤسسات، فهي كل عمل أو امتناع يأتيه الشخص قصد الإضرار بمكونات الحاسب وشبكات الاتصال الخاصة به هذا من جهة، ومن جهة أخرى فإن هذه الجريمة هي التي يكون النظام المعلوماتي فيها وسيلة أساسية لارتكاب جريمة تقليدية، إما ضد الأموال كالتحويل الإلكتروني غير المشروع للأموال أو ضد الأشخاص كجريمة السب أو القذف عبر شبكة الانترنيت.[6]

وبالرجوع إلى القانون الجزائري عرف المشرع الجزائري الجرائم السيبرانية وأطلق عليها تسمية الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وعرفها بموجب الفقرة "أ" المادة 02 من القانون رقم 09-04 على أنها: "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية".[7]

ومما سبق نلاحظ أن الإطار المفاهيمي الذي حدده المشرع الجزائري للجرائم السيبرانية قد اعتمد بالدرجة الأولى على الجمع بين معايير عديدة في تعريفه لهذه الجريمة الخاصة، ففي البداية اعتمد على معيار الوسيلة المتعمدة في الجريمة والتي تتمثل في نظام الاتصالات الإلكتروني، ثم اعتمد على المعيار القائم على أساس الموضوع والمتمثل في

المساس بأنظمة المعالجة الآلية للمعطيات، يليها بعد ذلك معيار القانون الواجب التطبيق أو ما يطلق عليه بالركن الشرعي في الجريمة.

2- خصائص الجرائم السيبرانية:

تتميز الجرائم السيبرانية بخصائص تختلف إلى حد ما عن الجريمة العادية على النحو التالي:

- **جرائم عابرة للدول:** وهي الجرائم التي تقع بين أكثر من دولة ولا تعترف بالحدود الجغرافية مثلها مثل جرائم غسيل الأموال والمخدرات وغيرها، ففي عصر الحاسوب والأنترنيت أمكن ربط أعداد هائلة من الحواسيب عبر العالم، وعند وقوع جريمة إلكترونية غالبا يكون الجاني في بلد والمجني عليه في بلد آخر كما قد يكون الضرر في بلد ثالث؛
- **جرائم صعبة الإثبات:** يستخدم فيها الجاني وسائل فنية معقدة وسريعة في كثير من الأحيان قد لا تستغرق أكثر من بضع ثواني، بالإضافة إلى سهولة محو الدليل والتلاعب فيه والأهم عدم تقبل القضاء في كثير من الدول للأدلة التقنية المعلوماتية التي تتكون من دوائر وحقول مغناطيسية ونبضات كهربائية غير ملموسة بالحواس الطبيعية للإنسان؛
- **جرائم سهلة الإرتكاب:** فهي جرائم ناعمة (Soft Crime) وأطلق عليها البعض اسم جرائم الياقات البيضاء، وعند توفر التقنية اللازمة للجاني يصبح ارتكاب الجريمة من السهولة بمكان ولا تحتاج إلى وقت ولا جهد؛
- **عدم قيام ضحايا الإجرام السيبراني بتقديم الشكوى أو التبليغ:** أي أنه لا يتم في غالب الأحيان تقديم شكوى أو الإبلاغ عند ارتكابها، إما لعدم اكتشاف الضحية لها وإما خوفا من التشهير، لذا نجد أن معظم جرائم الأنترنيت تكتشف بالمصادفة،

وأحيانا بعد وقت طويل من ارتكابها، زيادة على ذلك أن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي كشف الستار عنها، فالرقم المظلم بين حقيقة عدد الجرائم المرتكبة والعدد الذي تم اكتشافه هو رقم خطير[8].

3- أسباب ارتكاب الجرائم السيبرانية:

يمكن تلخيص أسباب انتشار الجرائم السيبرانية فيما يلي:[9]

- **الولع بجمع المعلومات:** هناك من يقوم بارتكاب جرائم الكمبيوتر بغية الحصول على الجديد من المعلومات، فيرى قراصنة الكمبيوتر أن الحصول على المعلومة يجب ألا يكون عليه أي قيد؛ فالقرصان يكرس كل جهده في تعلم كيفية اختراق المواقع المحمية، وغالبا ما يكون القراصنة مجموعات الهدف منها التعاون وتبادل المعلومات وتقاسم البرامج والأخبار؛
- **تحقيق مكاسب مالية:** قد تدفع حاجة البعض إلى تحقيق الثراء السريع عن طريق إتاحة الاطلاع على معلومات معينة أساسية ذات أهمية خاصة لمن يطلبها؛
- **الدوافع الشخصية:** يتأثر الإنسان في بعض الأحيان ببعض المؤثرات الخارجية التي تحيط به، ونتيجة لوجوده في بيئة المعالجة الآلية للمعلومات، مع توافر هذه المؤثرات، فإن الأمر يؤول في النهاية إلى ارتكابه لجريمة معلوماتية، هذا وتتعدد المؤثرات التي تدفع الإنسان إلى اقتراف مثل هذا السلوك، سواء كان ذلك بدافع اللهو أو الانتقام.

4- أهداف الجريمة السيبرانية:

يمكن توضيحها أهدافها في النقاط التالية:[10]

- الوصول إلى المعلومات بشكل غير قانوني كسرقة المعلومات وتعطيلها أو تخريبها وذلك عبر الأنترنيت؛

- الوصول إلى الأجهزة الخادمة الموفرة للمعلومات وتعطيلها أو تخريبها؛
- الحصول على عناوين تغيير مواقع الانترنيت بهدف تخريب المؤسسات العامة؛
- الوصول إلى الأشخاص أو الجهات المستخدمة للتكنولوجيا بغرض التهديد أو الابتزاز؛
- الاستفادة من تقنية المعلومات من أجل كسب مادي أو معنوي أو سياسي كعمليات تزوير بطاقات الائتمان وعمليات اختراق المواقع الإلكترونية؛
- استخدام التكنولوجيا في دعم الإرهاب والأفكار المتطرفة؛

يتضح مما سبق أن الجريمة السيبرانية ذات أهداف غير مشروعة تمارس ضغوطات لإلحاق الضرر بالطرف الآخر من خلال التهديد والابتزاز أو السرقة المعلوماتية أو تخريب نظم المعلومات لتحقيق مكاسب خاصة.

5- تصنيف الجرائم السيبرانية ومرتكبوها:

5-1- تصنيف الجرائم السيبرانية:

لم يستقر الفقهاء على معيار واحد لتصنيف الجرائم السيبرانية وذلك راجع إلى تشعب هذه الجرائم، وسرعة تطورها، فمنهم من يصنفها بالرجوع إلى وسيلة ارتكاب الجريمة، أو دافع المجرم، أو على أساس محل الجريمة، وعلى هذا الأساس يمكن تقسيمها إلى[11]:

- **الجرائم الواقعة على الأموال:** في ظل التحول من المعاملات التجارية التقليدية إلى المعاملات التجارية الإلكترونية، وما انجر عنه من تطور في وسائل الدفع والوفاء، وفي خضم التداول المالي عبر الأنترنيت، أصبحت هذه المعاملات عرضة لشتى أنواع الجرائم ومنها:
  - السطو على أرقام بطاقات الائتمان والتحويل الإلكتروني غير المشروع؛

- القمار وغسيل الأموال عبر الأنترنيت؛
- جريمة السرقة والسطو على أموال البنوك؛
- تجارة المخدرات عبر الأنترنيت.

➢ **الجرائم الواقعة على الأشخاص:** مع تطور شبكة الأنترنيت أصبحت المعلومات المتعلقة بالأفراد متداولة بكثرة عبرها، مما جعلها عرضة للانتهاك والاستعمال من طرف هؤلاء المجرمين وجعلت سمعة وشرف الأفراد مستباحة، ومن أهم هذه الجرائم ما يلي:

- جريمة التهديد والمضايقة والملاحقة؛
- انتحال الشخصية والتغرير والاستدراج؛
- صناعة ونشر الإباحة؛
- جرائم القذف والسب وتشويه السمعة.

➢ **الجرائم الواقعة على أمن الدولة:** من أهم الجرائم الإلكترونية التي تهدد أمن الدول ومجتمعاتها ما يلي:

- **الجماعات الإرهابية:** استغلت الكثير من الجماعات المتطرفة الطبيعة الاتصالية للأنترنيت من أجل بث معتقداتها وأفكارها، بل تعداه الأمر إلى ممارسات تهدد أمن الدولة المعتدى عليها؛
- **الجريمة المنظمة:** استغلت عصابات الجريمة المنظمة الإمكانيات المتاحة في وسائل الاتصال والأنترنيت في تخطيط وتمرير وتوجيه المخططات الإجرامية وتنفيذ العمليات الإجرامية بيسر وسهولة

- **الجرائم الماسة بالأمن الفكري:** يبقى الأمن الفكري من بين أخطر الجرائم المرتكبة عبر الأنترنيت، حيث تعطي الأنترنيت فرصا للتأثير على معتقدات وتقاليد مجتمعات بأكملها مما عرضة للهزيمة الفكرية وهو ما يسهل خلق الفوضى؛
- **جريمة التجسس الإلكتروني:** سهلت شبكة الأنترنيت الأعمال التجسسية بشكل كبير حيث يقوم المجرمون بالتجسس على الأشخاص أو الدول أو المنظمات أو الهيئات أو المؤسسات الدولية أو الوطنية، وتستهدف عملية التجسس في عصر المعلوماتية ثلاث أهداف رئيسية وهي: التجسس العسكري، والتجسس السياسي، والتجسس الاقتصادي.

ويعتبر أهم تصنيف للجرائم السيبرانية قد جاءت به الاتفاقية الأوروبية بشأن الجرائم الإلكترونية لسنة 2001 وهي اتفاقية بودابست لسنة 2001، حيث قسمت الاتفاقية هذه الجرائم إلى[12]:

- **الطائفة الأولى:** الجرائم التي تستهدف سرية وسلامة وتوفر المعطيات، أي الجرائم التي تستهدف معطيات الكمبيوتر سواء بالاطلاع عليها أو إفشائها أو تصويرها، أو إتلافها؛
- **الطائفة الثانية:** وهي الجرائم المرتبطة بالكمبيوتر أي الجرائم التي يلعب فيها الكمبيوتر أو الحاسب الآلي دور الوسيلة كجرائم الاحتيال والتزوير الإلكتروني؛
- **الطائفة الثالثة:** الجرائم المرتبطة بالمحتوى، أي يلعب فيها الكمبيوتر دور البيئة الجرمية كجرائم المواد اللاأخلاقية للأطفال، وجرائم القمار وغسيل الأموال والمخدرات؛
- **الطائفة الرابعة:** وهي الجرائم المتعلقة بحقوق الملكية الفكرية كحقوق المؤلف وهو نص مكمل لما جاءت به قوانين الملكية الفكرية المقررة وطنيا ودوليا.

أما في الجزائر، فلقد قسم المشرع الجزائري الجرائم المتصلة بتكنولوجيا الإعلام والاتصال أو الجرائم السيبرانية إلى الطوائف التالية[13]:

- **الطائفة الأولى**: جرائم الولوج إلى المعطيات المعالجة آليا عن طريق الغش والتزوير وكذا جريمة الحذف والتغيير والتخريب في هذه المعطيات؛
- **الطائفة الثانية**: الجرائم الإلكترونية بواسطة النظام المعلوماتي وأهمها استعمال أو إفشاء أو نشر معلومات منصوص عليها في قانون العقوبات، وكذا البحث أو تجميع في معطيات مخزنة في نظام معلوماتي، كجرائم التحويل الإلكتروني والسطو والنصب والاحتيال والسلب وغيرها؛
- **الطائفة الثالثة**: الجرائم الإلكترونية المتعلقة بأمن الدولة ومؤسساتها كجرائم التجسس والإرهاب؛
- **الطائفة الرابعة**: الجرائم الإلكترونية للشخص المعنوي.

ويلاحظ أن المشرع الجزائري قد توسع في نطاق الجرائم السيبرانية سواء وقعت على النظام المعلوماتي أو بواسطته، وسواء وقعت على الأشخاص أو الأموال أو على أمن الدولة ومؤسساتها.

وما يعاب على المشرع الجزائري عدم إفراد معيار واضح وواحد في تقسيم الجرائم السيبرانية وتحديد عقوبتها، ولكن من الاحسن اتباع المنهج المتبع من طرف الفقه وهو تقسيمها إلى جرائم واقعة على النظام المعلوماتي وجرائم واقعة بواسطة النظام المعلوماتي، بعد تحديد المصطلحات الخاصة بها لتسهيل فهم ما هيتها.

2-5- مرتكبو الجرائم السيبرانية:

أنواع الجناة في جرائم الأنترنيت كما يطلق عليهم اسم القراصنة، ويمكن حصر هؤلاء في ثلاثة فئات[14]:

- **الهاكرز**: أو القراصنة وتعتبر القرصنة من أخطر الجرائم المعلوماتية فقد تكون القرصنة ذات أغراض تخريبية أو تكون ذات أغراض ترفيهية فضولية. أكثر القراصنة من الفئات الشبابية ويتميزون بهوس التعمق بالكمبيوتر والأنترنيت؛
- **الكراكرز**: وهم القراصنة المحترفون، ويعد هذا النوع من أكثر أنواع مرتكبي الجرائم الإلكترونية خطورة، ويكون القراصنة من هذه الطائفة ذوي مكانة اجتماعية عادية أو متخصصين في العلوم الإلكترونية؛
- **الطائفة الحاقدة**: تستهدف غالبا هذه الطائفة المنظمات والمنشآت وأرباب العمل، ويكون الهدف من ارتكابها للجريمة بحق هذه الأطراف عادة بغية الانتقام والحصول على المنفعة المادية أو السياسية، وقد يكون تطرفا أو جاسوسا أو مخترق الأنظمة.

6- سبل مواجهة الجريمة السيبرانية:

إن المواجهة الفاعلة للهجمات السيبرانية تستلزم التعاون والتنسيق على المستوى الدولي وكذا على المستوى العربي والوطني، لتحقيق الأمن الإلكتروني والكشف عن التهديدات الأمنية المختلفة والتفاعل معها والتخفيف من الآثار السلبية المحتملة، وسنذكر بعض الإجراءات المتخذة على المستوى العربي والعالمي لمكافحة جرائم الأنترنيت والحاسوب:[15]

- **الشق الإعلامي**: يتحدد دور المؤسسات الإعلامية التقليدية والمنصات التفاعلية الإلكترونية المعروفة على مستوى العالم في مسؤوليتها الاجتماعية والأخلاقية تجاه الترويج للقواعد المعرفية والتعليمية الأساسية للتربية الإعلامية، وما تستوجبه هذه

المنظومة من أدوات وإمكانيات تسهل على الدول والحكومات الحد على الأقل من الآثار السلبية لتكنولوجيات الإعلام والاتصال بشكل مكثف وتدريجي كفيل بتأطير الاستخدام العالي لمنصات الإعلام التفاعلي بوعي وعقلانية؛

- **الشق التشريعي:** سنت عدد من الدول الأوروبية قوانين خاصة بجرائم الأنترنيت والحاسوب مثل بريطانيا وهولندا وفرنسا والدنمارك والمجر وبولندا واليابان وكندا، كما اهتمت البلدان الغربية بإنشاء أقسام خاصة بمكافحة جرائم الأنترنيت، بل إنها خطت خطوة إلى الأمام وذلك بإنشاء مراكز لاستقبال ضحايا تلك الجرائم.

أما على مستوى الدول العربية فقد قامت الدول العربية بالتوقيع على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات وذلك بتاريخ 2010/12/21، كما أدت هذه الاتفاقية كذلك لميلاد قوانين عديدة لمكافحة ما يسمى بالجرائم الإلكترونية في السعودية والأردن وقطر والإمارات والعراق وسلطنة عمان. وصارت الاتفاقية سارية المفعول بعد تصديق الرئيس المصري عليها سنة 2015 ليكتمل نصاب الدول السبع المطلوبة لسريانها؛

أما في الجزائر فقد قام المشرع الجزائري بإصدار القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات، حيث تضمن في القسم السابع مكرر الخاص بالمساس بأنظمة المعالجة الآلية للمعطيات ثمان مواد (من المادة 394 مكرر إلى المادة 394 مكرر 7)، بالإضافة للقانون رقم 09-04 المؤرخ في 05 أوت 2009 والمتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها الذي تضمن مجموعة من التدابير الوقائية التي يمكن الأخذ بها من طرف مصالح معينة لتفادي وقوع جرائم

معلوماتية أو الكشف عنها وعن مرتكبيها في وقت مبكر، نجد أيضا قانون رقم 18-07 مؤرخ في 10 يونيو 2018 يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي بهدف حماية الحياة الخاصة للأفراد والحفاظ على حقوقهم وكرامتهم. كما أصدرت الجزائر القانون رقم 18-05 مؤرخ في 10 ماي 2018 يتعلق بالتجارة الإلكترونية حيث تضمن 50 مادة، وهو يحدد القواعد العامة والشروط المتعلقة بالتجارة الإلكترونية للسلع والخدمات من أجل تأطير مختلف المعاملات التجارية المختلفة المحلية والخارجية القائمة على الاتصال الإلكتروني. بالإضافة إلى القانون رقم 15-04 المؤرخ في 01 فيفري 2015 يحدد القواعد المتعلقة بالتوقيع والتصديق الإلكترونيين مبرزا ماهية وآليات إنشاء التوقيع الإلكتروني الموصوف والتحقق منه وكذا دور مختلف سلطات التصديق الإلكتروني[16]؛

- **الشق الأمني**: إن مواجهة مخاطر الجرائم المعلوماتية تعتمد بشكل كبير على تبني استراتيجية أمنية – مجتمعية متكاملة، والتي تعمل فيها أجهزة مكافحة الجريمة الرسمية في الدولة جنبا إلى جنب مع أفراد المجتمع ومؤسسات القطاع الخاص، هو ما يمكن من خلاله مكافحة الأنشطة الإجرامية في الفضاء الإلكتروني والتقليل من مخاطرها والحد من انتشارها، وهذه الرؤية تتسق مع نتائج الدراسات التي أجريت في بلدان مختلفة من العالم حول التعامل مع جرائم الأنترنيت، والتي أوضحت أهمية مشاركة العديد من المصادر والمؤسسات الخاصة في تحمل جزء من المسؤولية فيما يتعلق بمكافحة هذه الجرائم والسيطرة عليها وتلك المصادر تتمثل في[17]:

  - مزودو الخدمة الانترنيت الذين يملكون القدرة على تحديد ما يعرف بـ (IP) (Internet Protocol) للمشتركين، ما يتيح إمكانية مراقبة الأنشطة الخطرة على الأنترنيت وتقييد اشتراك المستخدمين المنخرطين في تلك الأنشطة؛

- المواطن العادي بدوره كذلك يمكن أن يساهم من خلال تحمل مسؤولية حماية نفسه من الوقوع ضحية لجرائم الأنترنيت باقتنائه برمجيات الحماية من الفيروسات؛
- المصارف التجارية وشركات البطاقات الائتمانية عليها أيضا مسؤولية كبيرة في حماية عملائها من خلال تطبيق إجراءات وقائية ضد الاحتيال، وكذلك تنصيب برمجيات مراقبة خاصة لتعقب النشاطات غير المعتادة على حسابات العملاء ووضع أنظمة لتنبيه العميل على كل عملية تتم على حسابه؛
- المحققين الخاصين الذين يعملون بالتنسيق مع أجهزة العدالة الجنائية يمكن أن يلعبوا دورا مهما في مكافحة جرائم الأنترنيت.

ثانيا: الإطار العام لحماية المستهلك الالكتروني

أدى ازدهار المعاملات التجارية عبر الوسائط الالكترونية إلى الرفع من المخاطر التي تواجه المستهلكين، نتيجة استخدام الوسائل التكنولوجية الحديثة بما تملكه من تقنيات فنية كوسيلة لإغرائهم، حيث تدفعهم للتعاقد دون دراية كافية بالمنتج أو الخدمة، وهو ما يستوجب توفير آليات لحمايتهم.

1- تعريف المستهلك:

يعتبر المستهلك العنصر الأساسي في العملية التسويقية، فعنده تبدأ عملية دراسة السوق وعنده تنتهي من خلال محاولتها كسب رضا هذا المستهلك، وبهذا فهو يعتبر العنصر الرئيسي الذي يحرك العملية ككل.

هو الطرف أو الشخص الأخير في العملية التجارية للسلعة أو للخدمة والتي تبدأ من منتجي السلع والخدمات مرورا بالوسطاء وصولا إلى المستهلك النهائي الذي يعتبر محور الأساسي لكل ما يتم إنتاجه وتسويقه[18].

تناول المشرع الجزائري تعريف المستهلك في المادة 03، الفقرة 01 من القانون رقم 09-03 المتعلق بحماية المستهلك على أنه: "كل شخص طبيعي أو معنوي يقتني بمقابل أو مجانا سلعة أو خدمة موجهة للاستعمال النهائي من أجل تلبية حاجته الشخصية أو تلبية حاجة شخص آخر أو حيوان متكفل به".[19]

أما المادة 03، الفقرة 02 من القانون رقم 04-02 المؤرخ في 23 يونيو 2004 والذي يحدد القواعد المطبقة على الممارسات التجارية، فقد عرفت المستهلك على أنه: "كل شخص طبيعي أو معنوي يقتني سلعا قدمت للبيع أو يستفيد من خدمات عرضت ومجردة من كل طابع مهني".[20]

وبالرجوع إلى المرسوم التنفيذي رقم 90-39 المؤرخ في 30 يناير 1990 المتعلق برقابة الجودة وقمع الغش، حيث عرف المستهلك في المادة 02، الفقرة 09 على أنه: "كل شخص يقتني بثمن أو مجانا، منتوجا أو خدمة معدين للاستعمال الوسيطي أو النهائي لسد حاجاته الشخصية أو حاجة شخص آخر أو حيوان يتكفل به".[21]

وبهذا يمكن تعريف المستهلك على أنه ذلك الشخص الذي يستهلك واحدا أو أكثر من السلع أو الخدمات لإشباع حاجاته ورغباته.

1-1- تعريف المستهلك الإلكتروني:

من أهم الآثار التي نتجت عن استخدام وسائل الاتصال الحديثة في التعاقد، ظهور ما يسمى بمصطلح "المستهلك الإلكتروني"، وهو مصطلح ظهر في الواقع العملي حديثا، ويعبر عن انعكاس وسيلة التعاقد على شخص مستخدمها.

عرف المستهلك الإلكتروني بأنه: "الشخص الطبيعي أو المعنوي، الذي يتزود بالسلع والخدمات أيا كان نوعها، ويتسلمها ماديا أو حكميا، أو بدون مقابل، لإشباع حاجاته الشخصية أو العائلية الخاصة أو العامة، مادام أنها لا تتعلق بأعمال مهنته، عبر شبكة الأنترنيت".[22]

وبالتالي يمكن تقديم تعريف المستهلك الإلكتروني على أنه: "كل من يقوم باستعمال السلع أو الخدمات لإشباع حاجاته وحاجات من يعولهم ولا يهدف إلى إعادة بيعها أو تحويلها أو استخدامها في نشاطه المهني، وأن يقوم بالتعاقد بشأن تلك السلع أو الخدمات بالوسائل الإلكترونية الحديثة"[23]

المستهلك الإلكتروني هو ذلك الشخص الذي يقوم بإبرام العقود الإلكترونية المختلفة من شراء وإيجار وقرض وانتفاع وغيرها، من أجل توفير كل ما يحتاجه من سلع وخدمات لإشباع حاجاته الشخصية أو العائلية دون أن يقصد من ذلك إعادة تسويقها ودون أن تتوافر له الخبرة الفنية لمعالجة هذه الأشياء وإصلاحها.[24]

وبالتالي فإن مفهوم المستهلك الإلكتروني لا يختلف كثيرا عن مفهومه في التعاقد بوسائل تقليدية سوى أنه يستخدم وسائل حديثة في التعاقد، فيعتبر مفهوما حديثا للتعاقد يحتل مركزا وسطا بين حاضرين والتعاقد بين غائبين.

والمستهلك الإلكتروني يتميز بالعديد من الخصائص أهمها:[25]

- قدرته في التعامل والتفاعل مع المواقع الإلكترونية المتاحة على شبكة الأنترنيت؛

- إشراك المستهلك الالكتروني في تصميم السلعة والخدمة، وذلك من خلال الموقع الإلكتروني للمؤسسة على شبكة الأنترنيت الذي يسمح له من تحديد المواصفات الخاصة بالسلع أو الخدمة التي يريد الحصول عليها، لأن المؤسسات الحالية تعتمد على آراء مستخدمي الأنترنيت سواء الحاليين أو المرتقبين لتعديل سلعها وخدماتها بما يتناسب مع حاجاتهم ورغباتهم وإمكانياتهم؛
- مرونته اتجاه المتغيرات المحيطة به بفضل التطورات الحاصلة في تكنولوجيا الإعلام والاتصال؛
- يتميز بقدرته على إجراء المقارنة بين السلع والخدمات واختيار ما يناسبه بفضل تكنولوجيا الإعلام والاتصال؛
- يتميز المستهلك الإلكتروني عن غيره من المستهلكين التقليديين بخبرته الواسعة في مجال استخدام شبكة الأنترنيت والإعلام الآلي.

2-1- حماية المستهلك الإلكتروني:

يقصد بالحماية الإلكترونية الحفاظ على حقوق المستهلك وحمايته من الغش أو الاحتيال أو شراء بضائع مغشوشة باستخدام الأدوات الإلكترونية التي تستطيع الوصول لكل مكان وتمارس تأثيرا يتجاوز أحيانا الأدوات التقليدية.

بالرجوع دائما إلى النصوص القانونية، فقد كرس المشرع الجزائري آليات وإجراءات حماية المستهلك عموما بوضع الضوابط والالتزامات التي يجب أن يتقيد بها الطرف الثاني من العقد (التاجر أو البائع)، وهذا من حيث إلزامية النظافة والنظافة الصحية للمواد الغذائية، إلزامية أمن ومطابقة المنتجات (الحماية من الأضرار)، إلزامية الضمان والخدمة ما بعد البيع، إلزامية إعلام المستهلك، الإعلام بالأسعار وشروط البيع، وكل ما يتعلق

بالممارسات التجارية (غير الشرعية، التدليسية، غير النزيهة)، وكذا الممارسات التعاقدية التعسفية.

وبالنظر إلى مجمل التعاريف التي جاءت ضمن القوانين والنصوص التشريعية للمستهلك وكذا الضوابط والإجراءات التي تتعلق أساسا بحماية حقوقه فهي تتناول المستهلك العادي، وبالتالي ما ينطبق عن هذا الأخير ينطبق على المعاملات الإلكترونية التي يقوم بها من خلال القنوات الإلكترونية. أي بعبارة أخرى، فإن المستهلك يتمتع بنفس الحماية القانونية التي يقررها المشرع للمستهلك العادي مع الأخذ بعين الاعتبار القواعد الخاصة المتعلقة بخصوصية العقد الإلكتروني كونه من العقود التي تبرم عن بعد عبر شبكة إلكترونية.

فضلا عما سبق، فتجد بعض النصوص الأخرى التي ترتبط بمعالجة الجريمة السيبرانية، أين يمكن أن يقع فيها المستهلك إما وعيا أو دون وعي أثناء قيامه بمختلف العمليات المالية والتجارية بشكل إلكتروني. وفي هذا الصدد نذكر بإيجاز بعض النصوص التشريعية التي وضعها المشرع الجزائري وإن كانت لا تعتبر كافية أو متضمنة لجميع الجوانب التي تساهم في حماية المستهلك، باعتبار أنها لم تتعرض للعديد من الجوانب التقنية المتعلقة بحماية المستهلك الإلكتروني، متمثلة في[26]:

- الدستور الجزائري (المادة 38، المادة 39)؛
- قانون رقم 2000-03 المؤرخ في 2000/08/05 المحدد للقواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية؛

- قانون رقم 04-15 المتمم للأمر 66-155 المتضمن قانون العقوبات تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات متضمنا لثمانية مواد من المادة 394 مكرر إلى 394 مكرر 7؛
- قانون رقم 08-01 المتعلق بالتأمينات وذلك في جانب استعمال البطاقة الإلكترونية للمؤمنين (بطاقة الشفاء) والمعلومات التي تحتويها؛
- قانون رقم 09-04 المؤرخ في 05 أوت 2009، يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها؛
- القانون رقم 15-04 المؤرخ في 01 فيفري 2015 يحدد القواعد المتعلقة بالتوقيع والتصديق الإلكترونيين مبرزا ماهية وآليات إنشاء التوقيع الإلكتروني الموصوف والتحقق منه وكذا دور مختلف سلطات التصديق الإلكتروني؛
- رقم 18-07 مؤرخ في 10 جوان 2018 يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي بهدف حماية الحياة الخاصة للأفراد والحفاظ على حقوقهم وكرامتهم؛
- القانون رقم 18-05 مؤرخ في 10 ماي 2018 يتعلق بالتجارة الإلكترونية يحدد القواعد العامة والشروط المتعلقة بالتجارة الإلكترونية للسلع والخدمات من أجل تأطير مختلف المعاملات التجارية المختلفة المحلية والخارجية القائمة على الاتصال الإلكتروني.
- قانون الإجراءات الجزائية.

2-مبررات حماية المستهلك الإلكتروني:

تتمثل أهم مبررات حماية المستهلك الإلكتروني فيما يلي:[27]

- **حاجة المستهلك إلى الخدمات الإلكترونية:** إن التطور الحاصل في شبكة الإنترنيت أدى إلى الاهتمام بالمواقع التجارية التي تحتوي على خدمات متعددة كالخدمات العقارية والسياحية والمصرفية وغيرها من الخدمات الأخرى المهمة، وحاجة المستهلك الضرورية إلى الخدمات الإلكترونية تنبع من كونها توفر منتجات وخدمات ذات جودة عالية بأسعار معقولة بسبب كثرة المواقع الإلكترونية التجارية وزيادة المنافسة بين هذه المواقع على تقديم الأفضل للمستهلك بالإضافة إلى الخدمات الممتازة لعمليات ما بعد البيع فأهمية الخدمات الإلكترونية الموجودة على شبكة الإنترنيت تزيد من إقبال المستهلكين فهي محور طلب الكثير من المستهلكين، ومن هنا كانت الحاجة للبحث عن الحماية للمستهلك بشكل ملح وواضح؛
- **التطور الحديث في شبكة الأنترنيت:** ظهرت العديد من التقنيات والأدوات التي ساهمت في تطوير عالم الأنترنيت مما جعلها من أحدث الخدمات التقنية التي تعتمد على تفاعل المستهلك مع جهاز الحاسوب، فمن خلالها يمكن الوصول إلى العديد من السلع والخدمات بطريقة سهلة، ويمثل التطور التقني في هذا الجانب واقعا علميا يأتي بتطورات مستمرة، مما ينبغي أن يقود إلى تحسين الروابط التجارية بين المزود والمستهلك بهدف الحصول على أفضل أداء للممارسات التجارية الإلكترونية؛
- **افتقار المستهلك إلى التنوير المعلوماتي التقني:** تعتبر شبكة الأنترنيت المنتشرة حول العالم نافذة مفتوحة أمام الملايين من الناس، فالبريد الإلكتروني ومواقع الأنترنيت والتفاعل المباشر تتلخص جميعها في هدف واحد وهو ما عرض أنواعا متباينة من المنتجات والخدمات للمستهلك والتعاقد معه من خلالها.

فقدرة المستهلك على التعامل مع جهاز الحاسوب وشبكة الأنترنيت تسهل عليه الوصول إلى المنتجات والخدمات التي يريدها، وهنا يجب أن نفرق بين ما يسمى بإعلام المستهلك والذي هو حق من حقوق المستهلك وبين معرفة المستهلك المعلوماتية بشبكة الأنترنيت، والتي تمثل أدنى حد من أجل وصول المستهلك إلى معلومات عن الخدمات والمنتجات، فالحد الأدنى يعبر عن قدرة المستهلك على التعامل مع جهاز الحاسوب وشبكة الأنترنيت، فافتقار المستهلك للثقافة المعلوماتية يعني عدم توفر الحد الأدنى من القدرة على التعامل خلال هذه الشبكة، بالإضافة إلى المشاكل التي تواجهه عند التعمق في هذه الشبكة قد يؤدي إلى وقوع المستهلك بحيل وخداع قراصنة الأنترنيت من خلال المواقع الوهمية أو التعاقد الوهمي.

3-أهداف حماية المستهلك الإلكتروني:

من أهم هذه الأهداف نجد ما يلي:[28]

- التكفل بحماية المستهلكين من أساليب الغش والخداع الممارس عليهم من طرف المنتجين أو الوسطاء أثناء إتمام عمليات التبادل في إطار العمليات البيعية؛
- الالتزام بضمان الحقوق المختلفة للمستهلكين، وحمايتهم من مختلف أشكال وصور التلاعب الممكن حدوثه في السلع والخدمات التي يحتاجونها ويرغبون فيها،
- تأمين وتقديم المساعدة الممكنة لفئات الدخل المحدود، وتمكينهم من الحصول على السلع والخدمات التي يحتاجونها؛
- تفعيل التنسيق والتعاون مع منظمات الأعمال من أجل تمكينها من المعلومات التي تخص المستهلكين، والتي قد لا تتاح لتلك المنظمات نظرا لضعف قدراتها في الاتصال.

4-مبادئ حماية المستهلك الإلكتروني:

وضعت الأمم المتحدة العديد من المبادئ التي على أساسها تتحقق أطر لحماية المستهلك بما يتوافق مع عالمية شبكة الأنترنيت والمتجلية في:[29]

- **تحقيق العدالة والمناصفة:** يجب أن تتصرف المؤسسات الناشطة في الفضاء الافتراضي بصدق وأن تسعى إلى تحقيق ولاء اتجاه جميع مستهلكيها على طول مرحلة العلاقة معهم، لاسيما مع المستهلكين الضعفاء والمحرومين وأن تعمل على دمج هذه القواعد في ثقافتها المؤسسية؛
- **القيام بممارسات تجارية شريفة:** يجب على المؤسسات الناشطة في الفضاء الافتراضي الامتناع عن الممارسات التجارية غير القانونية وغير الأخلاقية أو التمييزية أو المضللة، مثل تقنيات البيع المسيئة أو أي سلوك غير لائق مضر لا مبرر له اتجاه المستهلكين؛
- **التواصل والشفافية:** يجب على المؤسسات تقديم معلومات كاملة ودقيقة وغير خادعة عن المنتجات، خاصة ما تعلق بشروط ورسوم البيع لمساعدة المستهلكين على اتخاذ قرارات مستنيرة، وينبغي أن تكفل سهولة الوصول إلى هذه المعلومات ولاسيما المتعلقة بالأحكام والشروط الرئيسية، مهما كان مستوى التكنولوجيا المستخدم في ذلك؛
- **التعليم والتوعية:** ينبغي على المؤسسات أن تضع عند الاقتضاء برامج وأجهزة تساعد المستهلكين على اكتساب المعارف والمهارات اللازمة لفهم المخاطر التي تنطوي عليها العمليات الإلكترونية، خاصة المخاطر الإلكترونية المرتبطة بعملية الدفع مع تقديم المشورة والمساعدة المهنية في ذلك؛

- **حماية الخصوصية:** ينبغي على المؤسسات أن تحمي خصوصية المستهلكين من خلال مجموعة من آليات المراقبة والأمن والشفافية مع استشارة الموافقة فيما يخص جمع واستخدام بياناتهم الشخصية؛
- **الشكاوى والتقاضي:** ينبغي على المؤسسات الناشطة في الفضاء الإلكتروني أن توفر آلية للشكاوى تكفل حل نزاعاتها بصورة عادلة وشفافة وغير مكلفة وفي الوقت المناسب بكفاءة ودون تكبد تكاليف، مع العمل على حل النزاعات بالطرق الودية والسعي الدائم إلى تحقيق رضا العملاء.

ثالثا: المخاطر التي يتعرض لها المستهلك الالكتروني في ظل الجرائم السيبرانية ووسائل حمايته منها:

1- المخاطر التي يتعرض لها المستهلك الإلكتروني في ظل الجرائم السيبرانية:

إن حاجة المستهلك إلى السلع والخدمات الضرورية التي تقدم عبر شبكة الانترنيت (كالخدمات السياحية، والمصرفية والتأمين، وبيع تذاكر الطيران والحجز في الفنادق وغيرها)، تدفعه إلى الإقبال عليها وإبرام التصرفات من خلال شبكة الإنترنيت، وغالبا ما يفتقد المستهلك إلى الخبرة والدراية والمعرفة في مجال تقنية تكنولوجيا المعلومات – لاسيما شبكة الانترنيت–، الأمر الذي يدفعه إلى الدخول في علاقات من خلال مواقع إلكترونية وهمية وبالتالي تعرضه لجملة من المخاطر والتي تأخذ أشكالا متعددة ومتنوعة وقد يكون الغرض منها تخريب البيانات أو الاطلاع على المعلومات الشخصية للأفراد، إلا أن هذه المخاطر أو الجرائم التي يتعرض لها المستهلك الإلكتروني هدفها واحد وهو الاستيلاء على الأموال. ومن بين هذه المخاطر نذكر على سبيل المثال:[30]

- **عمليات القرصنة:** والتي يقوم بها مجرمون غير مرئيون سواء كان من طرف الكراكرز (Crackers) الذين يقومون بخرق المواقع الالكترونية وسرقة المعلومات

الشخصية والحسابات المالية، أو من طرف الهاكرز (Hackers) وهم أشخاص متسللون يتابعون عن كثب آخر الأخبار وبرامج الحماية الأمنية والمعلومات إلى حد أنهم ينشؤون النوادي لتبادل المعلومات. وهؤلاء المجرمون يستطيعون الاجتياز الأمني لمختلف المواقع بقصد التخريب والاختلاس والتزوير؛

- **الخداع والاحتيال:** وذلك عن طريق فتح مواقع تجارية على الشبكة تكون وهمية تحمل كل الصفات التي تجذب المستهلك كالتخفيضات والخصومات على السلع التي تكون وهمية؛
- **استخدام الأسماء والعلامات التجارية المشابهة:** بعض المواقع الالكترونية تقوم بتقليد العلامات التجارية المشهورة على الشبكة بغرض جذب المستهلك والاحتيال عليه؛
- **طلب شراء السلع عبر الاحتيال:** وهو أحد أهم أشكال التطور في نشاط مجرمي الانترنيت ويتمثل في شحن البضائع الالكترونية والسلع الفاخرة المشتراة ببطاقات الائتمان المسروقة من مستهلك ما، إلى بلاد بعيدة عن محيط السرقة، حيث يحصل المجرمون على هذه السلع بأسعار أقل داخل الولايات المتحدة وأوروبا على سبيل المثال، ثم يقومون بشحنها إلى الخارج بأسعار أعلى بقليل من قيمتها الحقيقية، بعد ذلك تتحول البضاعة إلى نقود يتم تقاسمها بين المحتالين؛
- **الاحتيال على المستهلك في المزادات:** ترافق ظهور المزادات على الانترنيت بكثير من الأخطار والممارسات الاحتيالية من قبل المشتري والبائع على حد سواء، في بعض الحالات يسلم بدائل أقل جودة، وفي بعض الحالات يستلم البائع مستحقاته المالية بينما لا يتمكن من تسليم بضاعته فيما لا يتمكن من دفع مقابلها، هنالك

نمط آخر من أنماط الاحتيال في المزادات ويتم ذلك بعمل عدد من العطاءات الوهمية بهدف رفع سعر السلعة المعروضة للبيع وبالتالي خداع المستهلك وغشه في السعر؛

- **خطر سرقة بيانات البطاقة الائتمانية للمستهلك:** قد يتم الحصول على أرقام بطاقة الائتمان الخاصة بالغير بسرقة البطاقة ذاتها أو سرقة بياناتها خارج الوسط الالكتروني (سرقة تقليدية)، وقد يتم الحصول على تلك البيانات عبر الوسط الالكتروني أي الانترنيت وذلك بأحد الأساليب (التجسس، الخداع، أو تفجير الموقع)، ثم يقوم الجاني باستخدام بيانات البطاقة المملوكة للغير في شراء سلع أو خدمات عبر الانترنيت.

إضافة إلى:

- **القصور الوظيفي لأداة الدفع الإلكترونية:** ويقصد به ما قد يطرأ على أداة الدفع الإلكترونية من أعطال عرضية نتيجة اختلالات مادية أو كهربائية، أو قصور في أوامر التشغيل المرتبطة بلغة البرمجة الخاصة بتلك الأداة أو قصور في عملية الصيانة والتي يترتب عليها انحراف في سلوك أداة الدفع، وقصور في أداء وظائفها الأساسية كعدم دقة المدفوعات التي تتم من خلالها...؛
- **فقدان أداة الدفع الالكتروني:** كغيرها من الأشياء ولكونها في حيازة المستهلك، فقد تتعرض لمخاطر الفقد أو الضياع وقد يكون ذلك نتيجة لسهو أو إهمال الحامل ودون تدخل الغير أو بتدخل هذا الأخير ويكون ذلك نتيجة لعملية السرقة.

2- وسائل حماية المستهلك الالكتروني في ظل مخاطر الجرائم السيبرانية:

أصبحت مسألة حماية المستهلك الإلكتروني من المسائل الهامة، وخاصة في ظل الاقتصاد الرقمي حيث يكون المستهلك أكثر عرضة للتلاعب بمصالحه وعرضة لمختلف

الأخطار بصفة مستمرة فهؤلاء القراصنة والمخربين يسعون دائما إلى إيجاد وسائل وتقنيات جديدة من أجل استخدامها في إجراء عملياتهم التخريبية والتدميرية فكلما وجدت وسيلة لمحاربة مختلف الأخطار يقوم هؤلاء القراصنة بابتكار طرق جديدة أخرى أكثر خطورة وأكثر مكرا من التي قبلها، ولهذا فإن أمن وحماية المستهلك الإلكتروني يعد من القضايا المهمة والضرورية جدا لنجاح مشروع الاقتصاد الرقمي ومختلف تطبيقاته ومن بين أهم الوسائل والأنظمة المستخدمة في تأمين المعاملات التي يفرضها الاقتصاد الرقمي نذكر منها على سبيل المثال:

1-2- الوسائل الإدارية لحماية المستهلك الإلكتروني:

على الإدارة العليا القيام بعدة مهام تجاه أمن المعلومات كالرقابة والإشراف على أمن المعلومات وسنستعرض مهاما رئيسية يجب عليها القيام بها كالتالي:[31]

- **السياسة الأمنية المثقفة:** تعتبر تقنية النص التشعبي المعروفة لدى مصممي صفحات الويب من بين الطرائق الممكنة لتحقيق أمن المعلومات الإلكترونية، لدى استعمال هذه الطريقة تكتب في أول صفحتين عرضا موجزا عن المبادئ الأمنية الهامة ومعايير الحماية، ونضمن فيهما ارتباطات تهدف لإعطاء المزيد من التفاصيل؛
- توفير أمن الأجهزة: لتأمين الأجهزة لابد من تأمين المبنى كعدم السماح لغير المصرح لهم بالدخول إلى غرف الحاسب الآلي، ومخزن وسائط التخزين. ويفضل استخدام التكنولوجيا الحديثة للدخول على الأنظمة (بصمة الأصبع، بصمة العين، البطاقة الممغنطة...)؛
- **توفير أمن البيانات:** ويكون ذلك بتوزيع الصلاحيات والمسؤوليات حسب الهيكل التنظيمي بما يضمن رفع المستوى الأمني، وتقليص الجرائم، ووضع آلية يتم من

خلالها النسخ الاحتياطي وتأمين وسائط الحفظ الخارجية بما يكفل أمنها وتحديثها، ويجب صياغة الضوابط المنظمة لعمليات التشغيل، ولمبرمجي قواعد البيانات ومدرائها، ولإدارة الشبكات وخطوط الاتصال، ولعمليات الإدخال والإخراج، والضوابط الأمنية لبناء وتشغيل البرامج التطبيقية؛

- **توفير أمن الأفراد**: ويكون ذلك باتباع:

منع التوظيف المؤقت نهائيا، ومراعاة إجراءات إنهاء خدمة الموظف بطلب تسليم كل ما كان بحوزته كالمفاتيح والبطاقات الممغنطة، وتغيير كلمة المرور قبل مغادرته؛ متابعة العاملين ونقلهم إجباريا بين الأقسام المختلفة والإدارة، وملاحظة الذين لا يطلبون إجازة بإجبارهم على الإجازة ومراقبة النظام بعد ذلك للتأكد من عدم وجود خلل كانوا يتفادونه بوجودهم؛

عقد ندوات ومؤتمرات ومحاضرات بشكل دوري في مجال المعلومات؛

دفع العاملين لحضور المعارض العالمية للأجهزة والبرامج، وإرسالهم إلى الدورات المتخصصة بأمن المعلومات؛

منح الحوافز وربط الترقية والدورات بمدى التقيد بأمن المعلومات.

- **توفير قسم متخصص بأمن المعلومات**: تقوم المؤسسات الكبيرة بتعيين مدير أمن نظم المعلومات يرتبط بالإدارة العليا مباشرة لأهمية التقارير التي يعدها، ويرأس مدير الأمن قسما مستقلا من المتخصصين في مجال أمن المعلومات ومن ذوي الخبرة الفنية والأمنية في معالجة البيانات والبرمجة حسب نظم التشغيل ولغات البرمجة وقواعد البيانات المستخدمة في المؤسسة، ومدربين على التنسيق الأمني ولديهم المقدرة الكافية للتعامل مع جرائم المعلومات التي تطال زبائنها والحالات الطارئة؛

- **التصريح بالمرور عبر الشبكة:** تتميز السياسة الأمنية الجيدة بقدرتها على تنظيم المرور عبر شبكة الاتصال من خلال قبول أو رفض بعض الملفات على الشبكة.

2-2- الوسائل التقنية لحماية المستهلك الإلكتروني:

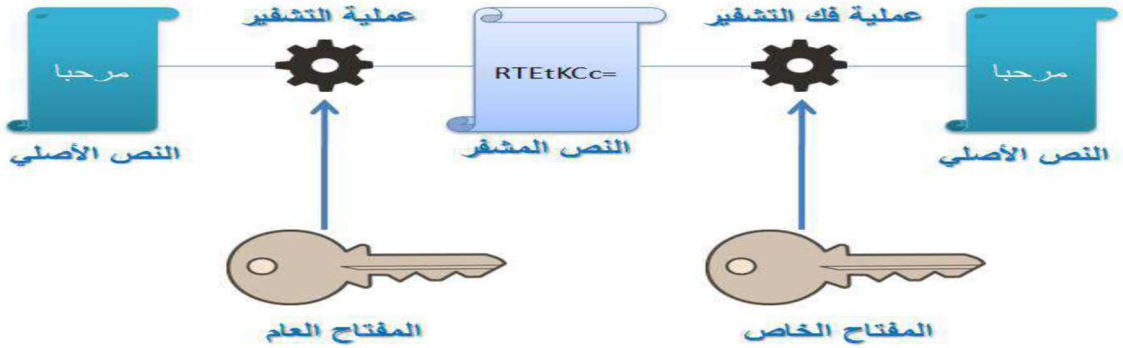
وتتمثل في مجموعة من الإجراءات الفنية التي تتبعها مختلف المؤسسات لحماية معلوماتها وزبائنها، أهمها:[32]

- **تقنية طبقة الفتحات الآمنة (SSL):** طورت هذه التقنية من طرف شركة نت سكيب التي ساعدت على زيادة الثقة في مختلف تطبيقات الاقتصاد الرقمي خاصة التجارة الالكترونية ومستوى الأمان فيها مما جعلها أساس التجارة الإلكترونية في العالم حيث قامت معظم الشركات المنتجة لمتصفحات الانترنيت بالأخذ بها وتزويد متصفحاتها بهذه التقنية. و(SSL) هو برنامج يحتوي على بروتوكول تشفير متخصص لنقل البيانات والمعلومات المشفرة بين جهازين عبر شبكة الانترنيت بطريقة آمنة بحيث لا يمكن قراءتها إلا من طرف المرسل والمستقبل (البائع والمشتري).
- **الحركات المالية الآمنة (SET):** استخدم هذا البروتوكول في أول عملية تبادل مالي سنة 1997 في الولايات المتحدة الأمريكية، ويشبه إلى حد كبير بروتوكول الطبقات الأمنية في استناده إلى التشفير والتوقيعات الرقمية، كما يستخدم هذا البروتوكول برمجيات المحفظة الإلكترونية حيث تحتوي على رقم حامل البطاقة والشهادة الرقمية التابعة له كذلك فإنه يحصل على شهادة رقمية صادرة من أحد البنوك الذي يعتمدها، وعند إجراء الحركات المالية عبر الانترنيت فإن كلا من

التاجر وحامل البطاقة والشهادة الرقمية لكل منهما مما يتيح التحقق من هوية الآخر؛

- **التشفير الإلكتروني**: يعرف التشفير بأنه تحويل المعلومات إلى شفرات غير مفهومة (دون معنى) لمنع الأشخاص غير المرخص لهم من الاطلاع على المعلومات، إذن فعملية التشفير تعمل على تحويل النصوص العادية إلى نصوص مشفرة وذلك باستخدام مفاتيح وهذه المفاتيح تستند إلى صيغ رياضية معقدة (خوارزميات) وتعتمد قوة وفعالية التشفير على أساسين: الخوارزمية وطول المفتاح (مقدار بالت Bits)؛ والشكل التالي يوضح مخطط التشفير الإلكتروني:

شكل رقم (01): مخطط التشفير الإلكتروني



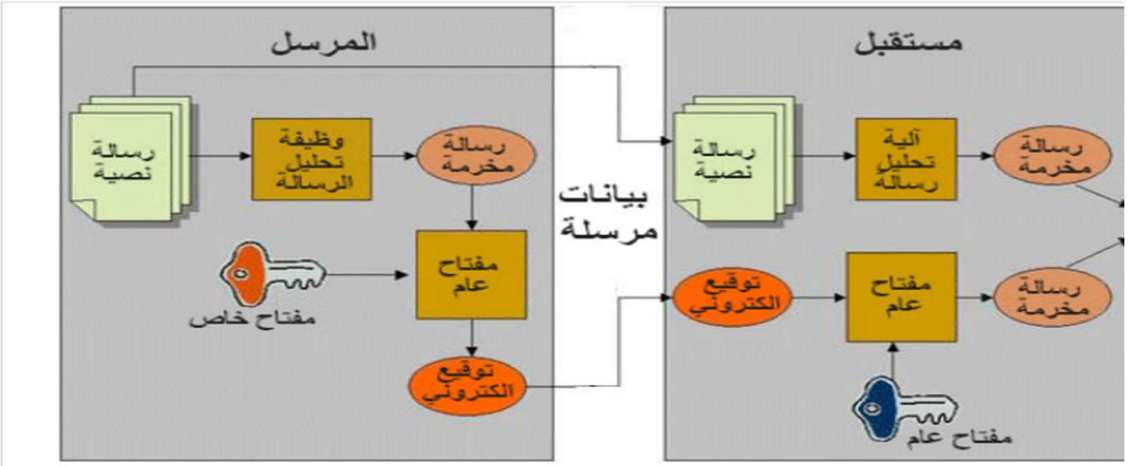
Source : http://anshrnow.com/article/60, consulté le 28/11/2021.

- **البصمة الإلكترونية**: هي بصمة رقمية يتم اشتقاقها وفق خوارزميات معينة تدعى دوال أو اقترانات التمويه تقوم هذه الخوارزميات بتطبيق حسابات رياضية على الرسالة لتوليد بصمة (رسالة صغيرة) تمثل ملف كامل أو رسالة (سلسلة كبيرة) وتتكون البصمة الإلكترونية للرسالة من بيانات لها طول ثابت (بين 128 و160 Bits) تؤخذ من الرسالة المحولة ذات الطول المتغير، وتتميز البصمات عن بعضها

البعض بحسب المفاتيح الخاصة التي أنشأتها والتي لا يمكن فك شيفرتها إلا باستخدام المفتاح العام؛

- **التوقيع الإلكتروني**: يجعل التوقيع الإلكتروني تحويل المعاملات أكثر أمنا وسرية فهو بمثابة ختم الهوية التي تلازم الرسالة عبر الانترنيت. وهو يستخدم من أجل التأكد من أن الرسالة قد جاءت من مصدرها دون التعرض لأي تغيير أثناء عملية النقل، بحيث يستخدم المرسل المفتاح الخاص لتوقيع الوثيقة الكترونيا أما المستقبل فيتحقق من صحة التوقيع عن طريق المفتاح العام والشكل التالي يوضح آلية عمل التوقيع الإلكتروني:

شكل رقم (02): آلية عمل التوقيع الإلكتروني



Source : http://tfig.itcilo.org/AR/contents/e-signature.htm, consulté le 26/11/2021.

- **الشهادة الإلكترونية**: وهي عبارة عن وثائق إلكترونية تثبت هوية المستخدمين عبر شبكة الانترنيت ويتولى إصدار هذه الشهادات جهة موثوق فيها يسمى سلطة

إصدار الشهادات، تحتوي كل شهادة رقمية يتم إصدارها على معلومات مهمة تتعلق بمالكها وبالسلطة التي أصدرت هذه الشهادة.

- **الجدران النارية:** تعتبر الجدران النارية وسيلة تستعمل لحماية الشبكات الخاصة من الدخول وتمنع الوصول غير المشروع للشبكة، حيث تحمي وحدات التحكم والإرسال في الأنترنيت، وتتجلى أهمية الجدران النارية في حماية الشبكات الخاصة من هذه المشكلات؛
- **استخدام المواقع الوسيطة:** أشهرها موقع PayPal الذي أنشأ سنة 1998، وهو تابع لشركة أمريكية مسجلة في كاليفورنيا، يقوم بتحويل المال عبر الحسابات المختلفة، وقامت بشرائه شركة (ebay) عام 2020 من أجل تسهيل عملية التبادل التجاري الخاصة بها، حيث يتميز ببساطة التعامل به وسهولة انتقال المال. كما يعد الرائد عالميا في مجال حلول الدفع عبر الأنترنيت مع أكثر من 169 مليون حساب في جميع أنحاء العالم، حيث يوفر خدماته في 203 سوقا و26 عملة في جميع أنحاء العالم مما أهله لأن يكون دعامة قوية للتجارة الإلكترونية العالمية من خلال إتاحة خيارات الدفع عبر المواقع والعملات واللغات المختلفة.

3-2- الوسائل القانونية لحماية المستهلك الالكتروني:

إن نجاح المعاملات الإلكترونية في أي بلد ما يتطلب بناء ثقة المستهلكين والتجار ومؤسسات الأعمال بهذا النمط من المعاملات، كما أن المخاطر التي تهدد المستهلك والمتمثلة في الجرائم الإلكترونية أو الافتراضية التي تتخطى الحدود والأماكن الجغرافية يعد أكبر تهديد لهذه الثقة.

وبالتالي أصبح لابد من إيجاد بيئة قانونية مضبوطة كي تضمن حماية حقوق ومصالح كل أطرافها المتعاملين فيها، وليس يجدي نفعا الاكتفاء بتضمين القوانين التقليدية

بمجموعة نصوص إضافية وإدخال تعديلات بقدر ما يكون الحل الأنفع هو الاجتهاد في وضع قانون مستقل للمعاملات التي تخص تطبيقات هذه الاقتصاد الجديد وتوفر الحماية الكافية للمستهلك الالكتروني في ظل هذا النمط من المعاملات.

وبالتالي فإن توفير الحماية للمستهلك الالكتروني في الدول تعتبر مرجعا تشريعيا مهما في شتى المجالات وهذا يعكس التطور التكنولوجي والاجتماعي الذي تحظى به، ولما كانت التعاقدات الإلكترونية تتم في الغالب على المستوى الدولي، وجب العمل على وضع الوسائل القانونية المناسبة من أجل الحماية الدولية للمستهلك، ولذلك أصدر المجلس الأوربي توجيهين في هذا الشأن، التوجيه الأول ونص فيه على ضرورة عمل المؤتمرات الدولية للمعاملات التجارية الإلكترونية وخاصة فيما يتعلق بالمعاملات التجارية الإلكترونية التي تتم خارج أوروبا، كما صدر التوجيه الثاني بشأن القواعد التي تحدد ما هي المحكمة التي الأفضل للمستهلك، وبصفة خاصة في ظل معاهدة روما الصادرة في 19 جويلية 1980، كما صدر التوجيه الأوروبي بشأن حماية المستهلك من الشروط التعسفية التي تفرض عليه من جانب البائع[33].

وتعتبر الجزائر من بين الدول التي سعت ومازالت تسعى بتبني نصوص تشريعية وقوانين خاصة بالحماية القانونية من المخاطر والجرائم الالكترونية التي تمسها إلا أن هذه المساعي غير كافية حاليا لتوفير الحماية القانونية المثلى للمستهلك الإلكتروني، ومن أبرز القوانين نذكر على سبيل المثال القانون رقم 09-04 المؤرخ في 14 شعبان 1430 هـ الموافق لـ 05 أوت 2009 والمتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها والذي نص في المادة الأولى منه على: أن الهدف الذي

وضع من أجله هو وضع قواعد خاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.[34]

خاتمة:

في خضم التطور العلمي والتقني الذي مس شتى المجالات، بات من الضروري حماية المستهلك الإلكتروني في ظل المعاملات الإلكترونية التي أصبحت هدفا ومقصدا للاستغلال من طرف العديد من مرتكبي الجرائم الإلكترونية أو ما يعرف بالجرائم السيبرانية، وعلى إثر ذلك فقد أصبح من الضروري تفعيل آليات ووسائل لتعزيز حماية المستهلك الإلكتروني من هذه المعاملات سواء كان على المستوى المحلي أو الدولي عن طريق توعية المستهلك أو سن القوانين والتشريعات التي تتكفل بحمايته.

التوصيات والاقتراحات:

- تفعيل نوع من الرقابة على مختلف العمليات والاتفاقيات الإلكترونية لحماية المستهلك؛
- سن القوانين والتشريعات التي تنظم نشاط التجارة والمعاملات الإلكترونية على المستوى الدولي، وأمن المعاملات التجارية والمدفوعات بما يعزز من حماية المستهلك الإلكتروني من مختلف أنماط الاحتيال والاختراق والغش الإلكتروني؛
- الاستعانة بالمواقع الوسيطة في المعاملات الإلكترونية فهي تضمن عدم ضياع أموال المستهلك عند تعرضه للاحتيال وتضمن سرية معلومات بطاقته الإلكترونية؛

- الحرص على تكوين كفاءات من القطاع الأمني متخصصة في مراقبة التجاوزات والكشف المبكر عن الجرائم الإلكترونية خاصة وأنها جرائم غير مادية ولا ملموسة ونادرا ما يتم الكشف عنها في مراحل متقدمة من ارتكابها؛
- حرص المستهلك الإلكتروني على اختيار مواقع مؤمنة ومحميين وتجار الكترونيين ذوي سمعة جيدة؛
- توحيد النظام القانوني الدولي بهدف التنسيق بين المراكز القانونية للمتعاقدين واتساع نطاق الحماية القانونية للمستهلك الإلكتروني وكذا مكافحة الجرائم السيبرانية؛
- العمل على توفير الحماية التقنية مع تعزيزها بالحماية القانونية لمواجهة المخاطر المتعلقة بالمعاملات الإلكترونية وتكنولوجيا الإعلام والاتصال؛
- تحديث القوانين والتشريعات بما يتناسب والجرائم الحديثة في المجال الإلكتروني التي تهدد مال المستهلك وصحته.

الهوامـــش:

[1] منال زهرة هلال، **تكنولوجيا الاتصال والمعلومات**، الطبعة الأولى، درا أسامة، الأردن، 2014، ص 374.

[2] Romain Beas, **La lutte contre la cybercriminalité au regard de l'action des états**, Doctorat de droit privé et sciences criminelles, Faculté de Droit, Université de Lorraine, Paris, 2016, pp 25 – 26.

[3] روان بنت عطية الله الصحفي، **الجرائم السيبرانية**، المجلة الإلكترونية الشاملة متعددة التخصصات، العدد 24، بدون بلد نشر، ماي 2020، ص 08.

[4] محمود أحمد القرعان، الجرائم الإلكترونية، الطبعة الأولى، دار وائل للنشر والتوزيع، عمان، 2017، ص 19.

[5] الطيب عيساوي وهشام شكاردة، **التربية الإعلامية كآلية للحد من الجريمة السيبرانية على شبكة الأنترنيت**، المجلة الجزائرية للأبحاث والدراسات، المجلد 03، العدد 04، جامعة محمد الصديق بن يحي، جيجل، الجزائر، سبتمبر 2020، ص 76.

[6] كركوري مباركة حنان، **خصوصية ارتكاب الجريمة السيبرانية في النظام المعلوماتي –دراسة تحليلية على ضوء القانون الجزائري–**، مجلة الدراسات الإستراتيجية والعسكرية، المجلد 02، العدد 08، المركز الديمقراطي العربي، برلين، ألمانيا، سبتمبر 2020، ص 12.

[7] المادة 02 من القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، عدد 47، مؤرخة في 16 أوت 2009، ص 05.

[8] عبد الرحمن جميل محمود حسين، **الحماية القانونية لبرامج الحاسب الآلي**، مذكرة ماجستير (غير منشورة)، كلية الدراسات العليا، جامعة النجاح الوطنية، نابلس، فلسطين، 2008، ص 09.

[9] نبيل دريس، الجريمة السيبرانية بين المفاهيم والنصوص التشريعية –الجزائر نموذجا–، مجلة القانون والمجتمع، المجلد 05، العدد 02، جامعة أحمد دراية، أدرار، الجزائر، 2017، ص ص 31، 32.

[10] حكيمة جاب الله، **انعكاسات الجريمة السيبرانية على البيئة الرقمية: دراسة في آليات واستراتيجيات مكافحتها**، حوليات جامعة الجزائر 1، المجلد 35، العدد 03، جامعة بن يوسف بن خدة، الجزائر، 2021، ص 653.

[11] حفوظة الأمير عبد القادر وغرداين حسام، **الجريمة الإلكترونية وآليات التصدي لها**، الملتقى الوطني حول آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، الجزائر، 29 مارس 2017، ص ص 93، 94.

[12] يونس عرب، **تطور التشريعات في مجال مكافحة الجرائم الإلكترونية**، هيئة تنظيم الاتصالات، سلطنة عمان، مسقط، 02 و04 أفريل 2006، متاح على الرابط:
https://www.a7wallaw.com/10807, consulté le : 25/11/2021.

[13] نمديلي رحمة، **خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة**، المؤتمر الدولي الرابع عشر حول الجرائم الإلكترونية، طرابلس، يومي 24 و25 مارس 2017، ص ص 11 – 12.

[14] صراع كريمة ودقيش جمال، **الأبعاد الاقتصادية للجريمة الإلكترونية**، مجلة الدراسات التسويقية وإدارة الأعمال، المجلد 02، العدد 01، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة طاهري محمد، بشار، الجزائر، جانفي 2018، ص 38.

[15] الطيب عيساوي وهشام شكاردة، مرجع سبق ذكره، ص 81.

[16] حكيمة جاب الله، مرجع سبق ذكره، ص ص 659 – 660.

[17] الطيب عيساوي وهشام شكاردة، مرجع سبق ذكره، ص 81.

[18] بن يعقوب الطاهر، **دور سلوك المستهلك في تحسين القرارات التسويقية**، مجلة العلوم الإنسانية، المجلد 04، العدد 06، جامعة محمد خيضر، بسكرة، الجزائر، جوان 2004، ص 06.

[19] المادة 03 من القانون رقم 09-03 المؤرخ في 25 فبراير 2009 المتعلق بحماية المستهلك وقمع الغش، الجريدة الرسمية، العدد 15، المؤرخة في 2009/03/08، ص 13.

[20] المادة 03، الفقرة 02 من القانون رقم 04-02 المؤرخ في 23 حوان 2004 المحدد للقواعد المطبقة على الممارسات التجارية، الجريدة الرسمية، العدد 41، المؤرخة في 2004/06/27، ص 04.

[21] المرسوم التنفيذي رقم 90-39 المؤرخ في 30 جانفي 1990 يتعلق برقابة الجودة وقمع الغش، الجريدة الرسمية، العدد 05، المؤرخة في 1990/01/31، ص 203.

[22] محمد محمد حسن الحسني، **حماية المستهلك الإلكتروني في القانون الدولي الخاص**، الطبعة الأولى، دار النهضة العربية للنشر والتوزيع، القاهرة، مصر، 2013، ص 35.

[23] شمس الدين التجاني ومحمد يوسف عمامرة، **واقع المستهلك الجزائري في ظل استخدام تكنولوجيا المعلومات والاتصال – مقومات وواقع القطاع ودوره في حماية المستهلك–**، الملتقى الوطني الثالث حول المستهلك والاقتصاد الرقمي –ضرورة الانتقال وتحديات الحماية–، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، المركز الجامعي عبد الحفيظ بوصوف، ميلة، الجزائر، يومي 23 و24 أفريل 2018، ص 1204.

[24] أسامة أحمد بدر، **حماية المستهلك في التعاقد الإلكتروني**، دار الجامعة الجديدة للنشر، مصر، 2005، ص 108.

[25] محمد بن ذهيبة وآخرون، **مخاطر الدفع الإلكتروني عبر الأنترنيت التي يتعرض لها المستهلك الإلكتروني واستراتيجية الجزائر لحمايته –مشروع التصديق والتوقيع الإلكترونيين**، الملتقى الوطني الثالث حول المستهلك والاقتصاد الرقمي –ضرورة الانتقال وتحديات الحماية–، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، المركز الجامعي عبد الحفيظ بوصوف، ميلة، الجزائر، يومي 23 و24 أفريل 2018، ص 1181.

[26] شمس الدين التجاني ومحمد يوسف عمامرة، مرجع سبق ذكره، ص ص 1204-1205.

[27] وشاش فؤاد وآخرون، **حماية المستهلك على الصعيد الدولي في ظل مخاطر التجارة الإلكترونية**، الملتقى الوطني الثالث حول المستهلك والاقتصاد الرقمي –ضرورة الانتقال وتحديات الحماية–، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، المركز الجامعي عبد الحفيظ بوصوف، ميلة، الجزائر، يومي 23 و24 أفريل 2018، ص ص 1895 – 1896.

[28] ثامر البكري، **أسس ومفاهيم معاصرة**، دار اليازوري العلمية للنشر والتوزيع، عمان، الأردن، 2006، ص 237.

[29] فارس طلوش ويونس زين، **قراءة حول الحماية القانونية للمستهلك ضمن تشريعات الأمم المتحدة وبعض الدول المتطورة**، الملتقى الوطني الثالث حول المستهلك والاقتصاد الرقمي –ضرورة الانتقال وتحديات الحماية–، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، المركز الجامعي عبد الحفيظ بوصوف، ميلة، الجزائر، يومي 23 و24 أفريل 2018، ص 1861.

[30] صباح عبد الرحيم ووهيبة عبد الرحيم، **واقع تسوق المستهلك عبر شبكة الانترنيت بين الحماية والجريمة**، مجلة الاجتهاد القضائي، المجلد 01، العدد 14، جامعة محمد خيضر، بسكرة،الجزائر، أفريل 2017، ص ص 130 – 132.

[31] بوزكري جيلالي، **الإدارة الإلكترونية في المؤسسات الجزائرية واقع وآفاق**، أطروحة دكتوراه علوم في علوم التسيير (غير منشورة)، تخصص إدارة الأعمال والتسويق، قسم علوم التسيير، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة الجزائر 03، الجزائر، 2016/2015، ص ص 154 – 155.

[32] صراع كريمة، **واقع وآفاق التجارة الإلكترونية في الجزائر**، مذكرة ماجستير في العلوم التجارية (غير منشورة)، تخصص استراتيجية، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة وهران 2 محمد بن أحمد، الجزائر، 2014/2013، ص ص 77 – 82.

[33] بلعطار زوليخة وبن عميروش مديحة، آليات حماية المستهلك الإلكتروني من مخاطر الاحتيال والاختراق، الملتقى الوطني الثالث حول المستهلك والاقتصاد الرقمي –ضرورة الانتقال وتحديات الحماية–، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، المركز الجامعي عبد الحفيظ بوصوف، ميلة، الجزائر، يومي 23 و24 أفريل 2018، ص 1605.

[34] واقد يوسف، **النظام القانوني للدفع الالكتروني**، مذكرة ماجستير في القانون (غير منشورة)، فرع القانون العام، تخصص قانون التعاون الدولي، كلية الحقوق، مدرسة دكتوراه للعلوم القانونية والسياسية، جامعة مولود معمري، تيزي وزو، الجزائر، 2011، ص 182.