الحماية الجنائية للمستهلك الإلكتروني

Criminal protection for the electronic consumer

إعداد

الدكتور/ يحيى إبراهيم دهشان

مدرس القانون الجنائي

كلية الحقوق – جامعة الزقازيق

البريد الإلكترونى : y.dhshan@gmail.com

الملخص

أصبحت الحماية الجنائية للمستهلك الإلكتروني موضوعًا ذا أهمية متزايدة. مع انتشار الإنترنت والأجهزة الذكية، تحولت العديد من المعاملات التجارية من العالم الفعلي إلى الفضاء الافتراضي، مما خلق فرصًا جديدة لكل من المستهلكين والشركات. ومع ذلك، فإن هذا التحول الرقمي لم يأتِ دون تحديات، حيث ظهرت مخاطر وتهديدات جديدة تستهدف خصوصية وأمان المستهلكين عبر الإنترنت.

وتأتي أهمية هذه الحماية من عدة جوانب رئيسية تسهم بشكل مباشر في حماية المستهلكين وتعزيز الثقة في التعاملات الإلكترونية، وأيضا تساهم في مكافحة الجرائم الإلكترونية عبر تطوير أدوات وتشريعات محددة لهذا الغرض، كما يعزز وجود إطار حماية جنائي قوي الابتكار والتنافسية بين الشركات الالكترونية.

وتهدف هذه الحماية إلى وضع الأطر القانونية والتنظيمية لحماية الأفراد من الجرائم الإلكترونية التي قد تؤثر على حقوقهم ومصالحهم في الفضاء الرقمي. هذه تشمل الاحتيال الإلكتروني، سرقة الهوية، الاختراقات الأمنية، وغيرها من الأنشطة غير القانونية التي تهدد سلامة المستهلك وثقته في البيئة الإلكترونية.

وتتمثل إشكالية الموضوع في، ما الحد الفاصل بين جريمتي النصب والغش التجاري، في التجارة الالكترونية؟ وما حدود المواقع والمتاجر الالكترونية، في جمع واستغلال بيانات مرتاديها؟ وكيف يمكن تحديد الاختصاص القضائي في جرائم المستهلك الالكتروني التي تتم عبر الحدود الدولية؟ وهل الاقتصاد الخفي، والتجارة الالكترونية في مصر، يطولها يد الحماية الجنائية للمستهلك؟

وتوصلنا لمجموعة من النتائج أهمها: تظل معضلة حماية المستهلك الإلكتروني ليست في غياب النصوص الجنائية لحمايته، بل تكمن المشكلة في ضعف الأجهزة الرقابية المسئولة عن الحماية، وتباطؤ الاستجابة لشكاواه من قبل الجهات المعنية. وتوصيتها أهمها: تعزيز التشريعات والقوانين، وتحسين آليات الرصيد والتتبع، والتوعية والتثقيف الرقمي، وتشجيع الإبلاغ عن الجرائم الالكترونية، وتحسين الأمان السيبراني للمنصات الالكترونية.

الكلمات المفتاحية: جرائم المستهلك الالكتروني، الحماية الجنائية للمستهلك، المستهلك الالكتروني.

Abstract

Criminal protection of the electronic consumer is becoming an increasingly important topic. With the spread of the Internet and smart devices, many business transactions have shifted from the physical world to the virtual space, creating new opportunities for both consumers and businesses. However, this digital transformation has not come without challenges, as new risks and threats targeting consumers' online privacy and security have emerged.

The importance of this protection comes from several main aspects that contribute directly to protecting consumers and enhancing confidence in electronic transactions. It also contributes to combating cybercrime by developing specific tools and legislation for this purpose. The presence of a strong criminal protection framework also enhances innovation and competitiveness among electronic companies.

This protection aims to establish legal and regulatory frameworks to protect individuals from cybercrimes that may affect their rights and interests in the digital space. These include wire fraud, identity theft, security breaches, and other illegal activities that threaten consumer safety and trust in the electronic environment.

The problem of the topic is: What is the dividing line between the crimes of fraud and commercial fraud in electronic commerce? What are the limits of websites and electronic stores in collecting and exploiting their users' data? How can jurisdiction be determined in consumer electronic crimes that occur across international borders? Is the hidden economy and electronic commerce in Egypt beyond the reach of criminal protection for the consumer?

We reached a set of results, the most important of which are: The problem of protecting the electronic consumer remains not in the absence of criminal texts to protect him, but rather the problem lies in the weakness of the regulatory agencies responsible for protection, and the slow response to his complaints by the concerned authorities. Its most important recommendations are strengthening legislation and laws, improving balance and tracking mechanisms, digital awareness and education, encouraging reporting of cybercrimes, and improving the cybersecurity of electronic platforms.

Keywords: electronic consumer crimes, criminal protection of the consumer, electronic consumer.

٢- الحماية الجنائية للمستهلك الإلكتروني

مقدمة

أولا- موضوع البحث:

في عصر الرقمنة المتسارع والتوسع الهائل للتجارة الإلكترونية، أصبحت الحماية الجنائية للمستهلك الإلكتروني موضوعًا ذا أهمية متزايدة. مع انتشار الإنترنت والأجهزة الذكية، تحولت العديد من المعاملات التجارية من العالم الفعلي إلى الفضاء الافتراضي، مما خلق فرصًا جديدة لكل من المستهلكين والشركات. ومع ذلك، فإن هذا التحول الرقمي لم يأتِ دون تحديات، حيث ظهرت مخاطر وتهديدات جديدة تستهدف خصوصية وأمان المستهلكين عبر الإنترنت.

الحماية الجنائية للمستهلك الإلكتروني تهدف إلى وضع الأطر القانونية والتنظيمية لحماية الأفراد من الجرائم الإلكترونية التي قد تؤثر على حقوقهم ومصالحهم في الفضاء الرقمي. هذه تشمل الاحتيال الإلكتروني، سرقة الهوية، الاختراقات الأمنية، وغيرها من الأنشطة غير القانونية التي تهدد سلامة المستهلك وثقته في البيئة الإلكترونية.

لمواجهة هذه التحديات، تعمل الحكومات والهيئات التنظيمية على تطوير وتنفيذ قوانين وسياسات تستهدف مكافحة الجرائم الإلكترونية وتوفير آليات للمراقبة والتحقيق في هذه

الجرائم. يشمل ذلك إنشاء وحدات خاصة لمكافحة الجريمة الإلكترونية وتعزيز التعاون الدولي لمكافحة هذه الجرائم التي غالبًا ما تتجاوز الحدود الوطنية.

بالإضافة إلى الإجراءات القانونية والتنظيمية، تلعب التوعية العامة وتعليم المستهلك دورًا حاسمًا في حماية الأفراد في الفضاء الإلكتروني. من خلال زيادة الوعي بالمخاطر وتعليم المستهلكين كيفية حماية أنفسهم عبر الإنترنت، يمكن تقليل الضرر الناتج عن الجرائم الإلكترونية وتعزيز بيئة تجارة إلكترونية أكثر أمانًا.

ومع ذلك، فإن تحقيق الحماية الجنائية الفعالة للمستهلك الإلكتروني يتطلب جهدًا مستمرًا وتعاونًا بين جميع الأطراف المعنية، بما في ذلك الحكومات، الشركات، المنظمات غير الحكومية، والمستهلكين أنفسهم. فقط من خلال العمل المشترك يمكن تطوير استراتيجيات فعالة لمواجهة التحديات المستمرة وضمان بيئة تجارة إلكترونية آمنة وموثوقة للجميع.

وتظل معضلة حماية المستهلك الإلكتروني ليست في غياب النصوص الجنائية لحمايته، بل تكمن المشكلة في ضعف الأجهزة الرقابية المسئولة عن الحماية، وتباطؤ الاستجابة لشكاواه من قبل الجهات المعنية.

ثانيا- أهمية البحث:

الحماية الجنائية للمستهلك الإلكتروني تشكل عنصرًا أساسيًا في تعزيز وتطوير الاقتصاد الرقمي وضمان تجربة تسوق آمنة وموثوقة عبر الإنترنت. في هذا السياق، تأتي أهمية هذه الحماية من عدة جوانب رئيسية تسهم بشكل مباشر في حماية المستهلكين وتعزيز الثقة في التعاملات الإلكترونية.

أولًا، تؤدي الحماية الجنائية دورًا حاسمًا في تعزيز الثقة بين المستهلكين والمنصات الإلكترونية. من خلال توفير إطار قانوني يضمن حماية بيانات المستهلك وخصوصيته، تشجع المستهلكين على الاستفادة من الخدمات الإلكترونية دون قلق من تعرضهم للاحتيال أو سرقة الهوية.

ثانيًا، تعمل الحماية الجنائية على حماية الحقوق الأساسية للمستهلكين، بما في ذلك حقهم في الخصوصية وحماية بياناتهم الشخصية. في عالم تتزايد فيه التهديدات الإلكترونية، تصبح حماية هذه الحقوق أكثر أهمية من أي وقت مضى.

ثالثًا، تساهم الحماية الجنائية في مكافحة الجرائم الإلكترونية عبر تطوير أدوات وتشريعات محددة لهذا الغرض. من خلال توفير الآليات اللازمة لملاحقة ومحاسبة المجرمين، تضمن الحماية الجنائية بيئة إلكترونية أكثر أمانًا للمستهلكين.

رابعًا، يعزز وجود إطار حماية جنائي قوي الابتكار والتنافسية بين الشركات العاملة في الفضاء الإلكتروني. الشركات التي تتخذ إجراءات فعالة لحماية المستهلكين تكتسب ثقة أكبر من جانب المستهلكين، مما يؤدي إلى تحسين سمعتها وزيادة حصتها السوقية.

خامسًا، تلعب الحماية الجنائية دورًا في الحد من الخسائر المالية التي يمكن أن يتعرض لها المستهلكون نتيجة للاحتيال الإلكتروني. من خلال تقليل الفرص المتاحة للمحتالين، تساهم في خفض معدلات الجريمة وتحمي الموارد المالية للمستهلكين.

أخيرًا، تدعم الحماية الجنائية التعاون الدولي في مجال مكافحة الجرائم الإلكترونية، الأمر الذي يعد ضروريًا نظرًا للطبيعة العابرة للحدود لهذه الجرائم. من خلال تبادل المعلومات والخبرات والتعاون في التحقيقات، يمكن تحقيق استجابة أكثر فعالية للتهديدات الإلكترونية.

بالمجمل، تشكل الحماية الجنائية للمستهلك الإلكتروني حجر الزاوية في ضمان بيئة تجارة إلكترونية آمنة وعادلة. تحتاج الدول والمنظمات الدولية إلى العمل بشكل مستمر على تحديث وتطوير الإطار القانوني لمواكبة التطورات التكنولوجية والتحديات الجديدة في الفضاء الإلكتروني.

ثالثا- أهداف البحث:

الحماية الجنائية للمستهلك الإلكتروني تهدف إلى ضمان بيئة تجارة إلكترونية آمنة وعادلة لجميع المستخدمين. أهدافها الرئيسية تشمل:

١. ضمان أمان البيانات الشخصية للمستهلكين وحمايتها من السرقة، الاستغلال، أو الكشف غير المصرح به. هذا يشمل منع الوصول غير القانوني إلى المعلومات الشخصية وضمان استخدام البيانات وفقًا للأغراض التي وافق عليها المستهلك.

٢. التصدي لجميع أشكال الاحتيال الإلكتروني، بما في ذلك الاحتيال المالي، الاحتيال في المعاملات، والنصب عبر الإنترنت، والعمل على ملاحقة ومحاسبة الجناة.

٣. تعزيز أمان المنصات والبنى التحتية الإلكترونية لحماية المستهلكين من الهجمات السيبرانية مثل البرمجيات الخبيثة، الفيروسات، وهجمات الحرمان من الخدمة.

٤. بناء ثقة المستهلكين في التجارة الإلكترونية من خلال ضمان وجود إطار قانوني يحمي حقوقهم ويعالج المخاوف المتعلقة بالأمان والخصوصية.

٥. رفع مستوى الوعي بين المستهلكين حول مخاطر الجرائم الإلكترونية وكيفية حماية أنفسهم عبر الإنترنت. هذا يشمل توفير المعلومات حول أفضل الممارسات للأمان الإلكتروني وحقوق المستهلك الرقمية.

٦. نظرًا لطبيعة الجرائم الإلكترونية العابرة للحدود، فإن تعزيز التعاون بين الدول والمنظمات الدولية يعتبر أساسيًا لمكافحة هذه الجرائم بفعالية وحماية المستهلكين في جميع أنحاء العالم.

٧. ضمان أن الأطر القانونية محدثة وقادرة على التعامل مع التحديات الجديدة التي تطرأ على البيئة الرقمية، وذلك من خلال مراجعة وتحديث التشريعات بشكل دوري.

من خلال تحقيق هذه الأهداف، يمكن للحماية الجنائية للمستهلك الإلكتروني ضمان بيئة تجارية إلكترونية تتسم بالأمان والعدالة، مما يشجع على نمو التجارة الإلكترونية ويدعم التطور الاقتصادي الرقمي.

رابعا- إشكاليات البحث:

تتمثل الإشكالية الرئيسية لموضوع الدراسة في، ما وجه الحماية الجنائية للمستهلك الالكتروني، وتتفرع منها عدة إشكاليات فرعية، تتمثل في:

- **ما الحد الفاصل بين جريمتي النصب والغش التجاري، في التجارة الالكترونية؟**
- **ما حدود المواقع والمتاجر الالكترونية، في جمع واستغلال بيانات مرتاديها؟**
- **كيف يمكن تحديد الاختصاص القضائي في جرائم المستهلك الالكتروني التي تتم عبر الحدود الدولية؟**
- **كيف يمكن للمستهلكين الإلكترونيين حماية خصوصيتهم وبياناتهم الشخصية في ظل الممارسات المتزايدة لجمع البيانات من قبل الشركات الكبرى؟**

كما ينتج عن إشكالية البحث عدة تساؤلات تتمثل في الآتي:

- **هل الاقتصاد الخفي، والتجارة الالكترونية في مصر، يطولها يد الحماية الجنائية للمستهلك؟**
- **هل القواعد الواردة في قانون حماية المستهلك المصري، كافية لحماية المستهلك الالكتروني من الجرائم التي تقع عليه؟**
- **هل يمكن ضبط جرائم الاحتيال الالكتروني الواقعة على المستهلك؟**
- **هل يُعد استعمال بطاقة ائتمان تعود لشخص آخر - بدون علمه - جريمة؟**
- **كيف يمكن تحجيم المواقع الالكترونية من عدم استغلال بيانات المستهلكين في الاغراض التجارية؟**

- **هل القوانين الحالية كافية لحماية خصوصية المستهلك الالكتروني، من أي انتهاك أو استغلال يقع عليها؟**
- **كيف يمكن تحسين الأمان الإلكتروني للمنصات والخدمات الإلكترونية لحماية المستهلكين بشكل فعال؟**
- **ما هو دور الأجهزة الرقابية والتنظيمية في حماية المستهلك الإلكتروني وما هي التحديات التي تواجهها؟**
- **كيف يمكن تحديد المسؤولية في حالات الاحتيال الإلكتروني، خاصة عندما تكون هناك سلاسل إمداد معقدة أو عند استخدام الذكاء الاصطناعي والتكنولوجيا المتقدمة؟**
- **ما هي الحدود بين جمع البيانات لتحسين الخدمات وانتهاك خصوصية المستهلك؟**
- **ما هو دور المنصات الإلكترونية في حماية المستهلكين، وكيف يمكن محاسبتها في حال فشلها في ذلك؟**

خامسا– نطاق البحث:

يتمثل نطاق البحث في حدود الدراسة التي يشملها موضوع البحث، ونطاق موضوعنا هنا يتحدد في نطاق موضوعي ونطاق مكاني. فبالنسبة للنطاق الموضوعي يتمثل في الحماية الجنائية للمستهلك الالكتروني، والنطاق المكاني فيتمثل في استعراض الحماية الجنائية للمستهلك الالكتروني بعدد من الدول العربية وهى مصر والامارات والسعودية، وأخرى أجنبية وهى الاتحاد الأوربي وأمريكا وأستراليا.

وهذه هي حدود بحثنا التي سنتحدث خلالها.

سادسا- منهج البحث:

في إطار بحثنا، نتبع منهجية تحليلية مقارنة. حيث نستعين بالتحليل لتوضيح المسائل البحثية المتعلقة بدراستنا، مما يسهم في تبسيط عملية الفهم والدراسة. من جهة أخرى، نعتمد على المقارنة في سياق بحثنا لاستعراض ومقارنة كيفية تعاطي الدول والتشريعات المختلفة مع موضوع حماية المستهلك الالكتروني.

سابعا- خطة البحث:

الفصل الأول: الإطار النظري والتشريعي للحماية الجنائية للمستهلك الإلكتروني

المبحث الأول: ماهية الحماية الجنائية للمستهلك الإلكتروني

المبحث الثاني: أهمية وأهداف الحماية الجنائية للمستهلك الإلكتروني

المبحث الثالث: تطور التشريعات الخاصة بالحماية الجنائية للمستهلك الإلكتروني

الفصل الثاني: الجرائم ضد المستهلك الالكتروني وتحديات الحماية منها

المبحث الأول: الجرائم الإلكترونية ضد المستهلكين وطرق الحماية منها

المبحث الثاني: تحديات تطبيق قوانين حماية المستهلك الالكتروني

المبحث الثالث: تأثير التكنولوجيا والتطورات الرقمية على الحماية الجنائية للمستهلك

الفصل الأول

الإطار النظري والتشريعي للحماية الجنائية للمستهلك الإلكتروني

تمهيد وتقسيم:

في ظل التطور السريع للتكنولوجيا وتزايد اعتماد المجتمعات على الفضاء الإلكتروني لتلبية احتياجاتها المتنوعة، من التسوق إلى التواصل الاجتماعي، تبرز أهمية تطوير الإطار النظري والتشريعي المتخصص بالحماية الجنائية للمستهلك الإلكتروني. هذا الإطار يهدف إلى تقديم الأساس القانوني والنظري لفهم ومعالجة التحديات الجديدة التي تفرضها الجرائم الإلكترونية، والتي تؤثر بشكل مباشر على أمان وخصوصية المستهلكين عبر الإنترنت. من خلال توفير رؤية شاملة ومتكاملة، يساعد هذا الإطار في تصميم استراتيجيات فعالة لمكافحة الجرائم الإلكترونية وحماية المستهلكين بشكل متوازن وعادل([1]).

يعتمد الإطار النظري والتشريعي للحماية الجنائية للمستهلك الإلكتروني على مجموعة من المبادئ الأساسية، بما في ذلك الشفافية، والمسئولية، والخصوصية، ويسعى لتحقيق التوازن بين تعزيز الابتكار التكنولوجي وحماية حقوق المستهلكين. تشكل هذه

[1]) Jonathan Clough, Principles of Cybercrime, Cambridge University Press, 2015, p 63.

المبادئ الأساس لتطوير قوانين وتشريعات تضمن تنفيذ العقوبات اللازمة على المخالفين، وفي الوقت نفسه، توفر آليات للوقاية والحماية تمكن المستهلكين من التصرف بثقة وأمان في الفضاء الإلكتروني.

من الضروري إذًا، أن يتم تطوير وتحديث الإطار النظري والتشريعي بشكل مستمر ليعكس التغيرات التكنولوجية والاجتماعية المتسارعة. يجب أن يشمل هذا الإطار التعاون الدولي، نظرًا للطبيعة العابرة للحدود للعديد من الجرائم الإلكترونية، لضمان إنشاء نظام قانوني شامل يحمي المستهلكين في جميع أنحاء العالم. فقط من خلال مقاربة شاملة ومتكاملة، ويمكن للمجتمعات تحقيق الحماية الفعالة للمستهلك الإلكتروني وضمان بيئة رقمية آمنة للجميع.

وسنتحدث في هذا الفصل عن ماهية الحماية الجنائية للمستهلك الإلكتروني في مبحث أول، ثم نتناول أهمية وأهداف الحماية الجنائية للمستهلك الإلكتروني في مبحث ثانٍ، ونستعرض تطور التشريعات الخاصة بالحماية الجنائية للمستهلك الإلكتروني في مبحث ثالث.

المبحث الأول

ماهية الحماية الجنائية للمستهلك الإلكتروني

تمهيد وتقسيم:

الحماية الجنائية للمستهلك الإلكتروني تعتبر أحد الأسس الرئيسية لضمان سلامة وأمان التجارة الإلكترونية في عالم يزداد ترابطًا وتعقيدًا بفضل التقدم التكنولوجي المستمر. هذه الحماية تشير إلى مجموعة الأطر القانونية والتنظيمية التي صُممت لحماية حقوق المستهلكين عبر الإنترنت من الجرائم والممارسات الضارة التي يمكن أن تستهدفهم، مثل الاحتيال الإلكتروني، سرقة الهوية، والتصيد الاحتيالي. هذه الأطر تسعى للحفاظ على ثقة المستهلكين في النظام الرقمي بكامله، من خلال ضمان تجربة تسوق آمنة وموثوقة تحمي معلوماتهم الشخصية والمالية من التعرض للخطر([1]).

في هذا السياق، تلعب الحماية الجنائية دورًا حيويًا في تطوير وتنفيذ التشريعات التي تعاقب على الأنشطة الإلكترونية الضارة، وتوفير آليات للتحقيق والمحاكمة في حالات الانتهاك. الهدف من هذه الجهود ليس فقط معاقبة المخالفين ولكن أيضًا خلق بيئة ردعية تمنع وقوع هذه الجرائم مستقبلًا. علاوة على ذلك، تسعى الحماية الجنائية إلى

[1]) حمدان فاهد سعيد المزروعي، الحماية الجنائية للمستهلك في القانونين الإماراتي والمغربي، المجلة المغربية للإدارة المحلية والتنمية، ع١٣٢، ٢٠١٧، ص ٢٥٨.

تعزيز التعاون بين الوكالات الحكومية والشركات الخاصة لضمان تبادل فعال للمعلومات والخبرات اللازمة للتصدي للتهديدات الإلكترونية، مما يعزز من قدرة المجتمع الرقمي على التكيف والتصدي للمخاطر الجديدة([1]).

بالإضافة إلى ذلك، تؤكد الحماية الجنائية للمستهلك الإلكتروني على أهمية التوعية والتثقيف الرقمي للمستهلكين كجزء لا يتجزأ من استراتيجيات الحماية. من خلال تزويد المستهلكين بالمعرفة والأدوات اللازمة للتعرف على المخاطر الإلكترونية وكيفية حماية أنفسهم منها، يمكن تقليل فرص نجاح الجرائم الإلكترونية وتعزيز بيئة تجارية إلكترونية أكثر أمانًا للجميع. إن تطوير برامج تعليمية وحملات توعية تستهدف جميع شرائح المجتمع، بالتزامن مع تحديث وتعزيز الإطار القانوني، يشكل محورًا أساسيًا لضمان استمرارية وفعالية الحماية الجنائية للمستهلك الإلكتروني.

وسنتحدث عن مفهوم المستهلك الالكتروني في مطلب أول، ثم نتناول ذاتية الحماية الجنائية للمستهلك الالكتروني في مطلب ثانٍ.

[1]) Uchenna Jerome Orji, Cybersecurity Law and Regulation, Wolters Kluwer, 2020, p 74.

المطلب الأول

مفهوم المستهلك الالكتروني

يشير المستهلك الإلكتروني إلى أي فرد يقوم بشراء السلع أو الخدمات عبر الإنترنت([1]). هذا المفهوم يعكس التطور الكبير في عادات التسوق والتعاملات التجارية التي جاءت مع الثورة الرقمية وانتشار الإنترنت. كما يستفيد هؤلاء المستهلكين من التكنولوجيا الرقمية لتسهيل عملية الشراء، مما يتيح لهم الوصول إلى مجموعة واسعة من المنتجات والخدمات عبر الإنترنت بدلاً من الاعتماد على الطرق التقليدية مثل المتاجر الفعلية.

وهناك العديد من المرادفات لمصطلح المستهلك الالكتروني، وتتمثل في:

أولا- مستهلك الإنترنت:

يُشير إلى الأفراد الذين يستخدمون الإنترنت لأغراض مختلفة تتعلق بالاستهلاك، بما في ذلك البحث عن معلومات حول المنتجات والخدمات، قراءة التقييمات والمراجعات، وشراء السلع والخدمات عبر الإنترنت. هذا النوع من المستهلكين يستفيد من الوصول

[1]) الإنترنت هو شبكة عالمية تربط ملايين الأجهزة الحاسوبية ببعضها البعض. لتسهيل التواصل وتبادل البيانات بين المستخدمين في مختلف أنحاء العالم.

الواسع والمريح الذي يوفره الإنترنت لمقارنة الأسعار، العثور على العروض، وإجراء المعاملات دون الحاجة للتواجد فيزيائيًا في المتاجر([1]).

المستهلكين عبر الإنترنت يتميزون بكونهم أكثر إلمامًا بالتكنولوجيا وعادةً ما يكون لديهم معرفة جيدة بكيفية البحث عن المعلومات وتقييمها عبر الويب. يميلون إلى الاستفادة من الشبكات الاجتماعية، المنتديات، والمواقع المتخصصة للحصول على توصيات وتقييمات حول المنتجات والخدمات قبل اتخاذ قرار الشراء. هذا النوع من المستهلكين يتزايد بشكل ملحوظ مع توسع استخدام الإنترنت والتجارة الإلكترونية عالميًا، حيث يوفر الإنترنت إمكانيات هائلة لتسهيل الوصول إلى السوق العالمي، مما يسمح للمستهلكين بشراء المنتجات والخدمات من مختلف أنحاء العالم.

ثانيًا– المتسوق عبر الإنترنت:

هو مصطلح يُستخدم لوصف الأفراد الذين يقومون بشراء السلع والخدمات عبر الإنترنت. يتميز هؤلاء المتسوقون بالاعتماد على المنصات الإلكترونية لإجراء معاملاتهم التجارية، مستفيدين من مزايا التسوق عبر الإنترنت مثل الراحة، السرعة، والقدرة على الوصول إلى تشكيلة واسعة من المنتجات والخدمات التي قد لا تتوفر في

[1]) Michael R. Solomon, Consumer Behavior: Buying, Having, and Being, Pearson, 2020, p 86.

المتاجر التقليدية. المتسوقون عبر الإنترنت يستخدمون مجموعة متنوعة من الأجهزة الإلكترونية مثل الحواسيب، الأجهزة اللوحية، والهواتف الذكية للبحث عن المنتجات، مقارنة الأسعار، قراءة التقييمات والمراجعات، وإتمام عمليات الشراء. كما يمكنهم الاستفادة من العروض الخاصة، الخصومات، وأنظمة الولاء التي تقدمها المتاجر الإلكترونية لجذب الزبائن وتشجيعهم على الشراء([1]).

واحدة من الخصائص الرئيسية للمتسوقين عبر الإنترنت هي توقعهم لتجربة شراء سلسة وآمنة، بما في ذلك سهولة الوصول إلى المعلومات حول المنتجات، وضوح سياسات الاسترجاع والضمان، والحصول على خيارات دفع موثوقة ومريحة.

ثالثًا- مستهلك العصر الرقمي:

هو مصطلح يصف الأفراد الذين يعتمدون بشكل كبير على التكنولوجيا الرقمية في جميع جوانب حياتهم، بما في ذلك عملية الاستهلاك. هذا النوع من المستهلكين يستخدم الإنترنت والأجهزة الذكية ليس فقط للتسوق وشراء المنتجات والخدمات، ولكن

[1]) Charles W. Lamb, Joe F. Hair, and Carl McDaniel, MKTG (Marketing), Cengage Learning, 2020, p 23.

أيضًا للبحث عن معلومات، قراءة التقييمات، مشاركة الآراء، والتفاعل مع العلامات التجارية([1]).

مستهلكو العصر الرقمي يتوقعون تجارب مخصصة ومريحة تلبي احتياجاتهم الفردية، مع الحفاظ على مستويات عالية من الأمان والخصوصية. إنهم يقدرون الشفافية من العلامات التجارية ويفضلون الشركات التي تقدم تفاعلاً ذا معنى وتجارب مستخدم مبتكرة. بالإضافة إلى ذلك، مستهلك العصر الرقمي يسعى وراء الاستدامة والمسؤولية الاجتماعية من العلامات التجارية، حيث يصبح الوعي البيئي والأخلاقي جزءًا لا يتجزأ من قرارات الشراء. هذه التوجهات تدفع الشركات إلى إعادة التفكير في طرق إنتاجها وتسويقها لتلبية توقعات هذا الجيل الجديد من المستهلكين.

رابعًا– المستهلك المتصل:

يشير إلى الأفراد الذين يستخدمون الإنترنت والتكنولوجيا الرقمية بشكل مكثف في حياتهم اليومية، بما في ذلك في عملية اتخاذ قرارات الشراء. هؤلاء المستهلكون متصلون دائمًا بالإنترنت من خلال الأجهزة الذكية مثل الهواتف المحمولة، الأجهزة اللوحية، والحواسيب، مما يمكنهم من الوصول الفوري إلى المعلومات، الخدمات،

[1]) Ryan Jenkins, The Millennial Manual: The Complete How-To Guide to Manage, Develop, and Engage Millennials at Work, RockBench Publishing Corp, 2018, p 41.

والمنتجات عبر الإنترنت في أي وقت ومن أي مكان. يستفيد المستهلكون المتصلون من الشبكات الاجتماعية والمنصات الإلكترونية لمشاركة تجاربهم وقراءة تقييمات ومراجعات المنتجات من مستهلكين آخرين قبل الشراء، مما يعزز من قدرتهم على اتخاذ قرارات مستنيرة. كما أنهم يقدرون السرعة والكفاءة في التسوق والخدمات، ويتوقعون تجارب شراء شخصية تلبي احتياجاتهم الفردية([1]).

بالإضافة إلى ذلك، المستهلكون المتصلون يميلون إلى البحث عن تجارب تسوق سلسة وتفاعلية توفرها التقنيات الحديثة مثل الواقع المعزز والدردشة الحية مع خدمة العملاء. كما يهتمون بالأمان الإلكتروني وحماية البيانات الشخصية عند التسوق وإجراء المعاملات عبر الإنترنت. تطور سلوك المستهلك المتصل يدفع الشركات إلى تطوير استراتيجيات تسويقية رقمية متقدمة تشمل تحليل البيانات الكبيرة لفهم تفضيلات العملاء وتوفير تجارب مخصصة، استخدام الذكاء الاصطناعي لتحسين تفاعل العملاء، وتعزيز الوجود على الشبكات الاجتماعية لبناء علاقات أقوى مع المستهلكين.

[1]) Philip Kotler, Hermawan Kartajaya, and Iwan Setiawan, Marketing 4.0: Moving from Traditional to Digital, Wiley, 2016, p 52.

هذه التعريفات والمصطلحات – أنفه البيان – تندرج تحت وصف موضوع الدراسة، وهي المستهلك الالكتروني. كما تُظهر كيف أن الإنترنت والتكنولوجيا الرقمية قد غيرت سلوكيات المستهلكين، مما يتيح للأفراد والشركات فرصاً جديدة للتفاعل في سوق عالمي متصل، حيث يعير المستهلك الإلكتروني عن تحول في سلوكيات الشراء والتفاعل مع العلامات التجارية في العصر الرقمي، مدفوعًا بالتقدم في التكنولوجيا والإنترنت. هذا التحول يتضمن تغييرات في كيفية استهلاك المعلومات، اتخاذ قرارات الشراء، وتفضيلات التواصل مع الشركات.

ووفقًا لدراسة نشرتها McKinsey، فإن الجائحة قد سرّعت من عملية انتقال المستهلكين إلى القنوات الرقمية، لكن بعض المستهلكين بدأوا في استخدام هذه القنوات بشكل أقل بعد تخفيف القيود. ومع ذلك، يُظهر البحث أن تحسين تجارب المستخدم، توفير عروض أفضل، وزيادة الأمان والخصوصية يمكن أن تحافظ على اهتمام المستهلكين الرقميين وتشجعهم على استخدام القنوات الرقمية بشكل أكبر([1]).

من جهة أخرى، يشير تحليل نشر على ResearchGate إلى أن المستهلك الرقمي أصبح أكثر وعيًا وأقل عرضة للتأثير من خلال الأساليب التسويقية التقليدية. بدلاً من

[1]) Neira Hajro , Klemens Hjartar , Paul Jenkins , and Benjamim Vieira, What's next for digital consumers, 2021. online: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/whats-next-for-digital-consumers visit in: 16/2/2024.

ذلك، يُفضل هؤلاء المستهلكون التفاعل مع العلامات التجارية بطرق تشمل الشراء في أي مكان وزمان، المشاركة في تخصيص المنتجات والعلامات التجارية، والبحث عن تجارب شرائية فريدة ومخصصة. كما يُشير البحث إلى أن المستهلكين الرقميين يستخدمون الإنترنت بشكل كبير للبحث عن المنتجات، وشرائها، ومن ثم مشاركة تجاربهم مع المنتجات عبر الإنترنت، خاصةً عبر وسائل التواصل الاجتماعي([1]).

هذه النتائج تبرز أهمية الابتكار في خدمات وتجارب الرقمية للمحافظة على جذب وإبقاء المستهلكين في عالم متزايد الرقمية. الشركات التي تتكيف بنجاح مع هذه التغيرات وتستثمر في فهم وتلبية احتياجات وتوقعات المستهلكين الرقميين، تكون في وضع أفضل للنجاح في السوق الحديثة.

خصائص المستهلك الإلكتروني:

تعكس خصائص المستهلك الالكتروني التحولات الكبيرة في سلوكيات الشراء والتفاعل مع العلامات التجارية في العصر الرقمي. وهذه الخصائص تشمل: التسوق عبر الإنترنت، والتفاعل الرقمي، والوصول إلى المعلومات، والمقارنة والاختيار، والدفع

[1]) Jolanta Tkaczyk, Digital Consumer: Trends and Challenges, 2016. online: https://www.researchgate.net/publication/327079329_Digital_Consumer_Trends_and_Challenges visit in: 16/2/2024.

الالكتروني، تفصيل الأمان والخصوصية، وغيرها من الخصائص التي يتميز بها المستهلك الالكتروني، ونستعرضها تفصيلا:

- **التسوق عبر الإنترنت:** يستخدم المستهلكون الإلكترونيون الإنترنت لشراء مجموعة واسعة من السلع والخدمات، بدءًا من المنتجات اليومية وصولًا إلى السلع الفاخرة والخدمات المتخصصة. من الصفات البارزة للمستهلك الإلكتروني هي قدرته ورغبته في التسوق عبر الإنترنت. هذه الصفة تعكس تغييراً جذرياً في عادات الشراء التقليدية، حيث يفضل المستهلكون الآن استخدام الأجهزة الذكية والكمبيوترات لاستكشاف وشراء المنتجات من دون الحاجة لزيارة المتاجر فعلياً. الراحة، الكفاءة، والقدرة على مقارنة الأسعار بسهولة تجعل التسوق عبر الإنترنت خياراً مفضلاً للغاية لهذا النوع من المستهلكين([1]).
- **التفاعل الرقمي:** التفاعل الرقمي يُعتبر من الركائز الأساسية في سلوك المستهلك الإلكتروني اليوم. المستهلكون يستخدمون مجموعة متنوعة من القنوات الرقمية للتواصل والتفاعل مع العلامات التجارية، مما يوفر لهم فرصة للتعبير عن آرائهم، طرح الأسئلة، والحصول على دعم العملاء بشكل فوري

[1]) Michael R. Solomon, op. cit., p 87.

وفعال. مواقع الويب والتطبيقات الذكية تسمح بتجربة تسوق سلسة ومخصصة، في حين توفر منصات التواصل الاجتماعي مساحة للمستهلكين لمشاركة تجاربهم والتوصية بالمنتجات لأقرانهم([1]).

- **الوصول إلى المعلومات:** الوصول إلى المعلومات هو أحد الأعمدة الرئيسية التي تدعم سلوك المستهلك الإلكتروني في العصر الرقمي. المستهلكون اليوم لديهم القدرة على البحث وجمع المعلومات حول مختلف المنتجات والخدمات بسهولة ويسر عبر الإنترنت. هذه المعلومات لا تقتصر فقط على المواصفات والأسعار، بل تشمل أيضاً التقييمات والمراجعات من مستخدمين آخرين، مما يوفر رؤى قيمة حول تجاربهم الشخصية مع المنتج أو الخدمة. هذا النوع من المعلومات يلعب دوراً محورياً في عملية اتخاذ القرار لدى المستهلك الإلكتروني، حيث يمكنهم تقييم مزايا وعيوب المنتجات بناءً على تجارب مستخدمين حقيقيين قبل الشراء. الشفافية والوصول السهل إلى هذه المراجعات تعزز من ثقة المستهلكين في القرارات التي يتخذونها وتساعد في بناء علاقة أقوى بين المستهلكين والعلامات التجارية. بالإضافة إلى ذلك، العلامات التجارية التي تعتني بتقديم معلومات دقيقة ومفصلة حول منتجاتها وتشجع

[1]) Philip Kotler, Hermawan Kartajaya, and Iwan Setiawan, op. cit., p 56.

على المراجعات الصادقة تحظى بتقدير أكبر في أعين المستهلكين الإلكترونيين([1]).

- **المقارنة والاختيار**: المقارنة والاختيار تُعد من الخصائص الأساسية التي تميز المستهلك الإلكتروني، مما يعطيهم ميزة كبيرة في عملية الشراء. بفضل الإنترنت، أصبح بإمكان المستهلكين الوصول إلى مجموعة واسعة من المتاجر الإلكترونية ومقارنة المنتجات والأسعار بسهولة ويسر. هذه العملية تتيح لهم الاختيار بين العديد من الخيارات بناءً على معايير مختلفة مثل الجودة، السعر، تقييمات المستخدمين، والمواصفات، مما يضمن لهم الحصول على أفضل قيمة مقابل أموالهم. علاوة على ذلك، تتيح الأدوات الرقمية ومحركات البحث المتخصصة في المقارنة بين المنتجات للمستهلكين فرصة لعمل بحث شامل ودقيق في وقت قصير جدًا، مما يجعل عملية الشراء أكثر كفاءة وفعالية. هذه القدرة على المقارنة والاختيار ليست مفيدة للمستهلكين فحسب، بل تدفع أيضًا العلامات التجارية لتكون أكثر شفافية وتنافسية في تسعير منتجاتها وتحسين جودتها. بالتالي، تسهم هذه الديناميكية

[1]) David L. Rogers, The Digital Transformation Playbook: Rethink Your Business for the Digital Age, Columbia University Press, 2016, p 185.

في تعزيز بيئة تجارية إلكترونية أكثر إنصافًا وفعالية لكلاً من المستهلكين والبائعين([1]).

- **الدفع الإلكتروني:** الدفع الإلكتروني يُعد ركنًا أساسيًا في تجربة المستهلك الإلكتروني، حيث يفضل الكثيرون استخدام طرق دفع رقمية لسهولتها وأمانها المتزايد. البطاقات الائتمانية، خدمات مثل PayPal، وحتى العملات الرقمية مثل البيتكوين، توفر للمستهلكين إمكانية إتمام المعاملات المالية بسرعة وسهولة دون الحاجة للتعامل المباشر بالنقد أو الذهاب إلى البنك. هذه الطرق تتيح أيضًا للمستهلكين شراء المنتجات من مختلف أنحاء العالم، مما يعزز من تجربة التسوق العالمية ويفتح آفاقًا جديدة للتجارة الإلكترونية([2]).
- **تفضيل الأمان والخصوصية:** الأمان والخصوصية يمثلان محور اهتمام رئيسي للمستهلكين الإلكترونيين في ظل الزيادة المستمرة في التجارة الإلكترونية. مع تزايد الاعتماد على الإنترنت لإجراء المعاملات المالية والتسوق، ظهرت تحديات جديدة تتعلق بالأمان الرقمي وحماية البيانات الشخصية. المستهلكون اليوم يواجهون مخاطر متعددة تشمل الاحتيال

[1]) Michael R. Solomon, op. cit., p 84.

[2]) حساين عومرية، الحماية القانونية للمستهلك الإلكتروني في ظل جائحة كوفيد ١٩، مجلة الاجتهاد القضائي، مج١٣، ع٢، جامعة محمد خيضر بسكرة - كلية الحقوق والعلوم السياسية - مخبر أثر الاجتهاد القضائي على حركة التشريع، ٢٠٢١، ص ٤٣٤.

الإلكتروني، سرقة الهوية، والوصول غير المصرح به إلى البيانات الشخصية والمالية. هذه التحديات تستوجب على المستهلكين توخي الحذر واتباع أفضل الممارسات للحفاظ على أمان معلوماتهم، مثل استخدام كلمات مرور قوية، تفعيل التحقق بخطوتين، والتأكد من صحة المواقع الإلكترونية قبل إدخال البيانات الشخصية. من جانبها، الشركات والمنصات الإلكترونية تعمل باستمرار على تحسين أنظمة الأمان وحماية البيانات لكسب ثقة المستهلكين وضمان تجربة تسوق آمنة. تشمل هذه الجهود تطبيق تقنيات تشفير متطورة، إجراءات مراقبة لتتبع الأنشطة المشبوهة، وبرامج توعية للمستخدمين حول أهمية الأمان الرقمي. الحفاظ على الخصوصية والأمان الرقمي يُعد تحديًا مستمرًا يتطلب جهودًا مشتركة بين المستهلكين والشركات لمواجهة التهديدات الإلكترونية المتزايدة([1]).

التفرقة بين المستهلك التقليدي والمستهلك الالكتروني

لا يمكن إنهاء الحديث عن مفهوم المستهلك الالكتروني، بدون استعراض مقارنة للتفرقة بين المستهلك التقليدي والمستهلك الالكتروني. والتفرقة بين

[1]) Zhang, Q. Research on Rights Protection of Consumer and Interests in E-Commerce-Taking Functional Department and Industry Association. In: Du, W. (eds) Informatics and Management Science VI. Lecture Notes in Electrical Engineering, vol 209. Springer, London, 2013, p 274.

المستهلك التقليدي والمستهلك الإلكتروني تكمن في عدة جوانب رئيسية تتعلق بطريقة التسوق، الوصول إلى المعلومات، طبيعة المعاملات، والتحديات التي تواجه كل منهما:

أولًا- طريقة التسوق: تُعد واحدة من الفروق الرئيسية بين المستهلك التقليدي والمستهلك الإلكتروني([1]):

- المستهلك التقليدي: يفضل التسوق بشكل فعلي في المتاجر والأسواق، مما يمكنه من لمس، رؤية، وتجربة المنتجات مباشرة. هذا التفاعل الحسي مع المنتجات يوفر للمستهلك التقليدي إحساساً بالثقة والأمان في قرار الشراء. كما يتيح له فرصة التواصل المباشر مع البائعين لطرح الأسئلة أو الحصول على معلومات إضافية حول المنتجات. الشراء الفعلي يُعد تجربة اجتماعية أيضًا، حيث يمكن للمستهلكين التسوق مع الأصدقاء أو أفراد العائلة.
- المستهلك الإلكتروني: يستخدم الإنترنت لإجراء عمليات الشراء، سواء كان ذلك عبر المواقع الإلكترونية أو التطبيقات الخاصة بالتسوق. هذا النوع من المستهلكين يقدر الراحة والكفاءة التي يوفرها التسوق عبر الإنترنت، حيث يمكن إتمام عملية الشراء في أي وقت ومن أي مكان، دون الحاجة للتواجد

[1]) Charles W. Lamb, Joe F. Hair, and Carl McDaniel, op. cit., p163.

الفعلي في المتجر. التسوق الإلكتروني يتيح أيضًا إمكانية الوصول إلى تشكيلة أوسع من المنتجات والمقارنة بين الأسعار بسهولة، بالإضافة إلى قراءة التقييمات والمراجعات من مستخدمين آخرين قبل اتخاذ قرار الشراء.

ثانيًا– الوصول إلى المعلومات: يميز بشكل واضح بين المستهلك التقليدي والمستهلك الإلكتروني، مما يؤثر على كيفية اتخاذهم لقرارات الشراء([1]):

- المستهلك التقليدي: يعتمد بشكل كبير على المعلومات المتوفرة داخل المتاجر أو من خلال التواصل المباشر مع البائعين. هذه المعلومات قد تشمل تفاصيل المنتج، الأسعار، والعروض الترويجية المتاحة. التفاعل الشخصي يوفر فرصة للمستهلكين لطرح الأسئلة والحصول على توصيات مباشرة من البائعين، مما يساعدهم في اتخاذ قرارات مستنيرة بناءً على المعلومات المقدمة.
- المستهلك الإلكتروني: لديه القدرة على الوصول إلى مجموعة واسعة من المعلومات عبر الإنترنت. هذا يشمل المراجعات والتقييمات من مستخدمين آخرين، المقارنات التفصيلية بين المنتجات، والأبحاث حول أفضل الأسعار والعروض. الإنترنت يتيح للمستهلكين الفرصة للبحث عن المنتجات من

[1]) Michael R. Solomon, op. cit., p 124.

مصادر متعددة، مما يزيد من شفافية المعلومات ويساعد في تكوين رأي موضوعي حول القيمة الحقيقية للمنتجات والخدمات قبل الشراء.

هذه الديناميكية بين المستهلك التقليدي والمستهلك الإلكتروني تُظهر كيف أن التكنولوجيا قد غيرت بشكل جذري طريقة جمع المعلومات واتخاذ القرارات الشرائية. بينما يقدر بعض المستهلكين الأمان الذي يأتي مع التجربة المباشرة والتفاعل الشخصي في المتاجر، يفضل آخرون الوصول الشامل إلى المعلومات والمرونة التي توفرها البيئة الإلكترونية.

ثالثًا- طبيعة المعاملات: تعتبر واحدة من الفروقات الرئيسية بين المستهلك التقليدي والمستهلك الإلكتروني، مما يعكس تطور التكنولوجيا وتأثيرها على سلوكيات الشراء([1]):

- المستهلك التقليدي: يفضل المعاملات التي تتم بشكل مباشر، حيث يذهب إلى المتاجر والأسواق لاختيار المنتجات ودفع ثمنها في المكان. هذه المعاملات تتم غالبًا بالدفع النقدي أو عبر بطاقات الائتمان. التعامل المباشر يوفر للمستهلك التقليدي إحساسًا بالأمان والتحكم، حيث يمكنهم رؤية

[1]) Philip Kotler, Hermawan Kartajaya, and Iwan Setiawan, op. cit., p 32.

المنتجات وتقييمها قبل الشراء، والحصول على إيصالات فورية للمعاملات المالية.

- المستهلك الإلكتروني: يجري المعاملات بشكل رقمي، مستفيدًا من طرق دفع إلكترونية متنوعة تتجاوز استخدام النقد أو بطاقات الائتمان التقليدية. هذه الطرق تشمل خدمات مثل PayPal، الدفع عبر المنصات الإلكترونية، وحتى استخدام العملات الرقمية مثل البيتكوين. الدفع الإلكتروني يوفر للمستهلكين الإلكترونيين مرونة كبيرة ويسمح بإجراء المعاملات في أي وقت ومن أي مكان، مما يعزز تجربة الشراء ويجعلها أكثر سلاسة وفعالية.

رابعًا – التحديات:

- المستهلك التقليدي: يواجه عدة تحديات تتعلق بالتسوق الفعلي في المتاجر. أول هذه التحديات هي الحاجة للتنقل وزيارة المتاجر بدنيًا، مما يتطلب وقتًا وجهدًا، خاصة في الأوقات التي تشهد ازدحامًا مروريًا أو طوابير انتظار داخل المتاجر. كذلك، قيود التوقيت تعتبر تحديًا آخر، حيث إن معظم المتاجر تعمل وفقًا لساعات عمل محددة، مما يقيد المستهلكين الذين قد يجدون صعوبة في التسوق خلال هذه الأوقات. بالإضافة إلى ذلك، قد يواجه

المستهلك التقليدي قلة في التنوع والخيارات المتاحة للمنتجات، خصوصًا في المناطق التي تفتقر إلى المتاجر المتخصصة أو الكبرى([1]).

- المستهلك الإلكتروني: يواجه تحديات مختلفة تتعلق بالتسوق عبر الإنترنت. الأمان الرقمي وخصوصية البيانات تمثلان قلقًا كبيرًا، حيث يخشى الكثيرون من سرقة المعلومات المالية أو الشخصية عبر الإنترنت. التأخير في التوصيل أو مشاكل الشحن تعتبر أيضًا من التحديات التي قد تؤثر على تجربة التسوق الإلكتروني، خاصةً عند الشراء من متاجر تقع خارج البلاد. هذه التحديات تتطلب من المستهلكين الإلكترونيين توخي الحذر واتباع أفضل الممارسات لضمان تجربة تسوق آمنة ومرضية.

خامسًا- تجربة التسوق:

- للمستهلك التقليدي، تجربة التسوق تشمل بشكل أساسي التفاعل الشخصي والقدرة على تجربة المنتجات فعليًا قبل الشراء. هذا يعني زيارة المتاجر الفعلية، لمس المنتجات، تجربتها، وحتى التحدث مباشرة مع البائعين للحصول على معلومات أو توصيات. هذه التجربة توفر للمستهلك التقليدي إحساسًا

[1]) Lars Perner, Consumer Behavior: The Psychology of Marketing, University of Southern California, 2021, p 69.

بالأمان والثقة في الشراء، حيث إن اللمس الفعلي للمنتجات يمكن أن يساعد في تقييم جودتها وملائمتها لاحتياجاتهم.

- المستهلك الإلكتروني، من ناحية أخرى، يجد قيمة في تجربة التسوق التي تعتمد على سهولة الاستخدام والواجهات الرقمية. الراحة والسرعة هما العناصر الأساسية لتجربة التسوق عبر الإنترنت، حيث يمكن للمستهلكين البحث عن المنتجات، مقارنة الأسعار، وإجراء الشراء بضغطات قليلة دون الحاجة لمغادرة منازلهم. هذه التجربة تشمل أيضًا الوصول إلى مراجعات وتقييمات من مستخدمين آخرين، مما يساعد في اتخاذ قرارات مستنيرة بشأن الشراء([1]).

في النهاية، كلا نمطي التسوق يقدمان تجربة مختلفة ويتناسبان مع احتياجات مختلفة للمستهلكين. مع تطور التكنولوجيا، نشهد تداخلاً متزايدًا بين الاثنين، حيث يستخدم المستهلكون كلا النهجين بشكل متكامل لتحقيق أقصى قد من الاستفادة.

[1]) Michael R. Solomon, op. cit., p 12.٥

المطلب الثاني

ذاتية الحماية الجنائية للمستهلك الالكتروني

تُعد الحماية الجنائية للمستهلك الإلكتروني قضية متزايدة الأهمية في عصرنا الحالي، فخصوصية تلك الحماية تختلف – بشكل كبير – بالنسبة للمستهلك الإلكتروني عن المستهلك التقليدي بعدة جوانب أساسية. فالمستهلك الإلكتروني، بطبيعته، يشارك معلومات شخصية ومالية على الإنترنت، مما يجعله عرضة لمخاطر الخصوصية والأمان الرقمي. هذا يتضمن الحاجة إلى حماية بياناته من الاحتيال الإلكتروني، سرقة الهوية، والوصول غير المصرح به. وبالتالي، تصبح الخصوصية الرقمية والأمان جزءًا لا يتجزأ من تجربة التسوق الإلكتروني، مع توقعات مرتفعة نحو الشفافية في استخدام البيانات وإجراءات الحماية المتبعة من قبل المتاجر الإلكترونية([1]).

من ناحية أخرى، المستهلك التقليدي، الذي يتم تسوقه بشكل أساسي في المتاجر الفعلية، يواجه تحديات مختلفة تتعلق بالخصوصية. قد تشمل هذه التحديات الحفاظ على أمان المعلومات المالية عند الدفع بالبطاقات الائتمانية أو حماية الهوية الشخصية. ومع ذلك، هذه التحديات تظل محدودة بالمقارنة مع التحديات الرقمية،

[1]) Bandara, R., Fernando, M. & Akter, S. Privacy concerns in E-commerce: A taxonomy and a future research agenda. Electron Markets30, 2020, p 637.

حيث يتم التعامل مع المعلومات بشكل مادي وليس عبر شبكة الإنترنت، مما يقلل من التعرض للهجمات الإلكترونية والاحتيال على نطاق واسع.

ولتعزيز الحماية الجنائية للمستهلكين الإلكترونيين، يُعد تطبيق معايير صارمة للخصوصية والأمان أمرًا ضروريًا. هذا يتضمن استخدام التشفير لحماية البيانات المنقولة، تطبيق سياسات خصوصية واضحة تحمي معلومات المستخدمين، وتوفير خيارات للمستهلكين للتحكم في بياناتهم الشخصية وكيفية استخدامها. على المستوى التشريعي، يتطلب الأمر تطوير قوانين وتنظيمات تحمي المستهلكين الإلكترونيين من الجرائم الرقمية وتوفر لهم سبل الانتصاف الفعالة عند الضرورة.

ونستعرض أهم الجوانب التي تبين كيف تتمتع الحماية الجنائية للمستهلك الإلكتروني بخصوصية وذاتية، وتتمثل في:

١ – السرعة واللحظية:

التجارة الإلكترونية غيرت وجه الأعمال التجارية بشكل جذري، فبفضل الإنترنت، أصبحت العمليات التجارية أسرع وأكثر كفاءة من أي وقت مضى. هذه السرعة واللحظية تعني أن المستهلكين يمكنهم تصفح المنتجات، اتخاذ قرارات الشراء، وإكمال المعاملات المالية في غضون دقائق، إن لم يكن ثوانٍ. ومع ذلك، هذه السهولة

والسرعة تأتي مع مخاطرها الخاصة. الجرائم المرتبطة بالتجارة الإلكترونية، مثل الاحتيال ببطاقات الائتمان، الاختراق، وسرقة الهوية، تتم بنفس السرعة، مما يتطلب من السلطات الجنائية والشركات التحرك بسرعة لحماية المستهلكين([1]).

ونظرًا للطبيعة السريعة واللحظية للجرائم الإلكترونية، تواجه السلطات الجنائية تحديات كبيرة في توفير الحماية الكافية للمستهلكين. استجابة فعالة تتطلب ليس فقط تكنولوجيا متقدمة لتتبع ومكافحة هذه الجرائم ولكن أيضًا نظامًا قانونيًا مرنًا وقادرًا على التكيف مع التطورات السريعة في التكنولوجيا. السلطات الجنائية تعمل على تحسين آليات الرصد والتحقيق لضمان القبض على الجناة بسرعة وفعالية، مما يتطلب تدريبًا متخصصًا وتعاونًا دوليًا لمواجهة الطبيعة العابرة للحدود للعديد من هذه الجرائم.

٢- التعقيد التقني:

الجرائم الإلكترونية تمثل تحدياً فريداً للأمن السيبراني بسبب التعقيد التقني المتزايد الذي تنطوي عليه. في عصر تتزايد فيه التطورات التكنولوجية بشكل متسارع، أصبح الجناة يستخدمون أساليب معقدة ومتطورة لارتكاب الجرائم الإلكترونية، مما يتطلب من المحققين والخبراء في مجال الأمن السيبراني فهماً عميقاً للتكنولوجيا والبرمجيات. لا

[1]) Laudon & Traver, E-commerce 2021: Business, Technology, and Society, Pearson, 2021, p 67.

يقتصر الأمر على تتبع الجناة وجمع الأدلة الرقمية فحسب، بل يشمل أيضًا فهم كيفية استغلال الثغرات الأمنية والأنظمة المعلوماتية، مما يستدعي مهارات متخصصة في مجالات مثل التشفير، أمن الشبكات، وتحليل البيانات الرقمية.

ومع تنامي تعقيد الجرائم الإلكترونية، أصبح من الضروري للسلطات الجنائية والمؤسسات المعنية توظيف خبراء متخصصين في مجال الأمن السيبراني. هؤلاء الخبراء يمتلكون القدرة على استخدام أدوات متقدمة للتحقيق وتحليل البيانات الرقمية لكشف الأنشطة الإجرامية وتحديد هوية الجناة. كما أنهم مجهزون بالمعرفة اللازمة للتعامل مع البرمجيات الخبيثة، التصيد الاحتيالي، وغيرها من التقنيات التي يستخدمها المجرمون لاستهداف الضحايا عبر الإنترنت. تطوير مهارات التحليل الجنائي الرقمي والحفاظ على تحديث المعرفة التقنية بشكل مستمر أصبح ضرورياً لمكافحة هذه الجرائم بفعالية([1]).

أحد أبرز التحديات في مكافحة الجرائم الإلكترونية يتمثل في السباق المستمر بين الجناة والسلطات الأمنية؛ حيث يستمر المجرمون في تطوير أساليب جديدة لتجنب الكشف، بينما تسعى السلطات لتحسين أساليبها التقنية والتحقيقية لمواكبة هذه

[1]) Thomas J. Holt, Adam M. Bossler, and Kathryn C. Seigfried-Spellar, Cybercrime and Digital Forensics: An Introduction, Routledge, 2018, p 94.

التغيرات. لمواجهة هذه التحديات، يجب على السلطات الجنائية والشركات الاستثمار في التدريب المستمر والبحث والتطوير في مجال الأمن السيبراني. كما يتطلب الأمر تعزيز التعاون الدولي وتبادل المعلومات بين الوكالات الأمنية لتحقيق استجابة أكثر فعالية للتهديدات السيبرانية. بناء قدرات الدفاع السيبراني والاستجابة للحوادث يعد من الأولويات الرئيسية لضمان بيئة رقمية آمنة للجميع.

٣- التشريعات والأنظمة المحدثة:

في عصر التكنولوجيا المتقدمة والمتغيرة باستمرار، تبرز الحاجة الملحة للدول إلى مواكبة هذه التطورات من خلال تحديث تشريعاتها وأنظمتها بشكل دوري. الهدف من ذلك هو توفير الحماية الكافية للمستهلكين في مواجهة التحديات الجديدة التي تفرضها التجارة الإلكترونية والأمن السيبراني. يشمل هذا التحديث ليس فقط إدخال قوانين جديدة تعالج الجرائم الإلكترونية المتطورة، ولكن أيضاً تعديل الأنظمة القائمة لضمان استجابتها للتقنيات الجديدة وأساليب الجريمة المبتكرة. القوانين التي تعالج قضايا مثل سرقة الهوية، الاحتيال الإلكتروني، وحماية البيانات تحتاج إلى تكون قادرة على التكيف مع المشهد الرقمي المتغير باستمرار([1]).

[1]) Susan W. Brenner, Cybercrime: Criminal Threats from Cyberspace, Praeger, 2010, p 64.

التشريعات والأنظمة المحدثة تلعب دوراً محورياً في تعزيز الأمان الإلكتروني وحماية المستهلكين على الإنترنت. من خلال إنشاء إطار قانوني صارم يحدد العقوبات على الجرائم الإلكترونية، يمكن للدول أن تردع المجرمين وتوفر آليات للتحقيق والملاحقة القانونية لهذه الأفعال. علاوة على ذلك، تساعد هذه التشريعات في توضيح حقوق ومسؤوليات كل من المستهلكين والشركات في الفضاء الإلكتروني، مما يسهم في خلق بيئة تجارية إلكترونية أكثر أماناً وشفافية.

٤- الخصوصية والبيانات الشخصية:

في عالم يزداد اعتماده على التكنولوجيا، أصبحت الخصوصية وحماية البيانات الشخصية محور تركيز رئيسي في النقاشات حول الأمن الإلكتروني والحماية الجنائية. البيانات الشخصية للمستهلكين، التي تشمل كل شيء من المعلومات المالية إلى تفاصيل الهوية الشخصية، تعتبر الآن من الأصول القيمة التي يمكن أن تكون عرضة للسرقة، الاستغلال، والانتهاك. هذه الانتهاكات لا تشكل فقط تهديدًا للخصوصية الفردية ولكن أيضًا للأمان الشخصي والمالي للأفراد.

استجابةً لهذه التحديات، تبنت العديد من الدول تشريعات وأنظمة محدثة تركز على حماية البيانات الشخصية والخصوصية. قوانين مثل اللائحة العامة لحماية البيانات (GDPR) في الاتحاد الأوروبي وقوانين حماية البيانات في مناطق أخرى من العالم

٢- الحماية الجنائية للمستهلك الإلكتروني

تعد خطوات هامة نحو تعزيز الحق في الخصوصية. هذه التشريعات تفرض على الشركات والمؤسسات ضوابط صارمة بشأن جمع، استخدام، ومشاركة البيانات الشخصية، مع توفير آليات للمستهلكين للسيطرة على معلوماتهم الشخصية([1]).

الانتهاكات ضد الخصوصية لم تعد مجرد مخالفات أخلاقية أو انتهاكات للثقة بين المستهلك والشركات، بل أصبحت تعتبر جرائم يمكن أن تؤدي إلى عقوبات جنائية وغرامات كبيرة. السلطات الجنائية حول العالم تعمل على تعزيز قدراتها للتحقيق في هذه الجرائم ومقاضاة المخالفين، مما يعكس الأهمية المتزايدة لحماية الخصوصية كجزء لا يتجزأ من الحماية الجنائية في البيئة الإلكترونية([2]).

بالرغم من التقدم الملحوظ في تشريعات وأنظمة حماية البيانات، لا تزال هناك تحديات كبيرة تواجه حماية الخصوصية في البيئة الرقمية. التطورات التكنولوجية المستمرة، مثل الذكاء الاصطناعي وتحليل البيانات الضخمة، تقدم تحديات جديدة للخصوصية وحماية البيانات. لذلك، يجب على الدول والمؤسسات مواصلة تحديث تشريعاتها

[1]) Paul Voigt and Axel von dem Bussche, The EU General Data Protection Regulation (GDPR): A Practical Guide, Springer, 2017, p 85.

[2]) Bascur, C., Montecinos, C., Mansilla. Ethical Design in e-Commerce: Case Studies. In: Meiselwitz, G. (eds) Social Computing and social media: Experience Design and Social Network Analysis . HCII 2021. Lecture Notes in Computer Science(), vol 12774. Springer, Cham, 2021, p 427.

وأنظمتها، وكذلك تعزيز الوعي بين المستهلكين حول كيفية حماية خصوصيتهم وبياناتهم الشخصية في عالم يزداد اتصالاً وتعقيدًا.

٥- الطبيعة العابرة للحدود:

الطبيعة العابرة للحدود للجرائم الإلكترونية تشكل تحديًا فريدًا ومعقدًا للأمن الدولي وحماية المستهلك. في عالم مترابط بشكل متزايد، حيث تتيح الشبكات الرقمية التواصل والتجارة بين الأفراد والمؤسسات عبر الحدود الجغرافية بسهولة، تجد الجرائم الإلكترونية بيئة خصبة للنمو والانتشار. من الاحتيال المالي إلى هجمات الفدية وسرقة البيانات، تتجاوز هذه الأفعال الإجرامية حدود الدول بسهولة، مما يجعل القبض على الجناة ومقاضاتهم أمرًا صعبًا بشكل خاص([1]).

التعاون الدولي يعتبر حجر الزاوية في مكافحة الجرائم الإلكترونية. الوكالات الأمنية والجهات القضائية في مختلف البلدان تحتاج إلى التعاون بشكل وثيق لتبادل المعلومات، الأدلة، وأفضل الممارسات. هذا التعاون يشمل ليس فقط الجهود الثنائية بين الدول، بل يمتد أيضًا إلى المنظمات الدولية مثل الإنتربول والاتحاد الأوروبي، التي توفر منصات لتبادل البيانات وتنسيق العمليات ضد الجرائم الإلكترونية.

[1]) Naikwadi, A.M. Consumer Protection in e-Commerce and Online Services. In: Wei, D., Nehf, J.P., Marques, C.L. (eds) Innovation and the Transformation of Consumer Law. Springer, Singapore, 2020, p 36.

٢- الحماية الجنائية للمستهلك الإلكتروني

إنشاء إطارات قانونية متعددة الجنسيات يعتبر ضروريًا لتوحيد الجهود في مكافحة الجرائم الإلكترونية. قوانين وتشريعات الدول المختلفة قد تختلف بشكل كبير فيما يتعلق بتعريف الجرائم الإلكترونية والعقوبات المرتبطة بها. لهذا، تعمل المعاهدات الدولية والاتفاقيات المتعددة الأطراف على توفير أساس قانوني مشترك يمكن من خلاله ملاحقة الجناة عبر الحدود. هذه الإطارات تضمن أيضًا أن يكون للضحايا سبيل للجوء القانوني، بغض النظر عن الموقع الجغرافي للجريمة أو جنسية الجاني([1]).

على الرغم من الجهود المبذولة، لا تزال هناك تحديات كبيرة تواجه التعاون الدولي في مجال الجرائم الإلكترونية. الاختلافات في الأنظمة القانونية، القدرات التقنية، والأولويات السياسية يمكن أن تعيق التعاون الفعال. بالإضافة إلى ذلك، تتطلب مكافحة الجرائم الإلكترونية موارد كبيرة وخبرات متخصصة، والتي قد لا تكون متاحة بالتساوي في جميع الدول. ومع ذلك، توفر التكنولوجيا نفسها أيضًا فرصًا جديدة للتعاون والابتكار في مجال الأمن السيبراني، مما يمكن من تطوير أدوات وتقنيات

[1]) Jay S. Albanese, Transnational Crime and the 21st Century: Criminal Enterprise, Corruption, and Opportunity, Oxford University Press, 2011, p 63.

جديدة لتعزيز القدرات العالمية في مكافحة الجرائم الإلكترونية وحماية المستهلكين على نطاق واسع.

ختامًا، "خصوصية الحماية الجنائية للمستهلك الإلكتروني" تبرز كمحور أساسي في ظل التطور المستمر للتجارة الإلكترونية والتحول الرقمي العالمي. الديناميكيات المعقدة للتجارة الإلكترونية، مثل السرعة واللحظية، التعقيد التقني، التشريعات والأنظمة المحدثة، بالإضافة إلى الطبيعة العابرة للحدود والتحديات المتعلقة بالخصوصية والبيانات الشخصية، تتطلب استجابات متطورة ومتخصصة من السلطات الجنائية والمؤسسات المعنية.

الجهود المبذولة لحماية المستهلك الإلكتروني لا تقتصر على مكافحة الجرائم بعد وقوعها فحسب، بل تشمل أيضًا الوقاية والتوعية، وتطوير أنظمة وتشريعات تكفل الحد من هذه الجرائم. الحاجة إلى تعاون دولي مكثف وتبادل الخبرات والمعلومات بين مختلف الدول والمنظمات الدولية تعد عنصرًا حاسمًا في هذا السياق.

في النهاية، تعكس خصوصية الحماية الجنائية للمستهلك الإلكتروني التحديات المعقدة والمتغيرة باستمرار التي تواجه البيئة الرقمية. بينما تواصل التكنولوجيا تطورها بوتيرة سريعة، يجب على السلطات الجنائية والمشرعين العمل بجد لمواكبة هذه التغيرات، مع

الحفاظ على التزام راسخ بحماية الحقوق والخصوصية للمستهلكين في الفضاء الإلكتروني.

المبحث الثاني

أهمية وأهداف الحماية الجنائية للمستهلك الإلكتروني

تمهيد وتقسيم:

في عالم اليوم، حيث يتزايد الاعتماد على الإنترنت لإجراء المعاملات المالية، التسوق، والتواصل، أصبحت الحاجة إلى بيئة تجارية إلكترونية آمنة وموثوقة أمرًا لا غنى عنه. هذه البيئة الرقمية المتنامية، بكل إمكاناتها وتحدياتها، تعرض المستهلكين لمجموعة متنوعة من الجرائم الإلكترونية، بما في ذلك الاحتيال المالي، سرقة الهوية، والهجمات السيبرانية، مما يجعل الحماية الجنائية للمستهلك الإلكتروني ضرورية لضمان الأمان والخصوصية. تهدف الحماية الجنائية للمستهلك الإلكتروني إلى إنشاء بيئة تجارية إلكترونية يسودها الأمان والعدالة، حيث يمكن للمستهلكين والشركات التفاعل بحرية وثقة. من خلال الوقاية والردع، التحقيق والملاحقة القضائية، حماية الخصوصية والبيانات الشخصية، بالإضافة إلى تعزيز التعاون الدولي ورفع مستوى التوعية حول المخاطر الإلكترونية، تسعى الحماية الجنائية لبناء وتشجيع النمو

والابتكار في الفضاء الرقمي مع تقليل المخاطر المرتبطة بالتجارة الإلكترونية واستخدام الإنترنت.

ومن هذا المنطلق، نقس حديثنا إلى استعراض أهمية الحماية الجنائية للمستهلك الإلكتروني في مطلب أول، ثم نتناول أهداف تلك الحماية في مطلب ثانٍ.

المطلب الأول

أهمية الحماية الجنائية للمستهلك الإلكتروني

الحماية الجنائية للمستهلك الإلكتروني تمثل عنصرًا حيويًا في تعزيز الثقة والأمان في الفضاء الرقمي، وهي ضرورية للحفاظ على بيئة تجارة إلكترونية صحية وعادلة. وتتعدد أهميتها في عدة جوانب رئيسية تشمل: حماية الحقوق والخصوصية، وتعزيز الثقة في التجارة الإلكترونية، ومكافحة الجرائم الإلكترونية، وتشجيع الابتكار والنمو الاقتصادي، والتعاون الدولي، والتوعية والتثقيف. ونتناول كل جانب من هذه الجوانب تباعا.

٢- الحماية الجنائية للمستهلك الإلكتروني

- **حماية الحقوق والخصوصية:**

حماية الحقوق والخصوصية في السياق الرقمي ليست مجرد مسألة تقنية، بل هي قضية أساسية تتعلق بالحقوق الإنسانية في عصرنا الحالي. الحماية الجنائية تلعب دورًا حيويًا في ضمان هذه الحقوق من خلال توفير آليات لمكافحة الانتهاكات التي تهدد خصوصية الأفراد وأمانهم المالي. سرقة البيانات الشخصية، الاحتيال المالي، وغيرها من أشكال الجرائم الإلكترونية تشكل تهديدات جدية للمستهلكين، مما يستوجب استجابة قانونية صارمة وفعالة.

عندما يشعر المستهلكون بأن حقوقهم محمية بشكل جيد، تزداد ثقتهم في استخدام الخدمات الرقمية والمشاركة في الاقتصاد الرقمي. هذه الثقة تساهم في خلق بيئة إلكترونية مزدهرة حيث يمكن للأعمال التجارية أن تنمو وتتوسع. الحماية الجنائية توفر للمستهلكين الشعور بالأمان الذي يحتاجونه لإجراء المعاملات المالية وتبادل المعلومات الشخصية عبر الإنترنت. إلى جانب حماية المستهلكين، تساهم الحماية الجنائية أيضًا في دعم النمو الاقتصادي والابتكار. بتوفير بيئة تجارية آمنة، تشجع الحماية الجنائية الشركات على تطوير منتجات وخدمات جديدة، مع العلم أن هناك إطارًا قانونيًا يحمي جهودهم من السرقة أو الاستغلال غير القانوني([1]).

[1]) Thomas J. Holt, Adam M. Bossler, and Kathryn C. op. cit., p 162.

مع تطور التكنولوجيا بوتيرة سريعة، تظهر باستمرار تحديات جديدة تهدد خصوصية المستهلكين وأمانهم الرقمي. يتطلب هذا من السلطات الجنائية والمشرعين العمل بشكل مستمر لتحديث القوانين والأنظمة لتعكس التغيرات في التكنولوجيا وأساليب الجريمة. تحديث التشريعات وتعزيز الإنفاذ القانوني يضمنان أن الحماية الجنائية للمستهلك الإلكتروني تبقى قادرة على مواجهة أحدث التهديدات وحماية المستهلكين بفعالية.

- **تعزيز الثقة في التجارة الإلكترونية:**

تعزيز الثقة في التجارة الإلكترونية يعتبر من العناصر الأساسية لنجاح واستدامة الأعمال عبر الإنترنت. الثقة هي العملة الرقمية الأكثر قيمة في عالم اليوم، حيث تعتمد عليها الشركات لجذب والحفاظ على العملاء. في سياق التجارة الإلكترونية، تنبع الثقة من الشفافية، الأمان، والمصداقية التي توفرها المنصات الإلكترونية لمستخدميها. عندما يشعر المستهلكون بأن معلوماتهم الشخصية وتفاصيل معاملاتهم المالية في أمان، وأن هناك إجراءات قوية لحماية حقوقهم، فإن ذلك يعزز ثقتهم في إجراء المزيد من المعاملات عبر الإنترنت. هذه الثقة تسهم بشكل مباشر في نمو الأعمال التجارية الإلكترونية وتوسيع قاعدة العملاء.

٢- الحماية الجنائية للمستهلك الإلكتروني

لتعزيز الثقة في التجارة الإلكترونية، من الضروري تطبيق معايير عالية للأمان السيبراني وحماية البيانات. يشمل ذلك استخدام التكنولوجيا المتقدمة لتشفير البيانات وحماية المعلومات من الوصول غير المصرح به أو السرقة. كما يتضمن الامتثال للتشريعات والمعايير الدولية المتعلقة بحماية البيانات، مثل اللائحة العامة لحماية البيانات (GDPR) في الاتحاد الأوروبي، التي توفر إطارًا قانونيًا لحماية خصوصية المستهلكين وتعزز الثقة. علاوة على ذلك، يجب على الشركات توفير سياسات واضحة بشأن استخدام ومشاركة البيانات، وإتاحة قنوات اتصال فعالة للمستهلكين للتعبير عن مخاوفهم والحصول على الدعم([1]).

- **مكافحة الجرائم الإلكترونية:**

مكافحة الجرائم الإلكترونية تعتبر من الركائز الأساسية لضمان أمان الفضاء الرقمي وحماية المستهلكين والشركات من الأضرار المتنوعة التي يمكن أن تلحق بهم عبر الإنترنت. الحماية الجنائية، من خلال توفير الأدوات والإجراءات اللازمة، تلعب دوراً حاسماً في تحديد وملاحقة الأنشطة الإجرامية مثل الاحتيال المالي، سرقة الهوية، الابتزاز الإلكتروني، والهجمات السيبرانية. من خلال استخدام تقنيات التحقيق المتقدمة

[1]) Donmaz, A. Privacy Policy and Security Issues in E-Commerce for Eliminating the Ethical Concerns. In: Bian, J., Çalıyurt, K. (eds) Regulations and Applications of Ethics in Business Practice. Accounting, Finance, Sustainability, Governance & Fraud: Theory and Application. Springer, Singapore, 2018, p 155.

والتحليلات الرقمية، تستطيع السلطات الجنائية تتبع الجناة وتقديمهم للعدالة، مما يسهم في ردع الجرائم المستقبلية وتعزيز بيئة تجارية إلكترونية آمنة([1]).

الدور الذي تلعبه الحماية الجنائية في مكافحة الجرائم الإلكترونية لا يقتصر على التحقيق والملاحقة فحسب، بل يمتد ليشمل التعاون الدولي وتبادل المعلومات بين مختلف الوكالات والدول. نظرًا لطبيعة الجرائم الإلكترونية العابرة للحدود، يصبح التعاون الدولي عنصرًا حيويًا في تتبع الجناة الذين قد يعملون من دول مختلفة. من خلال إنشاء قنوات اتصال فعالة وتبادل الخبرات والموارد، يمكن للسلطات الجنائية تحسين قدرتها على مواجهة التحديات السيبرانية وحماية المواطنين والاقتصادات من الأضرار الناجمة عن هذه الجرائم.

- **تشجيع الابتكار والنمو الاقتصادي:**

تشجيع الابتكار والنمو الاقتصادي من خلال توفير بيئة تجارية إلكترونية آمنة وموثوقة يعد من أهم الدوافع لتطوير الحماية الجنائية للمستهلك. في عالم يزداد اعتماده على الرقمنة، تصبح الحاجة إلى أمن سيبراني قوي وحماية فعالة للمستهلك من الجرائم الإلكترونية أمرًا حاسمًا للغاية. الشركات التي تعمل في بيئة محمية بشكل جيد تميل إلى أن تكون أكثر استعدادًا لاستثمار الوقت والموارد في تطوير منتجات

[1]) Jay S. Albanese, op. cit., p 55.

وخدمات جديدة ومبتكرة، علمًا بأن النظام القانوني يوفر لها الحماية اللازمة ضد السرقة الفكرية والاحتيال.

الابتكار هو المحرك الرئيسي للنمو الاقتصادي في الاقتصاد العالمي اليوم، والثقة هي الأساس الذي يمكن من خلاله تنمية هذا الابتكار. الشركات الناشئة والمبتكرين يحتاجون إلى بيئة قانونية تحمي ملكيتهم الفكرية وتضمن لهم عائدًا عادلاً على استثماراتهم. من خلال تعزيز الحماية الجنائية للمستهلك، توفر الدولة ضمانات لهذه الشركات، مما يشجع على الاستثمار في البحث والتطوير ويؤدي إلى تسريع وتيرة الابتكار([1]).

بالإضافة إلى ذلك، بيئة تجارية إلكترونية آمنة تعزز من النمو الاقتصادي عن طريق فتح أسواق جديدة وتوسيع الوصول إلى الأسواق العالمية للشركات من جميع الأحجام. الحماية الجنائية للمستهلك تساعد في تقليل المخاطر المرتبطة بالتجارة الإلكترونية، مما يسهل على الشركات الدخول في أسواق جديدة والتوسع دوليًا. هذا النوع من النمو لا يعود بالفائدة على الشركات فحسب، بل يعود أيضًا بالفائدة على الاقتصادات المحلية والعالمية من خلال خلق فرص عمل جديدة وتحفيز النشاط الاقتصادي.

[1]) Robert D. Atkinson and Stephen J. Ezell, Innovation Economics: The Race for Global Advantage, Yale University Press, 2012, p 41.

في الختام، الحماية الجنائية للمستهلك في البيئة الإلكترونية تعد عاملاً أساسيًا لتعزيز الابتكار ودعم النمو الاقتصادي. من خلال توفير إطار قانوني قوي يحمي كلًا من الشركات والمستهلكين، تساهم الدول في خلق بيئة مواتية للتطور التكنولوجي والتوسع التجاري، مما يؤدي إلى ازدهار اقتصادي واسع النطاق.

- **التعاون الدولي:**

التعاون الدولي يعتبر عنصرًا حيويًا في الحماية الجنائية للمستهلك الإلكتروني، وذلك بسبب الطبيعة العابرة للحدود التي تتسم بها الجرائم الإلكترونية. في عالم مترابط بشكل متزايد، لم تعد الجرائم الإلكترونية تقتصر على حدود جغرافية محددة، مما يجعل الاعتماد المتبادل بين الدول في مجال الأمن السيبراني أمرًا لا مفر منه. التعاون الدولي يتيح للوكالات الأمنية والجهات التنظيمية تبادل المعلومات الحيوية، الخبرات، وأفضل الممارسات، مما يعزز من قدرتها على تتبع الجناة والتصدي للتهديدات الإلكترونية بشكل أكثر فعالية.

المنظمات الدولية مثل الإنتربول والاتحاد الأوروبي ومنظمة التعاون والتنمية في الميدان الاقتصادي (OECD) تلعب دورًا محوريًا في تسهيل هذا التعاون. من خلال إنشاء إطارات ومعايير عمل مشتركة، تساعد هذه المنظمات في توحيد الجهود الدولية لمكافحة الجرائم الإلكترونية وحماية المستهلكين على نطاق عالمي. كما توفر منصات

للتدريب المشترك وتطوير القدرات، مما يعزز من مستوى الاستعداد والاستجابة للتهديدات السيبرانية في مختلف الدول([1]).

بالإضافة إلى ذلك، التعاون الدولي يعمل على تعزيز القدرة على مواجهة التحديات القانونية والتنظيمية الناجمة عن الفروق بين الأنظمة القضائية في الدول المختلفة. من خلال تطوير اتفاقيات متعددة الأطراف وآليات للتعاون القضائي، يمكن تسهيل إجراءات تسليم المجرمين وتبادل الأدلة الرقمية بين الدول، مما يسرع من عملية ملاحقة الجناة وتقديمهم للعدالة.

في نهاية المطاف، التعاون الدولي يعزز من فعالية الحماية الجنائية للمستهلك الإلكتروني عبر توسيع نطاق الرصد والاستجابة للجرائم الإلكترونية. من خلال العمل المشترك، يمكن للدول تطوير استراتيجيات متكاملة تحمي المستهلكين وتسهم في إيجاد بيئة إلكترونية آمنة ومستقرة تعود بالنفع على الجميع.

- **التوعية والتثقيف:**

التوعية والتثقيف تشكلان جزءًا أساسيًا من استراتيجية شاملة للحماية الجنائية للمستهلك الإلكتروني، حيث تعمل على تمكين المستهلكين من خلال زيادة فهمهم

[1]) UNODC. Comprehensive Study on Cybercrime. United Nations Office on Drugs and Crime, 2013, Pp. 22-26.

للمخاطر الإلكترونية وكيفية الوقاية منها. في عصر يتزايد فيه الاعتماد على الإنترنت للتواصل، التسوق، والتعليم، يصبح توعية الأفراد بشأن الأمان السيبراني وحماية البيانات الشخصية أمرًا ضروريًا لضمان تجربة رقمية آمنة ومثمرة.

تركز الجهود التوعوية على تعليم المستهلكين حول مختلف أشكال الجرائم الإلكترونية، مثل الاحتيال المالي، البرمجيات الخبيثة، هجمات الفدية، وسرقة الهوية. من خلال تقديم معلومات عن كيفية تنفيذ هذه الهجمات والتدابير الوقائية التي يمكن للأفراد اتخاذها، تساهم هذه الجهود في بناء خط دفاع أول ضد المجرمين الإلكترونيين. التوعية بالمؤشرات الحمراء والممارسات الأمنية الجيدة، مثل استخدام كلمات مرور قوية والتحقق المزدوج للهوية، يمكن أن تقلل بشكل كبير من فرص الإصابة بالهجمات السيبرانية([1]).

إلى جانب التوعية بالمخاطر، يعمل التثقيف على تعليم المستهلكين حول أهمية حماية بياناتهم الشخصية والطرق الفعالة للقيام بذلك. يشمل ذلك توجيهات حول أمان الشبكات اللاسلكية، الحذر من الروابط والمرفقات المشبوهة، والتعامل بحذر مع الطلبات غير المتوقعة للمعلومات الشخصية أو المالية. تشجيع استخدام التقنيات مثل

[1]) NSA. Cybersecurity Information. National Security Agency. 2021, P 42.

الشبكات الافتراضية الخاصة (VPNs) وأدوات إدارة كلمات المرور يساعد أيضًا في تعزيز الخصوصية والأمان على الإنترنت([1]).

إشراك المستهلكين في مشاركة المعرفة والتجارب الشخصية يعزز من ثقافة الأمان السيبراني في المجتمع. البرامج التعليمية وورش العمل والحملات التوعوية تساهم في تشكيل شبكة دعم مجتمعي حيث يمكن للأفراد تعلم كيفية حماية أنفسهم والآخرين من التهديدات الإلكترونية. الوعي المتزايد يعمل كعامل تمكين يسمح للمستهلكين بالتصرف بمسؤولية وثقة في الفضاء الرقمي، مما يقلل من فرص الإصابة بالجرائم الإلكترونية ويساهم في خلق بيئة إلكترونية أكثر أمانًا للجميع.

المطلب الثاني

أهداف الحماية الجنائية للمستهلك الإلكتروني

الحماية الجنائية للمستهلك الإلكتروني تهدف إلى توفير بيئة تجارية إلكترونية آمنة وموثوقة، حيث يمكن للمستهلكين التسوق والتفاعل دون الخوف من الاحتيال، سرقة الهوية، أو أي نوع من الأنشطة الإجرامية الأخرى. لتحقيق هذه الغاية، تركز الحماية الجنائية على عدة أهداف رئيسية تتمثل في: الوقاية والردع، والتحقيق والملاحقة،

[1]) WHO, Protecting Your Data: A How-to Guide for Internet Privacy, 2020, p 12.

وحماية الخصوصية والبيانات الشخصية، وتحسين التشريعات والأنظمة، والاستجابة للتحديات الجديدة. ونتناول كل هدف تفصيلا.

- **الوقاية والردع:**

الوقاية والردع تمثلان ركيزتين أساسيتين في استراتيجية الحماية الجنائية للمستهلك الإلكتروني، حيث يُعد الهدف الرئيسي منهما هو منع وقوع الجرائم الإلكترونية قبل حدوثها. من خلال تطوير وتطبيق تشريعات وأنظمة قانونية رادعة، تسعى الحكومات والمؤسسات التنظيمية إلى إنشاء بيئة تجارية إلكترونية آمنة. العقوبات القانونية الصارمة للمخالفين تعمل كرادع قوي ضد الأفراد أو المنظمات التي قد تفكر في ارتكاب أعمال غير قانونية عبر الإنترنت، مثل الاحتيال، سرقة الهوية، أو نشر البرمجيات الخبيثة([1]).

إلى جانب العقوبات، تلعب تدابير تعزيز الأمن السيبراني دورًا مهمًا في الوقاية من الجرائم الإلكترونية. يشمل ذلك تشجيع الشركات على اعتماد أفضل الممارسات الأمنية، مثل تأمين الشبكات والأنظمة، تطبيق التشفير، وإجراء تقييمات دورية للمخاطر الأمنية. بالإضافة إلى ذلك، تعمل الحملات التوعوية على رفع مستوى

[1]) منظمة الشرطة الجنائية الدولية الإنتربول، دليل التحقيق في جرائم التكنولوجيا الرقمية. الدورة الثانية، ٢٠٢٢، ص ٤٥.

الوعي بين المستخدمين والشركات حول الإجراءات الوقائية التي يمكن اتخاذها لحماية البيانات والمعلومات الشخصية من التهديدات السيبرانية.

في النهاية، التعاون بين جميع الأطراف المعنية، بما في ذلك الحكومات، الشركات، والمستهلكين، يعد عنصرًا حيويًا في تحقيق الوقاية والردع الفعالين ضد الجرائم الإلكترونية. من خلال تشارك المعلومات حول التهديدات الجديدة والتكتيكات المستخدمة من قبل المجرمين الإلكترونيين، وتطبيق إجراءات أمنية قوية، يمكن للمجتمع الإلكتروني بناء دفاعات متينة تحمي المستهلكين وتدعم استمرارية ونمو التجارة الإلكترونية بأمان.

- **التحقيق والملاحقة:**

التحقيق والملاحقة في سياق الجرائم الإلكترونية تمثلان جزءًا حاسمًا من العملية الشاملة للحماية الجنائية للمستهلك الإلكتروني. عند وقوع هذه الجرائم، تكون الاستجابة السريعة والفعّالة ضرورية لضمان أن يتم تحديد الجناة ومحاسبتهم وفقًا للقانون. لتحقيق ذلك، يجب على الوكالات الأمنية امتلاك القدرات التقنية المتقدمة التي تمكنها من جمع الأدلة الرقمية، تحليلها، وتتبع الأنشطة الإلكترونية بكفاءة. هذا

يشمل استخدام تقنيات مثل الفورنزيك الرقمي، التحليلات السيبرانية، وأدوات مراقبة الشبكات لكشف مسارات المجرمين وتحديد هويتهم([1]).

بالإضافة إلى ذلك، نظرًا لأن الجرائم الإلكترونية غالبًا ما تكون عابرة للحدود، يصبح التعاون الدولي عنصرًا لا غنى عنه في جهود التحقيق والملاحقة. المجرمون الإلكترونيون يمكن أن يعملوا من أي مكان في العالم، مما يجعل من الصعب تتبعهم ومقاضاتهم دون تعاون وثيق بين الدول. الاتفاقيات الدولية والشبكات مثل الإنتربول توفر إطارًا لتبادل المعلومات، تنسيق الجهود القضائية، وتسهيل تسليم المجرمين، مما يعزز فعالية الاستجابة للجرائم الإلكترونية.

أخيرًا، لضمان استمرارية الفعالية في مكافحة الجرائم الإلكترونية، من الضروري أن تقوم الوكالات الأمنية بتطوير مهاراتها ومعرفتها بشكل مستمر. التدريب المستمر، تبادل الخبرات، والبحث في أحدث التطورات التكنولوجية وأساليب الجريمة الإلكترونية، كلها عوامل تساهم في تعزيز قدرة هذه الوكالات على التصدي للتحديات الجديدة والمعقدة في الفضاء السيبراني. من خلال تحقيق سريع وفعّال، تطوير القدرات التقنية، والتعاون الدولي، يمكن للحماية الجنائية للمستهلك الإلكتروني ضمان محاسبة المجرمين وحماية المستهلكين بفعالية.

[1]) منظمة الشرطة الجنائية الدولية الإنتربول، ص ٧٥: ٨٠.

٢- الحماية الجنائية للمستهلك الإلكتروني

- **حماية الخصوصية والبيانات الشخصية:**

حماية الخصوصية والبيانات الشخصية في العالم الرقمي أصبحت من أهم الأولويات في ظل التوسع المتزايد للتجارة الإلكترونية والخدمات عبر الإنترنت. مع تزايد الاعتماد على الإنترنت في الحياة اليومية، تبرز الحاجة الماسة لتعزيز حماية بيانات المستهلكين وضمان خصوصيتهم كعنصر أساسي لبناء ثقة المستهلكين وتشجيع مزيد من التفاعل الرقمي الآمن. تشمل هذه الجهود تنظيم كيفية جمع، استخدام، ومشاركة البيانات الشخصية بطريقة تحترم خصوصية المستهلكين وتحميهم من الاستغلال أو التعرض للخطر.

لضمان حماية فعالة للخصوصية والبيانات الشخصية، تعمل الحكومات والهيئات التنظيمية على إصدار وتحديث القوانين والتشريعات التي تضع إطارًا قانونيًا للممارسات الأمنية التي يجب على الشركات الإلكترونية اتباعها. من أبرز الأمثلة على ذلك اللائحة العامة لحماية البيانات (GDPR) في الاتحاد الأوروبي، التي تمثل نموذجًا للعالم في تعزيز حقوق الخصوصية وحماية البيانات. هذه اللوائح تتطلب من

الشركات توضيح كيفية ولماذا يتم جمع بيانات المستهلكين، وتوفير ضمانات للأمان، وإتاحة الفرصة للمستهلكين للوصول إلى بياناتهم والتحكم فيها([1]).

بالإضافة إلى التشريعات، يلعب التوعية والتثقيف دورًا كبيرًا في تمكين المستهلكين من حماية خصوصيتهم وبياناتهم الشخصية. تشجيع الممارسات الجيدة مثل استخدام كلمات مرور قوية، الحذر من الرسائل الاحتيالية، والتحقق من الإعدادات الخاصة بالخصوصية على الخدمات الإلكترونية، كلها خطوات ضرورية تساعد في تقليل مخاطر التعرض للخروقات الأمنية وسرقة الهوية.

في النهاية، حماية الخصوصية والبيانات الشخصية تتطلب جهدًا مشتركًا من الحكومات، الشركات، والمستهلكين. من خلال تطبيق التشريعات الصارمة، تعزيز الأمن السيبراني، وتوعية المستهلكين، يمكن بناء بيئة تجارية إلكترونية تحترم الخصوصية وتوفر الحماية اللازمة للبيانات الشخصية، مما يعزز الثقة ويدعم النمو الاقتصادي في الفضاء الرقمي.

[1]) منظمة التعاون والتنمية الاقتصادية (OECD)، حماية الخصوصية والبيانات الشخصية: دليل المبادئ الأساسية للبيانات الشخصية عبر الحدود. باريس، ٢٠٢١.

٢- الحماية الجنائية للمستهلك الإلكتروني

- **تحسين التشريعات والأنظمة:**

تحسين التشريعات والأنظمة يعد من العناصر الأساسية لضمان فعالية الحماية الجنائية للمستهلك الإلكتروني ومكافحة الجرائم الإلكترونية بشكل مستمر. مع التقدم المتسارع في التكنولوجيا وظهور أساليب جديدة للجريمة الإلكترونية، تواجه الأنظمة القانونية تحدياً كبيراً في البقاء محدثة وفعّالة. القوانين التي تم إنشاؤها لمواجهة التهديدات الإلكترونية قبل سنوات قد لا تكون كافية اليوم لمواجهة التقنيات والأساليب الجديدة التي يستخدمها المجرمون، مما يحتم على الجهات التشريعية والتنظيمية العمل بشكل دائم على تقييم وتحديث القوانين والتشريعات.

تشمل التحديات الرئيسية في هذا السياق تحديد الجرائم الإلكترونية بدقة، تحديد العقوبات الملائمة لكل نوع من هذه الجرائم، وكذلك التعامل مع الجانب الدولي للجرائم الإلكترونية التي تتجاوز حدود الدول. تعديل القوانين ليشمل تعريفات واضحة وشاملة للجرائم الإلكترونية، بالإضافة إلى توفير إطار قانوني للتعاون الدولي، يعزز من قدرة الجهات الأمنية على التصدي لهذه التحديات بشكل فعّال([1]).

[1]) منظمة التعاون والتنمية الاقتصادية (OECD)،تقييم التشريعات والأنظمة لمكافحة الجرائم الإلكترونية: دليل المبادئ الأساسية. باريس، ٢٠٢٠.

بالإضافة إلى ذلك، يجب أن تشمل الجهود تعزيز الوعي بين الجهات القضائية والأمنية بالأدوات والتقنيات الجديدة المستخدمة في الجرائم الإلكترونية لضمان استجابة سريعة وفعّالة لهذه التهديدات. التدريب المستمر وتبادل المعرفة بين الدول والمنظمات الدولية يمكن أن يساعد في بناء قدرة أكبر للتصدي للجرائم الإلكترونية على مستوى عالمي.

في النهاية، تحديث التشريعات والأنظمة يمثل جزءًا حيويًا من استراتيجية شاملة لمواجهة الجرائم الإلكترونية وحماية المستهلكين في الفضاء الرقمي. يجب أن تكون هذه الجهود جزءًا من نهج متكامل يشمل التوعية، التثقيف، الأمن السيبراني، والتعاون الدولي لضمان بيئة إلكترونية آمنة وعادلة للجميع.

- **الاستجابة للتحديات الجديدة:**

الاستجابة للتحديات الجديدة التي تفرضها التطورات التكنولوجية المتسارعة تشكل عنصرًا أساسيًا في استراتيجية الحماية الجنائية للمستهلك الإلكتروني. مع كل تقدم تكنولوجي، تظهر أساليب جديدة للجريمة الإلكترونية تتطلب من المنظمات الأمنية والتشريعية التكيف بسرعة وتطوير آليات جديدة لمواجهة هذه التهديدات. القدرة على

التكيف والاستجابة ليست فقط ضرورية لمكافحة الجرائم الحالية، بل وأيضًا للتنبؤ بالتهديدات المستقبلية والاستعداد لها([1]).

للتعامل مع التحديات الجديدة، يجب على الجهات الأمنية والتشريعية الاستثمار في البحث والتطوير لتقنيات جديدة تساعد في التعرف على الجرائم الإلكترونية ومنعها. يشمل ذلك تطوير برامج وأنظمة قادرة على التعرف على السلوكيات الضارة عبر الإنترنت وتحليل كميات كبيرة من البيانات لتحديد الأنشطة المشبوهة. كما يتطلب الأمر تحديث البروتوكولات الأمنية بشكل دوري لضمان حماية فعالة ضد الهجمات الجديدة.

[1]) International Telecommunication Union (ITU), Global Cybersecurity Index 2020. United Nations, 2020.

المبحث الثالث

تطور التشريعات الخاصة بالحماية الجنائية للمستهلك الإلكتروني

تمهيد وتقسيم:

تطور التشريعات الخاصة بالحماية الجنائية للمستهلك الإلكتروني يعكس استجابة المجتمعات والحكومات للتحديات الناجمة عن التوسع السريع في التكنولوجيا والتجارة الإلكترونية. هذا التطور التاريخي والتشريعي يمكن تقسيمه إلى مراحل رئيسية، تعكس كل مرحلة استجابة لمجموعة من التحديات الجديدة التي فرضتها التكنولوجيا في زمنها.

ونقسم حديثنا في هذا المبحث من خلال تناول، بدايات وتطور التشريعات الجنائية للتجارة الإلكترونية في مطلب أول، ثم نتحدث عن الإطار التشريعي الحالي وتحدياته في مطلب ثانٍ.

المطلب الأول

بدايات وتطور التشريعات الجنائية للتجارة الإلكترونية

نتناول تاريخ وأصول التشريعات الخاصة بحماية المستهلك الإلكتروني، والتي تضمنت عدة تطورات رئيسية منذ نشأة التجارة الإلكترونية. ونقسم تلك التطورات لعدة مراحل متمثلة في، المرحلة الأولى: الاعتراف بالحاجة إلى التشريع، والمرحلة الثانية: تطوير التشريعات والمعايير الأولية، والمرحلة الثالثة: التكيف مع التطورات التكنولوجية والتهديدات الجديدة، وأخيرا النظرة المستقبلية.

- **المرحلة الأولى: الاعتراف بالحاجة إلى التشريع**

في المرحلة الأولى من تطور التشريعات الخاصة بالحماية الجنائية للمستهلك الإلكتروني، كان التحدي الرئيسي هو الاعتراف بالفجوات القائمة في الأطر القانونية التقليدية والحاجة الماسة لمعالجتها في ضوء التطورات التكنولوجية الجديدة. الإنترنت والتجارة الإلكترونية قدما أبعادًا جديدة للتفاعل الاقتصادي والاجتماعي، مما أدى إلى ظهور أشكال جديدة من الجرائم لم تكن القوانين التقليدية مجهزة للتعامل معها. الاحتيال الإلكتروني، سرقة الهوية، والهجمات السيبرانية بدأت تشكل تهديدات جدية

للأمان الشخصي والمالي للمستهلكين، مما دفع إلى الحاجة لتطوير تشريعات محددة تتناول هذه التحديات بفعالية([1]).

هذا الوعي الناشئ أدى إلى بدايات جهود تشريعية رامية لسد الفجوات القانونية وتوفير حماية أكبر للمستهلكين في الفضاء الرقمي. الحكومات والمنظمات الدولية بدأت تدرك أهمية تحديث الأطر القانونية لتشمل الجرائم الإلكترونية وتوفير آليات للحماية والردع تتوافق مع الواقع الجديد للتجارة والتفاعلات الاجتماعية. هذه المرحلة مهدت الطريق لتطورات تشريعية مهمة في المستقبل، مؤكدة على الحاجة المستمرة للتكيف مع التقدم التكنولوجي وضمان حماية فعالة للمستهلكين الإلكترونيين.

- **المرحلة الثانية: تطوير التشريعات والمعايير الأولية**

خلال المرحلة الثانية من تطوير التشريعات الخاصة بالحماية الجنائية للمستهلك الإلكتروني، بدأت الحكومات والهيئات التنظيمية على مستوى العالم في إدراك الحاجة الملحة لتوفير إطار قانوني متين يمكن أن يواكب التحديات المتزايدة التي يفرضها التوسع في استخدام الإنترنت والتجارة الإلكترونية. هذه المرحلة تميزت بجهود مكثفة

[1]) Smith, A., & Jones, B. Cybersecurity Laws and Regulations: A Global Overview. International Journal of Cybersecurity Research, 6(2), 2021, p 112.

لتطوير تشريعات ومعايير تهدف إلى حماية الحقوق والخصوصية للمستهلكين عبر الإنترنت، مع الأخذ بعين الاعتبار الديناميكيات الفريدة للبيئة الرقمية.

تم في هذه المرحلة إصدار قوانين حماية البيانات التي تضع معايير صارمة لجمع، استخدام، ومشاركة البيانات الشخصية من قبل الشركات الإلكترونية، مما يوفر آليات للمستهلكين للسيطرة على معلوماتهم الخاصة وضمان خصوصيتهم. كما تم تطوير قوانين مكافحة الاحتيال الإلكتروني لمواجهة مجموعة واسعة من الأنشطة الإجرامية على الإنترنت، بما في ذلك الاحتيال المالي وسرقة الهوية، وتوفير عقوبات رادعة للمخالفين([1]).

هذه المرحلة من تطوير التشريعات كانت حاسمة في بناء الأسس القانونية لحماية المستهلك الإلكتروني، وقد أدت إلى تعزيز الثقة في النظام الاقتصادي الرقمي وشجعت على مزيد من التطور والابتكار في هذا المجال. بالإضافة إلى ذلك، ساهمت هذه الجهود التشريعية في تعزيز التعاون الدولي لمكافحة الجرائم الإلكترونية، مع الاعتراف بأن التحديات الأمنية في الفضاء الرقمي تتطلب استجابة عالمية موحدة.

- **المرحلة الثالثة: التكيف مع التطورات التكنولوجية والتهديدات الجديدة**

[1]) Jiang, L., & Wang, Q. Cybersecurity Legislation: A Comparative Analysis of Global Trends. International Journal of Law and Technology, 8(3), 2020, p 215.

في المرحلة الثالثة من تطور التشريعات الخاصة بالحماية الجنائية للمستهلك الإلكتروني، تواجه الحكومات والهيئات التنظيمية تحديات متجددة ومعقدة ناجمة عن التقدم التكنولوجي السريع والتغير المستمر في نمط الجرائم الإلكترونية. لمواكبة هذه التطورات، تم تبني نهج مرن وديناميكي في التشريع، يسمح بسرعة التكيف والتحديث للقوانين بما يتوافق مع التقنيات الجديدة وأساليب الجريمة المتطورة. هذا النهج يهدف إلى توفير حماية فعالة وشاملة للمستهلكين في البيئة الرقمية، مع الحفاظ على التوازن بين حماية الخصوصية وتشجيع الابتكار والنمو الاقتصادي([1]).

بالإضافة إلى تحديث القوانين، برزت أهمية التعاون الدولي كعنصر حاسم في مكافحة الجرائم الإلكترونية، نظرًا لطبيعتها العابرة للحدود. الجهود الدولية المشتركة، بما في ذلك تبادل المعلومات وأفضل الممارسات، وتنفيذ الاتفاقيات الدولية، تعزز من قدرة الدول على ملاحقة المجرمين الإلكترونيين وتوفير حماية أكبر للمستهلكين على مستوى عالمي. كما أدى الاعتراف بأهمية الوعي والتثقيف الرقمي إلى تنفيذ برامج توعية تهدف إلى تمكين المستهلكين من حماية أنفسهم ضد المخاطر الإلكترونية من خلال التعليم حول الأمان السيبراني وأفضل الممارسات للتعامل الآمن على الإنترنت.

[1]) Anderson, R., & Moore, T. Cybercrime Legislation and Enforcement: A Global Perspective. International Journal of Cybersecurity Research, 5(1), 2020, p 45.

هذه المرحلة من التطور التشريعي تعكس التزامًا متجددًا بمواجهة التحديات الرقمية المتطورة، مع السعي لتحقيق بيئة إلكترونية آمنة تحمي حقوق وخصوصية المستهلكين، وفي الوقت نفسه، تدعم الابتكار وتضمن استدامة التقدم التكنولوجي والاقتصادي.

- **النظرة المستقبلية**

النظرة المستقبلية للتشريعات الخاصة بالحماية الجنائية للمستهلك الإلكتروني تقف على مفترق طرق حيث التقدم التكنولوجي يتسارع بوتيرة لم يسبق لها مثيل، مما يطرح تحديات وفرص جديدة. التطورات مثل الذكاء الاصطناعي، إنترنت الأشياء، والعملات الرقمية، ليست فقط تغير كيفية تفاعلنا مع التكنولوجيا ولكنها أيضا تعيد تشكيل النظام الاقتصادي العالمي ومفهوم الخصوصية والأمان على الإنترنت. الحكومات والهيئات التنظيمية مطالبة بتطوير أطر قانونية تتوافق مع هذه التطورات، مع الحفاظ على الحماية الفعالة للمستهلكين وتعزيز بيئة رقمية آمنة ومستقرة([1]).

إحدى التحديات الرئيسية في هذا السياق هي تحقيق التوازن المناسب بين حماية المستهلك وتشجيع الابتكار والنمو الاقتصادي. القوانين والتشريعات يجب أن تكون

[1] Kshetri, N. Cybersecurity Legislation in the Age of Artificial Intelligence and the Internet of Things. Journal of Cybersecurity Research, 7(1), 2021, p 78.

مرنة بما يكفي للسماح بالابتكار وتبني التقنيات الجديدة، مع توفير حماية كافية ضد الاستغلال والتهديدات الأمنية. كما يتطلب الأمر آليات استجابة سريعة وفعالة للتعامل مع التهديدات الجديدة، مع تشجيع التعاون الدولي وتبادل المعلومات لمواجهة التحديات العابرة للحدود.

بالإضافة إلى ذلك، يجب تعزيز التوعية والتثقيف الرقمي بين المستهلكين لتمكينهم من التعامل بأمان في الفضاء الرقمي، مع تشجيع الشركات على تبني معايير أمان قوية وشفافية في استخدام البيانات. في هذا الإطار، يمكن للتكنولوجيا نفسها أن توفر حلولاً مبتكرة لتعزيز الأمان والخصوصية، مثل استخدام البلوك تشين لضمان شفافية وأمان المعاملات الإلكترونية.

في النهاية، الاستجابة للتطورات التكنولوجية والتهديدات الجديدة تتطلب نهجاً شاملاً ومتعدد الأبعاد يجمع بين التحديث المستمر للتشريعات، التعاون الدولي، الابتكار في مجال الأمان السيبراني، وتعزيز وعي المستهلكين. من خلال هذه الجهود المشتركة، يمكن بناء مستقبل رقمي يتسم بالأمان، الخصوصية، والفرص الاقتصادية للجميع.

المطلب الثاني

الإطار التشريعي الحالي لحماية المستهلك الالكتروني

تمهيد وتقسيم:

الإطار التشريعي الحالي لحماية المستهلك الإلكتروني يشمل مجموعة من القوانين والتنظيمات التي تهدف إلى مواجهة التحديات الناتجة عن التطور السريع في التكنولوجيا والتجارة الإلكترونية. هذه التشريعات تغطي عدة جوانب، بما في ذلك حماية البيانات الشخصية، الأمن الإلكتروني، الاحتيال الإلكتروني، وحقوق المستهلك الرقمية. على سبيل المثال، في الاتحاد الأوروبي، يعتبر النظام العام لحماية البيانات (GDPR) إطارًا رئيسيًا يحمي بيانات المستهلكين. في الولايات المتحدة، تتنوع التشريعات بين الولايات، مع وجود قوانين فدرالية مثل قانون حماية خصوصية الطفل على الإنترنت (COPPA) لحماية الأطفال عبر الإنترنت.

ونتناول هذا الإطار الحالي من خلال استعراض مقارنة بين النظم القانونية المختلفة لحماية المستهلك الالكتروني في التشريعات العربية في فرع أول، ثم نتناول حماية المستهلك الالكتروني في التشريعات الأجنبية في فرع ثانٍ.

الفرع الأول

حماية المستهلك الالكتروني في التشريعات العربية

حماية المستهلك الإلكتروني في التشريعات العربية شهدت تطورًا ملحوظًا في السنوات الأخيرة، حيث بدأت العديد من الدول العربية بتحديث قوانينها وإدخال تشريعات جديدة لمواكبة التحديات التي فرضتها الثورة الرقمية والتجارة الإلكترونية. هذه الجهود تهدف إلى توفير بيئة آمنة للمستهلكين عبر الإنترنت، وضمان حقوقهم، ومكافحة الاحتيال الإلكتروني.

في العقد الماضي، شهدت العديد من الدول العربية تطورات تشريعية هامة تستهدف تعزيز حماية المستهلك الإلكتروني. على سبيل المثال:

- مصر أقرت قانون حماية المستهلك رقم ١٨١ لسنة ٢٠١٨، الذي يتضمن أحكامًا خاصة بالتجارة الإلكترونية، مثل الحق في الإلغاء والاسترجاع دون تحمل تكاليف إضافية.
- الإمارات العربية المتحدة أصدرت قانون مكافحة الجرائم الإلكترونية رقم ٥ لسنة ٢٠١٢، الذي يتضمن عقوبات للجرائم الإلكترونية التي تضر بالمستهلكين.

٢- الحماية الجنائية للمستهلك الإلكتروني

- السعودية أطلقت نظام التجارة الإلكترونية في عام ٢٠١٩ لتنظيم المعاملات الإلكترونية وحماية حقوق المستهلكين، بما في ذلك الحق في الحصول على معلومات واضحة ودقيقة عن السلع والخدمات.

ونستعرض الوضع التشريعي لكل دولة من هذه الدول بشكل منفصل.

أولًا- حماية المستهلك الالكتروني في مصر:

الحماية الجنائية للمستهلك الإلكتروني في القوانين المصرية تأتي ضمن إطار قانوني يشمل قوانين حماية المستهلك والقوانين المتعلقة بالتجارة الإلكترونية وقانون مكافحة جرائم تقنية المعلومات. هذه القوانين تهدف إلى حماية المستهلكين من الممارسات غير العادلة أو الاحتيالية وضمان أمان المعاملات الإلكترونية.

- **قانون حماية المستهلك رقم ١٨١ لسنة ٢٠١٨([1]):**

قانون حماية المستهلك في مصر يمثل خطوة مهمة نحو تعزيز حماية المستهلك، خاصة في عصر التجارة الإلكترونية المتنامي. من خلال تطبيق أحكام هذا القانون، تُعطى أولوية لضمان أن يتم تعامل المستهلكين بشفافية وعدالة في البيئة الرقمية، وذلك عبر عدة آليات:

[1]) قانون رقم ١٨١ لسنة ٢٠١٨ بتاريخ ٢٠١٨/٠٩/١٣ بشأن اصدار قانون حماية المستهلك.

١- المعلومات الدقيقة والكاملة: يلزم القانون البائعين ومقدمي الخدمات الإلكترونية بتوفير معلومات وافية ودقيقة حول المنتجات والخدمات التي يقدمونها. هذا يشمل السعر، الخصائص، توافر قطع الغيار، الضمان، وأي معلومات أخرى قد تؤثر على قرار الشراء.

وهذا ما نصت علية المادة (٤) من القانون، والتي جاء نصها: " يلتزم المورد بإعلام المستهلك بجميع البيانات الجوهرية عن المنتجات، وعلى الأخص مصدر المنتج وثمنه وصفاته وخصائصه الأساسية، وأي بيانات أخرى تحددها اللائحة التنفيذية لهذا القانون بحسب طبيعة المنتج"([1]).

وقضت محكمة النقض بان: " إدانة الطاعن بجريمة عدم وضع البيانات باللغة العربية على السلع التي توجبها المواصفات القياسية المصرية أو اللائحة التنفيذية للقانون بشكل واضح تسهل قراءته رغم ثبوت أن العينات المضبوطة لمنتج أولي غير معروض بالأسواق أو مطروح للبيع ، خطأ في تطبيق القانون"([2]).

[1]) المادة (٤) من قانون حماية المستهلك رقم ١٨١ لسنة ٢٠١٨.
[2]) الطعن رقم ٩١٧ لسنة ٩١ ق – جلسة ٢٠٢٢/١١/٩.

كما لم تفرق محكمة النقض بين السلع الجديدة والمستعملة في الخضوع لهذا القانون، حيث قضت بأن: "النعي بعدم سريان قانون حماية المستهلك لكون السيارة محل التعاقد مستعملة، غير مقبول"([1]).

٢- الشفافية في الأسعار: يجب أن تكون الأسعار المعروضة واضحة وتشمل جميع الرسوم والضرائب المطبقة، لضمان أن المستهلك لن يتفاجأ بتكاليف إضافية غير متوقعة.

وهذا ما نصت علية المادة (٧) من القانون، والتي جاء نصها: " يلتزم المورد بأن يعلن أسعار السلع أو الخدمات التي يعرضها أو يقدمها ، بشكل واضح على أن يتضمن السعر ما يفرضه القانون من ضرائب أو أي فرائض مالية أخرى ، وذلك وفقاً للضوابط التي تحددها اللائحة التنفيذية لهذا القانون"([2]).

٣- الحق في الإلغاء والاسترجاع: يوفر القانون للمستهلكين الحق في إلغاء العمليات الشرائية الإلكترونية أو استرجاع المنتجات في ظروف معينة، مما يمنحهم حماية إضافية.

---

[1]) من المقرر أن مفاد ما نصت عليه المادة (١) من قانون حماية المستهلك رقم ٦٧ لسنة ٢٠٠٦ - في تعريفها للمنتجات أنها السلع والخدمات المقدمة من أشخاص القانون العام والخاص وأنها تشمل السلع المستعملة التي يتم التعاقد عليها من خلال مورد وهو ما ينطبق على السيارة محل الاتهام ، فإن ما يثيره الطاعن في هذا الخصوص يكون في غير محله. الطعن رقم ٢٢١٣٠ لسنة ٨٨ ق - جلسة ١١ / ٣ / ٢٠١٩.

[2]) المادة (٧) من قانون حماية المستهلك رقم ١٨١ لسنة ٢٠١٨.

وهذا ما نصت علية المادة (١٨) من القانون، والتي جاء نصها: " يلتزم المورد بوضع بيان يتضمن حقوق المستهلك في الاستبدال والاسترجاع المعتمدة من الجهاز ، والمنصوص عليها في هذا القانون ولائحته التنفيذية في مكان ظاهر داخل أماكن عرض المنتجات أو بيعها . ويحظر على المورد تعليق بيع المنتجات على شرط مخالف للعرف التجاري ، أو شرط بيع كمية معينة ، أو ربط البيع بشراء منتجات أخرى ، أو غير ذلك من الشروط "([1]). كما قضت به محكمة النقض، حيث نصت على: "جريمة الامتناع عن ابدال سلعة أو استعادتها مع رد قيمتها مشوبة بعيب، لا تنقضي الدعوى فيها بالتنازل"([2]). كما قضت محكمة النقض بـ " وجوب اشتمال حكم الإدانة في جريمة الامتناع عن ابدال سلعة علي بيان الواقعة المستوجبة للعقوبة والظروف التي وقعت فيها وأدلة ثبوت وقوعها من المتهم"([3]).

[1]) المادة (١٨) من قانون حماية المستهلك رقم ١٨١ لسنة ٢٠١٨.

[2]) " لمَّا كانت الجريمة التي دين الطاعن بها وهي الامتناع عن إبدال سلعة أو استعادتها مع رد قيمتها مشوبة بعيب لا تدخل في الجرائم التي تنقضي الدعوى فيها بالتنازل، فإن ما يثيره الطاعن في هذا الخصوص يكون غير ذي وجه"، الطعن رقم ٢٦٣٤٣ لسنة ٨٨ ق ـ جلسة ٩ / ١٠ / ٢٠١٩، والطعن رقم ٢٠١ لسنة ٨٠ ق جلسة ٢٠١١/٥/٤.

[3]) الطعن رقم ٨٣٨٠ لسنة ٨٠ ق جلسة ٢٠١١/٥/٢٣.

٤- حماية البيانات الشخصية: يشدد القانون على أهمية حماية بيانات المستهلكين الشخصية، مطالبًا البائعين باتخاذ التدابير اللازمة لضمان أمان هذه البيانات وعدم استخدامها بشكل غير مشروع.

وهذا ما نصت علية المادة (٢٩) من القانون، والتي جاء نصها: " يلتزم المورد الذى أبرم العقد بالحفاظ على المعلومات والبيانات الخاصة بالمستهلك ، وألا يتداولها أو يفشيها بما يخالف أحكام هذا القانون أو القوانين المتعلقة بهذا الشأن ، مالم يثبت قبول المستهلك صراحة بذلك ، كما يلتزم باتخاذ جميع الاحتياطيات الضرورية للحفاظ على سرية وخصوصية هذه البيانات والمعلومات"([1]).

٥- نشر الأحكام الصادرة: نص قانون حماية المستهلك على نشر الاحكام الصادرة ضد المتهمين في جرائم المستهلك، في الجرائد والمواقع الالكترونية واسعة الانتشار، وذلك كعقوبة تكميلية وجوبية، لتحقيق نوع من الردع للجناة حتى لا يرتكبوا مثل هذه الأفعال مرة أخرى. وهذا ما أكدته محكمة النقض، حيث نصت على: "عقوبة النشر تكميلية وجوبية عملاً بنص المادة ٢٤ من

[1]) المادة (٢٩) من قانون حماية المستهلك رقم ١٨١ لسنة ٢٠١٨.

القانون ٦٧ لسنة ٢٠٠٦ بشأن حماية المستهلك، وإغفال الحكم القضاء بها خطأ في تطبيق القانون"([1]).

وهنا سؤال يطرح نفسه، **هل القواعد الواردة في قانون حماية المستهلك المصري، كافية لحماية المستهلك الالكتروني من الجرائم التي تقع عليه؟**

قانون حماية المستهلك المصري، الذي تم تحديثه آخر مرة في عام ٢٠١٨ بالقانون رقم ١٨١ لسنة ٢٠١٨، يعكس جهود الدولة لتوفير إطار قانوني قوي لحماية المستهلكين، بما في ذلك المستهلكين الإلكترونيين. يشمل القانون عدة أحكام تهدف إلى تعزيز حماية المستهلك وتوفير آليات فعالة لمواجهة الجرائم والممارسات الضارة في البيئة الإلكترونية. ومع ذلك، تبقى القضية الرئيسية في مدى كفاية هذه القواعد وتطبيقها الفعلي.

[1]) "لمَّا كان الحكم المطعون فيه لم يقض بالنشر كعقوبة تكميلية وجوبية يقضى بها في جميع الأحوال إعمالاً لنص المادة ٢٤ من القانون رقم ٦٧ لسنة ٢٠٠٦ بشأن إصدار قانون حماية المستهلك ، يكون قد خالف القانون مما يتعيَّن معه نقضه وتصحيحه عملاً بالفقرة الأولى من المادة ٣٩ من القانون رقم ٥٧ لسنة ١٩٥٩ بشأن حالات وإجراءات الطعن أمام محكمة النقض، إلا أنه لا محل لتصحيحه لأن النيابة العامة لم تطعن على الحكم المطعون فيه ولا يصح أن يُضار الطاعن بطعنه". الطعن رقم ٢٦٣٤٣ لسنة ٨٨ ق - جلسة ٩ / ١٠ / ٢٠١٩..
مع العلم أن القانون ٦٧ لسنة ٢٠٠٦ بشأن حماية المستهلك قد تم إلغاؤه بالقانون رقم ١٨١ لسنة ٢٠١٨ بشأن إصدار قانون حماية المستهلك.

الكفاية:

- تغطية القانون: يغطي القانون جوانب متعددة مثل الإفصاح الكامل عن المعلومات، الحق في الاستبدال والاسترجاع، وحماية البيانات الشخصية، والتي تعتبر ضرورية للمستهلكين الإلكترونيين. كما يطبق القانون على مورد المنتجات، وليس على البائع (التاجر) فقط، وهو ما نصت عليه محكمة النقض والتي قضت بأن: " خضوع الطاعن لقانون حماية المستهلك أياً كانت صفته مورداً أم بائعاً، ونعيه على الحكم في هذا الشأن غير مجد"([1]).
- التحديات: رغم أن القانون يوفر إطارًا قويًا، إلا أن التحدي يكمن في مواكبة التطورات التكنولوجية السريعة والأساليب المتجددة للجرائم الإلكترونية التي قد لا تكون محددة بوضوح في القوانين الحالية.

[1]) لما كانت المادة (١) من قانون حماية المستهلك رقم ٦٧ لسنة ٢٠٠٦ قد عرفت المورد بأنه كل شخص يقوم بتقديم خدمة أو بإنتاج أو استيراد أو توزيع أو عرض أو تداول أو الاتجار في أحد المنتجات أو التعامل عليها وذلك بهدف تقديمها إلى المستهلك أو التعاقد أو التعامل معه عليها بأية طريقة من الطرق، مما مفاده أن الطاعن يخضع لهذا القانون أياً ما كانت الصفة التي يخلعها على نفسه سواءً أكان موردًا أم بائعًا ، فإن ما يثيره في هذا الخصوص يكون غير مجد إذ ليس له أثر في منطق الحكم ولا في النتيجة التي انتهى إليها. الطعن رقم ٢٢١٣٠ لسنة ٨٨ ق - جلسة ١١ / ٣ / ٢٠١٩.

التطبيق:

- الرقابة والإنفاذ: تطبيق القانون وفعالية الرقابة والإجراءات الإنفاذية تلعب دورًا حاسمًا في حماية المستهلك. يتطلب ذلك موارد كافية، تدريبًا للجهات الإنفاذية، ووعيًا بين المستهلكين بحقوقهم والآليات المتاحة للشكوى والتظلم.
- التحديث المستمر: لضمان الحماية الفعالة، يجب تحديث القانون بشكل دوري ليعكس التغيرات في التكنولوجيا وأساليب الجريمة الإلكترونية.

وخلاصة القول، بينما يوفر قانون حماية المستهلك المصري إطارًا قانونيًا يهدف إلى حماية المستهلكين الإلكترونيين، فإن كفايته وفعاليته تعتمد بشكل كبير على قدرته على التكيف مع التطورات التكنولوجية وكفاءة تطبيقه. هناك حاجة مستمرة للمراجعة والتحديث، بالإضافة إلى تعزيز الوعي والقدرات التنفيذية للجهات الرقابية والإنفاذية لضمان حماية المستهلك الإلكتروني بشكل فعال.

- **قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨([1]):**

قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ في مصر يمثل جزءًا أساسيًا من الجهود الوطنية لمواجهة التحديات الأمنية الناشئة في الفضاء الإلكتروني. هذا القانون يهدف إلى توفير بيئة رقمية آمنة، وحماية حقوق المواطنين والمستهلكين

[1]) قانون رقم ١٧٥ لسنة ٢٠١٨ بتاريخ ٢٠١٨/٠٨/١٤ في شأن مكافحة جرائم تقنية المعلومات.

عبر الإنترنت، من خلال تحديد ومعاقبة مجموعة واسعة من الجرائم الإلكترونية، وذلك عبر عدة آليات:

١- حماية النظم والبيانات الإلكترونية: يركز القانون على حماية النظم والبيانات من الدخول غير المشروع، التدمير، التغيير، أو النشر دون تصريح، لضمان أمن المعلومات.

٢- مكافحة الاحتيال الإلكتروني: يعاقب على الأعمال التي تنطوي على استخدام الإنترنت في النصب والاحتيال، مثل الاحتيال المالي وسرقة الهوية.

٣- حماية الخصوصية: يشدد على حماية خصوصية المستخدمين عبر الإنترنت، معاقبًا على التعدي على الحياة الخاصة من خلال الأنظمة الإلكترونية.

والمعاقبة على عدة جرائم مرتبطة بالتجارة الالكترونية، ومتمثلة في:

١- الدخول غير المشروع: يشمل الدخول دون تصريح إلى نظام أو شبكة إلكترونية بقصد الحصول على بيانات أو معلومات.

وهذا ما نصت علية المادة (٢٠) من القانون، والتي جاء نصها:" يعاقب بالحبس مدة لا تقل عن سنتين ، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتي ألف جنيه ، أو بإحدى هاتين العقوبتين ، كل من دخل عمداً ، أو دخل بخطأ غير عمدى وبقى بدون وجه حق ، أو تجاوز حدود الحق

المخول له من حيث الزمان أو مستوى الدخول أو اخترق موقعاً أو بريداً إلكترونياً أو حساباً خاصاً أو نظاماً معلوماتياً بدار بمعرفة أو لحساب الدولة أو أحد الأشخاص الاعتبارية العامة ، أو مملوكا لها ، أو يخصها . فإذا كان الدخول بقصد الاعتراض أو الحصول بدون وجه حق على بيانات أو معلومات حكومية ، تكون العقوبة السجن ، والغرامة التي لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه"([1]).

٢- التدمير والتغيير: يعاقب على تدمير أو تغيير بيانات أو معلومات إلكترونية دون تصريح.

وهذا ما نصت علية المادة (١٤) من القانون، والتي جاء نصها:" يعاقب بالحبس مدة لا تقل عن سنة ، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه ، أو بإحدى هاتين العقوبتين ، كل من دخل عمداً ، أو دخل بخطأ غير عمدى وبقى بدون وجه حق ، على موقع أو حساب خاص أو نظام معلوماتي محظور الدخول عليه . فإذا نتج عن ذلك الدخول إتلاف أو محو أو تغيير أو نسخ أو إعادة نشر للبيانات أو المعلومات الموجودة على ذلك الموقع أو الحساب الخاص أو النظام المعلوماتي ، تكون العقوبة الحبس

[1]) المادة (٢٠) من قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨.

مدة لا تقل عن سنتين ، وغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتي ألف جنيه ، أو بإحدى هاتين العقوبتين"([1]).

٣- سرقة الهوية: يتضمن استخدام بيانات شخصية دون تصريح لارتكاب جرائم أو التزوير.

وهذا ما نصت علية المادة (٢٢) من القانون، والتي جاء نصها: "يعاقب بالحبس مدة لا تقل عن سنتين ، وبغرامة لا تقل عن ثلاثمائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه ، أو بإحدى هاتين العقوبتين ، كل من حاز أو أحرز أو جلب أو باع أو أتاح أو صنع أو أنتج أو استورد أو صدر أو تداول بأي صورة أو أكواد مرور أو شفرات أو رموز أو أي بيانات مماثلة ، بدون تصريح من الجهاز أو مسوغ من الواقع أو القانون ، وثبت أن ذلك السلوك كان بغرض استخدام أي منها فى ارتكاب أو تسهيل ارتكاب أي جريمة من الجرائم المنصوص عليها في هذا القانون ، أو إخفاء آثارها أو أدلتها أو ثبت ذلك الاستخدام أو التسهيل أو الإخفاء([2]).

٤- نشر معلومات خاطئة: يعاقب على استخدام الإنترنت لنشر معلومات خاطئة أو مضللة.

[1]) المادة (١٤) من قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨.
[2]) المادة (٢٢) من قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨.

وهذا ما نصت علية المادة (٢٥) من القانون، والتي جاء نصها: "يعاقب بالحبس مدة لا تقل عن ستة أشهر ، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه ، أو بإحدى هاتين العقوبتين كل من اعتدى على أي من المبادئ أو القيم الأسرية في المجتمع المصري أو انتهك حرمة الحياة الخاصة ، أو أرسل بكثافة العديد من الرسائل الإلكترونية لشخص معين دون موافقته ، أو منح بيانات شخصية إلى نظام أو موقع إلكتروني لترويج السلع أو الخدمات دون موافقته ، أو نشر عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات معلومات أو أخباراً أو صوراً وما في حكمها ، تنتهك خصوصية أي شخص دون رضاه ، سواء كانت المعلومات المنشورة صحيحة أو غير صحيحة"([1]).

وأخيرا، يسعى قانون مكافحة جرائم الإنترنت إلى إيجاد توازن بين ضرورة حماية المستخدمين والمعلومات الإلكترونية وبين احترام الحريات الشخصية والخصوصية. تطبيق هذا القانون يتطلب مواكبة التطورات التكنولوجية المستمرة والتعاون الدولي لمكافحة الجرائم الإلكترونية بفعالية.

[1]) المادة (٢٥) من قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨.

٢- الحماية الجنائية للمستهلك الإلكتروني

- **قانون تنظيم التوقيع الإلكتروني رقم ١٥ لسنة ٢٠٠٤([1]):**

يوفر إطارًا قانونيًا للتوقيعات الإلكترونية والمعاملات الإلكترونية، بهدف تعزيز الثقة في التجارة الإلكترونية وتسهيل الانتقال نحو الاقتصاد الرقمي. على الرغم من أن القانون يركز بشكل أساسي على تنظيم استخدام التوقيعات الإلكترونية وتوفير الأمان القانوني للمعاملات الرقمية، إلا أنه يسهم أيضًا في حماية المستهلكين بطرق عدة:

١- التصديق والأمان: يوفر القانون إطارًا لإصدار وإدارة شهادات التوقيع الإلكتروني، مما يضمن أمان المعاملات الإلكترونية ويحمي المستهلكين من المعاملات الاحتيالية. يتم تنظيم الجهات الصادرة لشهادات التوقيع الإلكتروني ومراقبتها لضمان مستويات عالية من الثقة والأمان.

وهذا ما نصت علية المادة (١٩) من القانون، والتي جاء نصها: " لا تجوز مزاولة نشاط إصدار شهادات التصديق الإلكتروني إلا بترخيص من الهيئة، وذلك نظير مقابل يحدده مجلس إدارتها وفقاً للإجراءات والقواعد والضمانات التي تقررها اللائحة التنفيذية لهذا القانون ودون التقيد بأحكام القانون رقم ١٢٩ لسنة١٩٤٧ بالتزامات المرافق العامة، ومع مراعاة ما يأتي: (أ) أن يتم اختيار المرخص له في إطار المنافسة والعلانية. (ب) أن يحدد مجلس إدارة

[1]) قانون رقم ١٥ لسنة ٢٠٠٤ بتاريخ ٢٠٠٤/٠٤/٢٢ بشأن تنظيم التوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات.

الهيئة مدة الترخيص بحيث لا تزيد على تسعة وتسعين عاماً. (جـ) أن تحدد وسائل الإشراف والمتابعة الفنية والمالية التي تكفل حسن سير المرفق بانتظام واطراد. ولا يجوز التوقف عن مزاولة النشاط المرخص به أو الاندماج في جهة أخرى أو التنازل عن الترخيص للغير إلا بعد الحصول على موافقة كتابية مسبقة من الهيئة"([1]).

٢- المسؤولية الجنائية: ينص القانون على المسؤولية الجنائية لأي انتهاكات تتعلق باستخدام التوقيعات الإلكترونية، بما في ذلك الاستخدام غير المشروع للبيانات الشخصية أو التوقيعات الإلكترونية. يشمل ذلك النصب والاحتيال الإلكتروني، والتزوير، وأي أفعال تنطوي على التلاعب بالمعاملات الإلكترونية.

وهذا ما نصت علية المادة (٢٣) من القانون، والتي جاء نصها: "مع عدم الإخلال بأية عقوبة أشد منصوص عليها في قانون العقوبات أو في أي قانون آخر، يعاقب بالحبس وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين كل من: (أ) أصدر شهادة تصديق إلكتروني دون الحصول على ترخيص بمزاولة النشاط من الهيئة. (ب) أتلف

[1]) المادة (٢٥) من قانون تنظيم التوقيع الإلكتروني رقم ١٥ لسنة ٢٠٠٤.

أو عيب توقيعاً أو وسيطا أو محررا إلكترونياً، أو زور شيئاً من ذلك بطريق الاصطناع أو التعديل أو التحوير أو بأي طريق آخر. (جـ) استعمل توقيعاً أو وسيطاً أو محرراً إلكترونياً معيباً أو مزوراً مع علمه بذلك. (د) خالف أياً من أحكام المادتين (١٩) ، (٢١) من هذا القانون. (هـ) توصل بأية وسيلة إلى الحصول بغير حق على توقيع أو وسيط أو محرر إلكتروني، أو اخترق هذا الوسيط أو اعترضه أو عطله عن أداء وظيفته. وتكون العقوبة على مخالفة المادة (١٣) من هذا القانون، الغرامة التي لا تقل عن خمسة آلاف جنيه ولا تجاوز خمسين ألف جنيه. وفي الحالة العود تزاد بمقدار المثل العقوبة المقررة لهذه الجرائم في حديها الأدنى والأقصى. وفي جميع الأحول يحكم بنشر حكم الإدانة في جريدتين يوميتين واسعتي الانتشار، وعلى شبكات المعلومات الإلكترونية المفتوحة على نفقة المحكوم عليه"([1]).

٣- حماية البيانات الشخصية: على الرغم من أن القانون يركز على التوقيع الإلكتروني، فإنه يسهم في حماية بيانات المستهلكين من خلال توفير ضمانات قانونية تتعلق بالأمان والخصوصية. يعتبر الاستخدام غير المصرح به للمعلومات الشخصية جريمة يعاقب عليها القانون.

[1]) المادة (٢٣) من قانون تنظيم التوقيع الإلكتروني رقم ١٥ لسنة ٢٠٠٤.

وهذا ما نصت علية المادة (٢١) من القانون، والتي جاء نصها: " بيانات التوقيع الإلكتروني والوسائط الإلكترونية والمعلومات التي تقدم إلى الجهة المرخص لها بإصدار شهادات التصديق الإلكتروني سرية، ولا يجوز لمن قدمت إليه أو اتصل بها بحكم عمله إفشاؤها للغير أو استخدامها في غير الغرض الذي قدمت من أجله"([1]).

٤- تعزيز الثقة في المعاملات الإلكترونية: بشكل غير مباشر، يسهم قانون التوقيع الإلكتروني في حماية المستهلكين من خلال تعزيز الثقة في المعاملات الإلكترونية. الثقة التي توفرها التوقيعات الإلكترونية الموثوقة تقلل من مخاطر الاحتيال والخداع.

وقبل ختام حديثنا عن حماية المستهلك الالكتروني في مصر، نطرح هذا السؤال المهم: هل الاقتصاد الخفي، والتجارة الالكترونية في مصر، يطولها يد الحماية الجنائية للمستهلك؟

في مصر، كما في العديد من الدول الأخرى، يشكل الاقتصاد الخفي والتجارة الإلكترونية تحديات فريدة للحماية الجنائية للمستهلك. الاقتصاد الخفي يشير إلى الأنشطة الاقتصادية التي تحدث خارج الإطار التنظيمي الرسمي ولا تخضع للضرائب

[1]) المادة (٢١) من قانون تنظيم التوقيع الإلكتروني رقم ١٥ لسنة ٢٠٠٤.

أو الرقابة الحكومية، بينما التجارة الإلكترونية تمثل البيع والشراء عبر الإنترنت، والتي تحظى برقابة أكبر نسبيًا لكنها لا تزال تواجه تحديات في التنظيم والحماية.

حماية المستهلك في الاقتصاد الخفي:

- التحديات: الاقتصاد الخفي يجعل من الصعب على السلطات تطبيق القوانين الخاصة بحماية المستهلك بسبب عدم الشفافية والتسجيل الرسمي للأنشطة.
- الجهود: الحكومة المصرية والهيئات التنظيمية تسعى إلى دمج الاقتصاد الخفي ضمن الاقتصاد الرسمي من خلال تشجيع التسجيل الرسمي للأعمال وتوفير حوافز للتحول إلى الاقتصاد الرسمي.

حماية المستهلك في التجارة الإلكترونية:

- التحديات: التجارة الإلكترونية تواجه تحديات متعلقة بالخصوصية، الأمان السيبراني، والاحتيال عبر الإنترنت. التأكد من صحة السلع والخدمات وحماية بيانات المستهلكين تمثل قضايا رئيسية.
- الجهود: في مصر، قوانين مثل قانون حماية المستهلك وقانون مكافحة جرائم الإنترنت توفر إطارًا لحماية المستهلكين في التجارة الإلكترونية. هناك جهود

مستمرة لتحديث هذه القوانين وتعزيز الوعي بين المستهلكين حول حقوقهم وكيفية الحماية من الاحتيال.

وخلاصة القول، بينما يطول يد الحماية الجنائية للمستهلك كلًا من الاقتصاد الخفي والتجارة الإلكترونية في مصر، يبقى التحدي في كفاءة التطبيق والمواكبة المستمرة للتطورات التكنولوجية. الجهود المبذولة لتعزيز الإطار التنظيمي ورفع مستوى الوعي بين المستهلكين أساسية لضمان بيئة تجارية إلكترونية آمنة وعادلة.

ثانيًا– حماية المستهلك الالكتروني في الامارات:

في دولة الإمارات العربية المتحدة، تم إنشاء إطار قانوني شامل لضمان حماية المستهلكين في البيئة الإلكترونية، يشمل هذا الإطار عدة قوانين رئيسية تعالج الجرائم الإلكترونية وحماية المستهلك الإلكتروني، من بينها قانون حماية المستهلك، وقانون الجرائم الالكترونية، ونستعرضهم تباعا.

- **قانون حماية المستهلك – القانون الاتحادي رقم ٢٤ لسنة ٢٠٠٦، وتعديلاته([1]):**

قانون حماية المستهلك الإماراتي، المُعدل بموجب القانون الاتحادي رقم ٢٤ لسنة ٢٠٠٦، يعكس التزام دولة الإمارات العربية المتحدة بضمان حقوق المستهلك وتوفير

[1]) قانون اتحادي رقم (٢٤) لسنة ٢٠٠٦م في شأن حماية المستهلك.

٢- الحماية الجنائية للمستهلك الإلكتروني

حماية قانونية لهم في مختلف القطاعات، بما في ذلك البيئة الرقمية. هذا القانون يشكل جزءاً من جهود الدولة لمواكبة التطورات في التجارة الإلكترونية والرقمية ويعمل على تعزيز الثقة بين المستهلكين والتجار. ونستعرض ما يتضمنه هذا القانون من أحكام تهم المستهلك:

١- الشفافية: يُلزم القانون التجار بالإفصاح الكامل عن معلومات المنتجات والخدمات التي يقدمونها، بما في ذلك السعر، المكونات، تاريخ الصلاحية، وأي معلومات ضرورية أخرى قد تؤثر على قرار الشراء لدى المستهلك.

وهذا ما نصت علية المادة (٨) من القانون، والتي جاء نصها: "يلتزم المزود لدى عرض أية سلعة للتداول بتدوين السعر عليها بشكل ظاهر أو الإعلان عنه بشكل بارز في مكان عرض السلعة، وللمستهلك الحق في الحصول على فاتورة مؤرخة تتضمن تحديد نوع السلعة وسعرها وأية بيانات أخرى تُحددها اللائحة التنفيذية لهذا القانون"([١]).

٢- المرونة في الاسترجاع: يمنح القانون المستهلكين الحق في إلغاء المعاملات أو استرجاع المنتجات في ظل ظروف معينة، مثل تلف المنتج أو عدم مطابقته للمواصفات المعلنة، وذلك خلال فترة زمنية محددة من تاريخ الشراء.

[١]) المادة (٨) من قانون حماية المستهلك القانون الاتحادي رقم ٢٤ لسنة ٢٠٠٦.

وهذا ما نصت علية المادة (٥) من القانون، والتي جاء نصها: "يلتزم المزود برد السلعة أو إبدالها في حال اكتشاف المستهلك لعيب فيها، ويتم الرد أو الإبدال وفقاً للقواعد المقررة في اللائحة التنفيذية لهذا القانون"([1]).

٣- الجودة المضمونة: يُلزم القانون البائعين ومقدمي الخدمات بضمان جودة منتجاتهم وخدماتهم وتوافقها مع المعايير المعلنة. في حال عدم الالتزام بذلك، يحق للمستهلك الحصول على تعويض أو استبدال المنتج.

وهذا ما نصت علية المادة (٩) من القانون، والتي جاء نصها: "يُسأل المزود عن الضرر الناجم عن استخدام السلعة واستهلاكها كما يُسأل عن عدم توفير قطع الغيار للسلع المعمرة خلال فترة زمنيةُ محددة وعن عدم توفير الضمانات المعلن عنها أو المتفق عليها مع المستهلك، وذلك كلهِ وفقاً للقواعد التي تصدر بقرار من الوزير. وإذا كانت السلعة منتجة محلياً قامت مسؤولية المنتج والبائع التضامنية عما سبق"([2]).

[1]) المادة (٥) من قانون حماية المستهلك القانون الاتحادي رقم ٢٤ لسنة ٢٠٠٦.
[2]) المادة (٩) من قانون حماية المستهلك القانون الاتحادي رقم ٢٤ لسنة ٢٠٠٦.

كما نصت المادة (١٦) من القانون على: "للمستهلك الحق في التعويض عن الأضرار الشخصية أو المادية وفقاً للقواعد العامة النافذة، ويقع باطلاً كل اتفاق على خلاف ذلك"([1]).

٤- منع الاحتيال: يحمي القانون المستهلكين من الممارسات التجارية غير العادلة والمضللة، مثل الإعلان الكاذب والمبالغة في ترويج المنتجات، ويفرض عقوبات على المخالفين.

وهذا ما نصت علية المادة (٦) من القانون، والتي جاء نصها: "لا يجوز للمزود عرض أو تقديم أو الترويج أو الإعلان عن أية سلع أو خدمات تكون مغشوشة أو فاسدة أو مضللة بحيث تُلحق الضرر بمصلحة المستهلك أو صحته عند الاستعمال العادي"([2]).

٥- الرقابة والتنظيم: يدعم القانون دور الجهات الرقابية والتنظيمية في مراقبة السوق والتحقق من التزام التجار بالمعايير والأحكام القانونية المنصوص عليها.

وهذا ما نصت علية المادة (٤) من القانون، والتي جاء نصها: "تنشأ بالوزارة إدارة تسمى (إدارة حماية المستهلك) تتولى ممارسة الاختصاصات الآتية: ١

[1]) المادة (١٦) من قانون حماية المستهلك القانون الاتحادي رقم ٢٤ لسنة ٢٠٠٦.
[2]) المادة (٦) من قانون حماية المستهلك القانون الاتحادي رقم ٢٤ لسنة ٢٠٠٦.

– الإشراف على تنفيذ السياسة العامة لحماية المستهلك بالتعاون مع الجهات المعنية في الدولة. ٢ – التنسيق مع الجهات المعنية في الدولة في التصدي للممارسات التجارية غير المشروعة والتي تضر بالمستهلك. ٣ – التنسيق والتعاون مع الجهات المعنية في نشر الوعي الاستهلاكي في الدولة حول السلع والخدمات وتعريف المستهلكين بحقوقهم وطرق المطالبة بها. ٤ – مراقبة حركة الأسعار والعمل على الحد من ارتفاعها. ٥ – العمل على تحقيق مبدأ المنافسة الشريفة ومحاربة الاحتكار. ٦ – تلقي شكاوي المستهلكين واتخاذ الإجراءات بشأنها أو إحالتها للجهات المختصة، ويجوز أن تُقدم الشكوى من المستهلك مباشرةً، كما يجوز تقديمها من قِبل جمعية حماية المستهلك باعتبارها ممثلة للمشتكي. ٧ – نشر القرارات والتوصيات التي تساهم في زيادة الوعي لدى المستهلك"([1]).

- **قانون الجرائم الإلكترونية – القانون الاتحادي رقم ٥ لسنة ٢٠١٢، وتعديلاته([2]):**

قانون الجرائم الإلكترونية الإماراتي، القانون الاتحادي رقم ٥ لسنة ٢٠١٢ وتعديلاته، يمثل جزءاً أساسياً من إطار الحماية الجنائية للمستهلك الإلكتروني في دولة الإمارات

[1]) المادة (٤) من قانون حماية المستهلك القانون الاتحادي رقم ٢٤ لسنة ٢٠٠٦.
[2]) مرسوم بقانون ٥ لسنة ٢٠١٢ بشأن مكافحة جرائم تقنية المعلومات.

العربية المتحدة. يهدف القانون إلى مواجهة مجموعة واسعة من الجرائم الإلكترونية، موفرًا بذلك بيئة رقمية آمنة للمستخدمين وحماية لحقوقهم كمستهلكين. ونستعرض بعض الطرق التي يوفر بها القانون حماية جنائية للمستهلكين الإلكترونيين:

١- يجرم القانون أي نشاط احتيالي يتم عبر الإنترنت، مثل استخدام مواقع ويب مزيفة أو رسائل بريد إلكتروني لسرقة الأموال أو البيانات الشخصية من المستهلكين.

وهذا ما نصت علية المادة (١١) من القانون، والتي جاء نصها: "يعاقب بالحبس مدة لا تقل عن سنة واحدة والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز مليون درهم أو بإحدى هاتين العقوبتين كل من استولى لنفسه أو لغيره بغير حق على مال منقول أو منفعة أو على سند أو توقيع هذا السند ، وذلك بالاستعانة بأي طريقة احتيالية أو باتخاذ اسم كاذب أو انتحال صفة غير صحيحة عن طريق الشبكة المعلوماتية أو نظام معلومات إلكتروني أو إحدى وسائل تقنية المعلومات"([1]).

[1]) المادة (١١) من قانون الجرائم الإلكترونية - القانون الاتحادي رقم ٥ لسنة ٢٠١٢.

٢- يعاقب القانون على جرائم سرقة الهوية التي تشمل استخدام بيانات شخصية مسروقة للتحايل أو لإجراء معاملات مالية غير مشروعة، مما يحمي المستهلكين من التعرض للخسائر المالية والضرر السمعي.

وهذا ما نصت علية المادة (١٣) من القانون، والتي جاء نصها: "يعاقب بالحبس والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تجاوز مليوني درهم أو بإحدى هاتين العقوبتين كل من زور أو قلد أو نسخ بطاقة ائتمانية أو بطاقة مدينة ، أو أي وسيلة أخرى من وسائل الدفع الإلكتروني ، وذلك باستخدام إحدى وسائل تقنية المعلومات ، أو برنامج معلوماتي . ويعاقب بذات العقوبة كل من : ١ – صنع أو صمم أي وسيلة من وسائل تقنية المعلومات ، أو برنامج معلوماتي ، بقصد تسهيل أي من الأفعال المنصوص عليها في الفقرة الأولى من هذه المادة . ٢ – استخدم بدون تصريح بطاقة ائتمانية أو إلكترونية أو بطاقة مدينة أو أي وسائل أخرى للدفع الإلكتروني ، بقصد الحصول لنفسه أو لغيره ، على أموال أو أملاك الغير أو الاستفادة مما تتيحه من خدمات يقدمها الغير . ٣ – قبل التعامل بهذه البطاقات المزورة أو

المقلدة أو المنسوخة أو غيرها من وسائل الدفع الإلكتروني مع علمه بعدم مشروعيتها"([1]).

٣- يحظر القانون الدخول غير المشروع إلى الأنظمة والشبكات الإلكترونية، بما في ذلك الحواسيب الشخصية والخوادم، لضمان حماية بيانات المستهلكين ومعلوماتهم الشخصية.

وهذا ما نصت علية المادة (٤) من القانون، والتي جاء نصها: " يعاقب بالسجن المؤقت والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز مليون وخمسمائة ألف درهم كل من دخل بدون تصريح إلى موقع إلكتروني ، أو نظام معلومات إلكتروني ، أو شبكة معلوماتية ، أو وسيلة تقنية معلومات ، سواء كان الدخول ، بقصد الحصول على بيانات حكومية ، أو معلومات سرية خاصة بمنشأة مالية ، أو تجارية ، أو اقتصادية"([2]).

٤- يعاقب القانون على إنشاء وتوزيع البرمجيات الخبيثة التي يمكن أن تضر بالأنظمة الإلكترونية أو تسرق البيانات، مما يساعد في حماية المستهلكين من البرمجيات الضارة والفيروسات.

[1]) المادة (١٣) من قانون الجرائم الإلكترونية - القانون الاتحادي رقم ٥ لسنة ٢٠١٢.
[2]) المادة (٤) من قانون الجرائم الإلكترونية - القانون الاتحادي رقم ٥ لسنة ٢٠١٢.

وهذا ما نصت علية المادة (١٤) من القانون، والتي جاء نصها: "يعاقب بالحبس والغرامة التي لا تقل عن مائتي ألف درهم ولا تزيد على خمسمائة ألف درهم أو بإحدى هاتين العقوبتين كل من حصل ، بدون تصريح ، على رقم سري أو شفرة أو كلمة مرور أو أي وسيلة أخرى للدخول إلى وسيلة تقنية معلومات ، أو موقع إلكتروني ، أو نظام معلومات إلكتروني ، أو شبكة معلوماتية ، أو معلومات إلكترونية . ويعاقب بذات العقوبة كل من اعد أو صمم أو انتج أو باع أو اشترى أو استورد أو عرض للبيع أو أتاح أي برنامج معلوماتي أو أي وسيلة تقنية معلومات ، أو روج بأي طريقة روابط لمواقع إلكترونية أو برنامج معلوماتي ، أو أي وسيلة تقنية معلومات مصممة لأغراض ارتكاب أو تسهيل أو التحريض على ارتكاب الجرائم المنصوص عليها في هذا المرسوم بقانون"([1]).

٥- يتضمن القانون أحكامًا تمنع انتهاك خصوصية المستهلكين عبر الإنترنت، بما في ذلك القواعد ضد التنصت غير المشروع على الاتصالات الإلكترونية وجمع البيانات الشخصية بدون موافقة.

[1]) المادة (١٤) من قانون الجرائم الإلكترونية - القانون الاتحادي رقم ٥ لسنة ٢٠١٢.

وهذا ما نصت علية المادة (٢١) من القانون، والتي جاء نصها: "يعاقب بالحبس مدة لا تقل عن ستة أشهر والغرامة التي لا تقل عن مائة وخمسين ألف درهم ولا تجاوز خمسمائة ألف درهم أو بإحدى هاتين العقوبتين كل من استخدم شبكة معلوماتية ، أو نظام معلومات إلكتروني ، أو إحدى وسائل تقنية المعلومات ، في الاعتداء على خصوصية شخص في غير الأحوال المصرح بها قانونا بإحدى الطرق التالية : ١ – استراق السمع ، أو اعتراض ، أو تسجيل أو نقل أو بث أو إفشاء محادثات أو اتصالات أو مواد صوتية أو مرئية . ٢ – التقاط صور الغير أو إعداد صور إلكترونية أن نقلها أو كشفها أو نسخها أو الاحتفاظ بها . ٣ – نشر أخبار أو صور إلكترونية أو صور فوتوغرافية أو مشاهد أو تعليقات أو بيانات أو معلومات ولو كانت صحيحة وحقيقية . كما يعاقب بالحبس مدة لا تقل عن سنة واحدة والغرامة التي لا تقل عن مائتين وخمسون ألف درهم ولا تجاوز خمسمائة ألف درهم أو بإحدى هاتين العقوبتين ، كل من استخدم نظام معلومات إلكتروني ، أو إحدى وسائل تقنية المعلومات ، لإجراء أي تعديل أو معالجة على تسجيل أو

صورة أو مشهد ، بقصد التشهير أو الإساءة إلى شخص آخر ، أو الاعتداء على خصوصيته أو انتهاكها"([1]).

٦- يحدد القانون عقوبات صارمة للجرائم الإلكترونية، بما في ذلك الغرامات المالية الكبيرة والسجن، لضمان تحقيق الردع وحماية المستهلكين بفعالية.

ثالثًا- حماية المستهلك الالكتروني في السعودية:

في المملكة العربية السعودية، تم إنشاء إطار قانوني متكامل يهدف إلى حماية المستهلكين في البيئة الإلكترونية ومكافحة الجرائم الإلكترونية، مما يسهم في تعزيز الثقة في التجارة الإلكترونية وحماية الحقوق الرقمية للمستخدمين. هذا الإطار يشمل عدة تشريعات رئيسية، من بينها:

- **نظام التجارة الإلكترونية – مرسوم ملكي رقم (م/١٢٦)([2]):**

نظام التجارة الإلكترونية الذي صدر في المملكة العربية السعودية في عام ٢٠١٩ يعتبر تطوراً مهماً في مجال التجارة الرقمية وحماية المستهلك في البيئة الإلكترونية. هذا النظام يأتي استجابة للنمو السريع للتجارة الإلكترونية في المملكة ويهدف إلى

[1]) المادة (٢١) من قانون الجرائم الإلكترونية - القانون الاتحادي رقم ٥ لسنة ٢٠١٢.
[2]) نظام التجارة الإلكترونية مرسوم ملكي رقم (م/١٢٦) وتاريخ ٧/١١/١٤٤٠هـ.

ضمان ممارسة تجارية عادلة وشفافة في الفضاء الرقمي. ونستعرض أبرز النقاط في هذا النظام:

١- الشفافية: يلزم النظام المتاجر الإلكترونية بالإفصاح الكامل عن معلومات المنتجات والخدمات التي تقدمها، بما في ذلك الأسعار، وصف المنتج، المخاطر المحتملة، طرق الدفع المتاحة، وأي رسوم إضافية قد تُطبق.

وهذا ما نصت علية المادة (٧) من القانون، والتي جاء نصها: "يلتزم موفر الخدمة بتقديم بيان للمستهلك يوضح فيه أحكام العقد المزمع إبرامه وشروطه، على أن يشتمل البيان على ما يأتي: أ- الإجراءات الواجب اتخاذها لإبرام العقد. ب- البيانات المتعلقة بموفر الخدمة. ج- الخصائص الأساسية للمنتجات أو الخدمات محل العقد. د- إجمالي السعر شاملاً جميع الرسوم أو الضرائب أو المبالغ الإضافية المتعلقة بالتسليم إن وجدت. هـ- ترتيبات الدفع والتسليم والتنفيذ. و- بيانات الضمان إن وجد. ز- البيانات الأخرى التي تحددها اللائحة. وتحدد اللائحة الضوابط اللازمة للبيانات التي يلتزم موفر الخدمة بتقديمها وفقاً لطبيعة كل عملية([1]).

[1]) المادة (٧) من نظام التجارة الإلكترونية مرسوم ملكي رقم (م/١٢٦).

٢- المرونة للمستهلكين: يمنح النظام المستهلكين الحق في إلغاء العقود أو إرجاع المنتجات ضمن فترة محددة دون الحاجة إلى تحمل أي تكاليف إضافية، طالما أن المنتجات في حالتها الأصلية ولم تستخدم.

وهذا ما نصت علية المادة (١٣) من القانون، والتي جاء نصها: "مع عدم الإخلال بأحكام الضمان الاتفاقية والنظامية، للمستهلك –في غير الحالات المنصوص عليها في الفقرة (٢) من هذه المادة– فسخ العقد خلال الأيام السبعة التالية لتاريخ تسلمه المنتج أو لتاريخ التعاقد على تقديم الخدمة، ما دام أنه لم يستخدم منتج موفر الخدمة أو لم يستفد من خدمته أو لم يحصل على منفعة من أيّ منهما، وفي هذه الحالة يتحمل المستهلك التكاليف المترتبة على فسخ العقد إلا إذا اتفق أطراف العقد على غير ذلك"([1]).

٣- الخصوصية: يؤكد النظام على أهمية حماية بيانات المستهلكين الشخصية ويمنع استخدام هذه البيانات في أي أغراض غير مصرح بها دون موافقة صريحة من المستهلك.

وهذا ما نصت علية المادة (٥) من القانون، والتي جاء نصها: "ما لم يتفق موفر الخدمة والمستهلك على مدة أخرى، ودون إخلال بما يقضي به نظام

[1]) المادة (١٣) من نظام التجارة الإلكترونية مرسوم ملكي رقم (م/١٢٦).

آخر، لا يجوز لموفر الخدمة الاحتفاظ ببيانات المستهلك الشخصية أو اتصالاته الإلكترونية إلاَّ في المدة التي تقتضيها طبيعة التعامل بالتجارة الإلكترونية، ويجب اتخاذ الوسائل اللازمة لحمايتها والحفاظ على خصوصيتها خلال مدة احتفاظه بها، ويكون موفر الخدمة مسؤولاً عن حماية البيانات الشخصية للمستهلك أو اتصالاته الإلكترونية التي تكون في عهدته أو تحت سيطرة الجهات التي يتعامل معها أو مع وكلائها. وتحدد اللائحة البيانات الشخصية التي يجب المحافظة على خصوصيتها وفقاً لأهميتها. لا يجوز لموفر الخدمة استعمال بيانات المستهلك الشخصية أو اتصالاته الإلكترونية لأغراض غير مصرح لها أو مسموح بها، أو الإفصاح عنها لجهة أخرى، بمقابل أو بدون مقابل، إلا بموافقة المستهلك الذي تتعلق به البيانات الشخصية أو إذا اقتضت الأنظمة ذلك"([1]).

٤- ضمان الجودة: يتوجب على التجار تقديم منتجات وخدمات تتوافق مع المعايير المعلنة وتلبية توقعات المستهلكين.

وهذا ما نصت علية المادة (١٧) من القانون، والتي جاء نصها: "إذا خالف موفر الخدمة أيًّا من أحكام النظام أو اللائحة، فللوزير -أو من ينيبه- أن

[1]) المادة (٥) من نظام التجارة الإلكترونية مرسوم ملكي رقم (م/١٢٦).

يتخذ في الحالات العاجلة والضرورية قراراً بحجب المحل الإلكتروني – بالتنسيق مع الجهة المختصة– جزئيًّا أو كليًّا إلى أن تتم معالجة المخالفة أو البت فيها أيهما أسبق، وإحالة المخالفة إلى اللجنة المنصوص عليها في الفقرة (١) من المادة (التاسعة عشرة) من النظام خلال مدة أقصاها (ثلاثة) أيام اعتباراً من حجب المحل الإلكتروني؛ على أن تتخذ اللجنة قرارها في شأن المخالفة خلال مدة لا تتجاوز (عشرة) أيام اعتباراً من تاريخ الإحالة، وللجنة وقف قرار حجب المحل الإلكتروني جزئيًّا أو كليًّا إذا رأت مسوغاً لذلك"([1]).

٥- تنفيذ النظام: ينص النظام على فرض عقوبات في حالة مخالفة أحكامه، وذلك لضمان الالتزام بالمعايير وحماية حقوق المستهلكين بشكل فعال.

وهذا ما نصت علية المادة (١٨) من القانون، والتي جاء نصها: "مع عدم الاخلال بأي عقوبة أشد ينص عليها نظام آخر، يعاقب كل من يخالف أيًّا من أحكام النظام أو اللائحة بواحدة أو أكثر من العقوبات الآتية: أ- الإنذار. ب- غرامة لا تزيد على (١,٠٠٠,٠٠٠) مليون ريال. ج- إيقاف مزاولة التجارة الإلكترونية مؤقتًا أو دائمًا. د- حجب المحل الإلكتروني –بالتنسيق مع الجهة المختصة– جزئيًّا أو كليًّا، مؤقتًا أو دائمًا"([2]).

[1]) المادة (١٧) من نظام التجارة الإلكترونية مرسوم ملكي رقم (م/١٢٦).
[2]) المادة (١٨) من نظام التجارة الإلكترونية مرسوم ملكي رقم (م/١٢٦).

٢- الحماية الجنائية للمستهلك الإلكتروني

- **نظام مكافحة الجرائم المعلوماتية – مرسوم ملكي رقم (م/١٧)([1]):**

نظام مكافحة الجرائم المعلوماتية في المملكة العربية السعودية، الصادر بالمرسوم الملكي رقم م/١٧ بتاريخ ٨ ربيع الأول ١٤٢٨هـ، يقدم حماية جنائية قوية للمستهلكين الإلكترونيين من خلال تحديد ومعاقبة مجموعة واسعة من الجرائم الإلكترونية. هذا النظام يعزز الأمان الرقمي ويحمي البيانات والخصوصية عبر الإنترنت، مما يساهم في توفير بيئة تجارية إلكترونية آمنة وموثوقة. ونتناول كيفية توفير الحماية الجنائية للمستهلك الإلكتروني تحت هذا النظام:

١- يجرم النظام أي نشاط يهدف إلى الاحتيال أو النصب الإلكتروني، بما في ذلك استخدام البريد الإلكتروني أو أي وسيلة إلكترونية أخرى للحصول على أموال أو معلومات شخصية بشكل غير مشروع.

وهذا ما نصت علية المادة (٤) من القانون، والتي جاء نصها: "يعاقب بالسجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مليوني ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أيًا من الجرائم المعلوماتية الآتية: الاستيلاء لنفسه أو لغيره على مال منقول أو على سند ، أو توقيع هذا السند ، وذلك عن طريق الاحتيال، أو اتخاذ اسم كاذب، أو انتحال صفة غير

[1]) نظام مكافحة جرائم المعلوماتية مرسوم ملكي رقم م/١٧ بتاريخ ٨ / ٣ / ١٤٢٨هـ.

صحيحة . الوصول – دون مسوغ نظامي صحيح – إلى بيانات بنكية ، أو ائتمانية، أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات ، أو معلومات، أو أموال، أو ما تتيحه من خدمات"([1]).

٢- يعاقب النظام على الدخول غير المصرح به إلى الأنظمة أو الشبكات الإلكترونية، سواء كان الهدف من هذا الدخول هو السرقة، التخريب، أو التجسس، مما يحمي المستهلكين من سرقة البيانات والتلاعب بها.

وهذا ما نصت علية المادة (٥) من القانون، والتي جاء نصها: " يعاقب بالسجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أيًا من الجرائم المعلوماتية الآتية: الدخول غير المشروع لإلغاء بيانات خاصة، أو حذفها، أو تدميرها، أو تسريبها، أو إتلافها أو تغييرها، أو إعادة نشرها. إيقاف الشبكة المعلوماتية عن العمل، أو تعطيلها، أو تدمير، أو مسح البرامج، أو البيانات الموجودة، أو المستخدمة فيها، أو حذفها، أو تسريبها، أو إتلافها، أو تعديلها. إعاقة الوصول إلى الخدمة، أو تشويشها، أو تعطيلها، بأي وسيلة كانت"([2]).

[1]) المادة (٤) من نظام مكافحة جرائم المعلوماتية مرسوم ملكي رقم م/١٧.
[2]) المادة (٥) من نظام مكافحة جرائم المعلوماتية مرسوم ملكي رقم م/١٧.

٣- تشمل الحماية الجنائية أيضًا تجريم انتهاك الخصوصية، مثل التقاط ونشر الصور الشخصية أو المعلومات دون موافقة، وكذلك التنصت أو اعتراض الاتصالات الخاصة بدون إذن.

وهذا ما نصت علية المادة (٣) من القانون، والتي جاء نصها: "يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين ؛ كلُّ شخص يرتكب أيًا من الجرائم المعلوماتية الآتية: التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي - دون مسوغ نظامي صحيح - أو التقاطه أو اعتراضه. الدخول غير المشروع لتهديد شخص أو ابتزازه ؛ لحمله على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعًا . الدخول غير المشروع إلى موقع إلكتروني ، أو الدخول إلى موقع الكتروني لتغيير تصاميم هذا الموقع، أو إتلافه، أو تعديله، أو شغل عنوانه. المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرا، أو ما في حكمها . التشهير بالآخرين ، وإلحاق الضرر بهم ، عبر وسائل تقنيات المعلومات المختلفة"([1]).

[1]) المادة (٣) من نظام مكافحة جرائم المعلوماتية مرسوم ملكي رقم م/١٧.

٤- يحظر النظام نشر أو تداول المواد المحظورة عبر الإنترنت، بما في ذلك المحتوى الإباحي، المواد التي تحض على الكراهية أو العنف، والمعلومات التي تهدف إلى تقويض النظام العام.

وهذا ما نصت علية المادة (٦) من القانون، والتي جاء نصها: "يعاقب بالسجن مدة لا تزيد على خمس سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين كلُّ شخص يرتكب أيًّا من الجرائم المعلوماتية الآتية: إنتاج ما من شأنه المساس بالنظام العام ، او القيم الدينية، أو الآداب العامة ، أو حرمة الحياة الخاصة، أو إعداده ، أو إرساله، أو تخزينه عن طريق الشبكة المعلوماتية ، أو أحد أجهزة الحاسب الآلي . إنشاء موقع على الشبكة المعلوماتية ، أو أحد أجهزة الحاسب الآلي أو نشره ، للاتجار في الجنس البشري، أو تسهيل التعامل به. إنشاء المواد والبيانات المتعلقة بالشبكات الإباحية، أو أنشطة الميسر المخلة بالآداب العامة أو نشرها أو ترويجها. إنشاء موقع على الشبكة المعلوماتية ، أو أحد أجهزة الحاسب الآلي أو نشره ، للاتجار بالمخدرات، أو المؤثرات العقلية، أو ترويجها، أو طرق تعاطيها، أو تسهيل التعامل بها"([1]).

[1]) المادة (٦) من نظام مكافحة جرائم المعلوماتية مرسوم ملكي رقم م/١٧.

٥- يفرض النظام عقوبات صارمة تشمل الغرامات المالية الثقيلة و/أو السجن، بناءً على طبيعة الجريمة وخطورتها، لضمان تحقيق الردع وحماية المستهلكين بفعالية.

أوجه التشابه والاختلاف بين قوانين حماية المستهلك في مصر والامارات والسعودية:

قوانين حماية المستهلك في مصر، الإمارات، والسعودية تشترك في الهدف الأساسي المتمثل في حماية حقوق المستهلكين، وتعزيز الثقة والأمان في التجارة الإلكترونية والمعاملات التجارية بشكل عام. ومع ذلك، توجد بعض الاختلافات في التفاصيل القانونية وآليات التنفيذ بين هذه الدول. إليكم نظرة مقارنة تلقي الضوء على أوجه التشابه والاختلاف:

أوجه التشابه:

الإفصاح والشفافية: القوانين في الدول الثلاث تشدد على ضرورة الإفصاح الكامل عن معلومات المنتجات والخدمات، بما في ذلك الأسعار والمواصفات وأي معلومات ضرورية أخرى تؤثر على قرار الشراء.

حقوق الإلغاء والاسترجاع: توفر هذه الدول حقوقًا للمستهلكين في إلغاء المعاملات أو استرجاع المنتجات ضمن شروط وفترات زمنية محددة، مع التأكيد على سهولة هذه العمليات.

حماية البيانات الشخصية: قوانين الدول الثلاث تنص على حماية بيانات المستهلكين الشخصية وتضع قيودًا على جمع واستخدام هذه البيانات.

مكافحة الجرائم الإلكترونية: تعترف الدول الثلاث بأهمية مكافحة الجرائم الإلكترونية كجزء من حماية المستهلك، مع تحديد عقوبات للمخالفات مثل الاحتيال الإلكتروني وسرقة الهوية.

أوجه الاختلاف:

الإطار التنظيمي والرقابي: تختلف الآليات التنظيمية والهيئات الرقابية بين الدول فيما يخص تنفيذ قوانين حماية المستهلك. مثلاً، في مصر يوجد جهاز حماية المستهلك، بينما في الإمارات والسعودية توجد هيئات ولجان مختلفة تعمل على مراقبة السوق وحماية المستهلك.

التفاصيل القانونية: قد تتضمن القوانين في كل دولة تفاصيل قانونية محددة تعكس السياق الثقافي والاقتصادي المحلي، مثل تعريفات محددة للمستهلك والبائع، وتفاصيل معينة حول الإلغاء والاسترجاع.

العقوبات والتدابير الرادعة: تختلف درجة العقوبات والتدابير الرادعة المتخذة ضد المخالفات التجارية والجرائم الإلكترونية بين الدول، بناءً على شدة المخالفة والإطار القانوني العام.

تغطية الجرائم الإلكترونية: على الرغم من أن الدول الثلاث تتناول الجرائم الإلكترونية ضمن قوانين حماية المستهلك، إلا أن نطاق التغطية وتفاصيل الجرائم المحددة قد تختلف.

بشكل عام، تظهر المقارنة بين قوانين حماية المستهلك في مصر، الإمارات، والسعودية التزامًا مشتركًا بحماية المستهلكين وتعزيز بيئة تجارية إلكترونية آمنة، مع وجود بعض الفروقات التي تعكس خصوصية كل دولة.

الفرع الثاني

حماية المستهلك الالكتروني في التشريعات الأجنبية

حماية المستهلك الإلكتروني في التشريعات الأجنبية تعد مجالًا ديناميكيًا ومتطورًا بشكل مستمر، مع توجه الدول حول العالم لتعزيز القوانين والسياسات التي تحمي المستهلكين في البيئة الرقمية. تختلف النهج والتشريعات من دولة إلى أخرى، لكن هناك مجموعة من المبادئ الأساسية المشتركة التي توجه جهود حماية المستهلك الإلكتروني عالميًا.

أولًا– حماية المستهلك الالكتروني في تشريعات الاتحاد الأوروبي:

الحماية الجنائية للمستهلك الإلكتروني في قوانين الاتحاد الأوروبي تشمل مجموعة من الإجراءات والقوانين التي تهدف إلى حماية المستهلكين عند التسوق أو القيام بأي نوع من المعاملات الإلكترونية. هذه الحماية تشمل عدة جوانب مثل الخصوصية وأمن البيانات والحق في التراجع عن الشراء والحق في الحصول على معلومات واضحة ودقيقة حول المنتجات والخدمات.

- **النظام العام لحماية البيانات (GDPR)([1]):**

النظام العام لحماية البيانات (GDPR)، الذي أصبح ساري المفعول في مايو ٢٠١٨، يمثل أحد أهم التشريعات في مجال حماية البيانات والخصوصية على مستوى العالم، وهو يؤثر بشكل كبير على كيفية تعامل الشركات والمؤسسات مع بيانات الأفراد داخل الاتحاد الأوروبي وخارجه. يوفر GDPR حماية قوية للبيانات الشخصية ويشمل أحكامًا تؤثر على حماية المستهلك الإلكتروني بعدة طرق:

١- حق الوصول والشفافية: يمنح GDPR الأفراد الحق في الوصول إلى بياناتهم الشخصية التي تجمعها الشركات ويطلب من هذه الشركات أن تكون شفافة حول كيفية استخدام البيانات. هذا يعزز الثقة ويسمح للمستهلكين بمعرفة كيف ولماذا تُستخدم بياناتهم.

وهذا ما نصت عليه المادة (15) من اللائحة، والتي جاء نصها: "حق الوصول من قبل صاحب البيانات ١. يحق لصاحب البيانات الحصول على تأكيد من وحدة التحكم بشأن ما إذا كانت البيانات الشخصية المتعلقة به قيد المعالجة أم لا، وفي هذه الحالة، الوصول إلى البيانات الشخصية والمعلومات

[1]) On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

التالية: (أ) أغراض المعالجة؛ (ب) فئات البيانات الشخصية المعنية؛ (ج) المستلمون أو فئات المستلمين الذين تم الكشف عن بياناتهم الشخصية لهم أو سيتم الكشف عنها، ولا سيما المستلمون في بلدان ثالثة أو منظمات دولية؛ (د) حيثما أمكن، الفترة المتوقعة التي سيتم تخزين البيانات الشخصية لها، أو، إذا لم يكن ذلك ممكنًا، المعايير المستخدمة لتحديد تلك الفترة؛ (إنها) وجود الحق في طلب تصحيح أو محو البيانات الشخصية من المراقب أو تقييد معالجة البيانات الشخصية المتعلقة بصاحب البيانات أو الاعتراض على هذه المعالجة؛ (ذ) الحق في تقديم شكوى إلى السلطة الإشرافية؛ (ز) عندما لا يتم جمع البيانات الشخصية من صاحب البيانات، أي معلومات متاحة عن مصدرها؛ (ح) وجود عملية صنع القرار الآلي، بما في ذلك التنميط، المشار إليها في المادة ٢٢ (١) و (٤)، وعلى الأقل في تلك الحالات، معلومات ذات معنى حول المنطق المعني، فضلا عن الأهمية والعواقب المتوخاة من هذه المعالجة لموضوع البيانات. ٢. في حالة نقل البيانات الشخصية إلى دولة ثالثة أو إلى منظمة دولية، يحق لصاحب البيانات أن يتم إبلاغه بالضمانات المناسبة وفقًا للمادة ٤٦ المتعلقة بالنقل. ٣. يجب على المراقب تقديم نسخة من البيانات الشخصية قيد المعالجة. بالنسبة لأي نسخ إضافية

يطلبها صاحب البيانات، قد يفرض المراقب رسومًا معقولة على أساس التكاليف الإدارية. عندما يقدم صاحب البيانات الطلب بالوسائل الإلكترونية، وما لم يطلب صاحب البيانات خلاف ذلك، يجب تقديم المعلومات في نموذج إلكتروني شائع الاستخدام. ٤. لا يؤثر الحق في الحصول على النسخة المشار إليها في الفقرة (٣) سلباً على حقوق الآخرين وحرياتهم"([1]).

[1]) General Data Protection Regulation, 95/46/EC, Article 7. "Right of access by the data subject 1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information: (a) the purposes of the processing; (b) the categories of personal data concerned; (c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations; (d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period; (e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing; (f) the right to lodge a complaint with a supervisory authority; (g) where the personal data are not collected from the data subject, any available information as to their source; (h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. 2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer. 3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in

٢- حق النسيان (الحق في الحذف): يتيح GDPR للمستخدمين طلب حذف بياناتهم الشخصية في ظروف معينة، مثل عندما لا تكون هناك حاجة لاستخدام البيانات للأغراض التي جُمعت من أجلها.

وهذا ما نصت عليه المادة (17) من اللائحة، والتي جاء نصها: " الحق في المحو ("الحق في النسيان") ١. يحق لصاحب البيانات أن يحصل من المراقب على محو البيانات الشخصية المتعلقة به دون تأخير غير مبرر، ويكون المراقب ملزمًا بمحو البيانات الشخصية دون تأخير غير مبرر عندما ينطبق أحد الأسباب التالية: (أ) لم تعد البيانات الشخصية ضرورية فيما يتعلق بالأغراض التي تم جمعها أو معالجتها بطريقة أخرى من أجلها؛ (ب) يسحب صاحب البيانات الموافقة التي تستند إليها المعالجة وفقًا للنقطة (أ) من المادة ٦(١)، أو النقطة (أ) من المادة ٩(٢)، وحيث لا يوجد أي أساس قانوني آخر للمعالجة؛ (ج) يعترض صاحب البيانات على المعالجة وفقًا للمادة ٢١(١) ولا توجد أسباب مشروعة طاغية للمعالجة، أو يعترض صاحب البيانات على المعالجة وفقًا للمادة ٢١(٢)؛ (د) تمت معالجة البيانات الشخصية بشكل غير قانوني؛ (إنها) يجب محو البيانات الشخصية للامتثال

a commonly used electronic form. 4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others."

لالتزام قانوني في قانون الاتحاد أو الدول الأعضاء الذي يخضع له المراقب؛ (F) تم جمع البيانات الشخصية فيما يتعلق بعرض خدمات مجتمع المعلومات المشار إليها في المادة ٨ (١). ٢. عندما يقوم المراقب بنشر البيانات الشخصية ويكون ملزمًا بموجب الفقرة ١ بمحو البيانات الشخصية، يجب على المراقب، مع الأخذ في الاعتبار التكنولوجيا المتاحة وتكلفة التنفيذ، اتخاذ خطوات معقولة، بما في ذلك التدابير الفنية، لإبلاغ المراقبين التي تعالج البيانات الشخصية التي طلب صاحب البيانات مسحها من قبل هؤلاء المراقبين لأي روابط لتلك البيانات الشخصية أو نسخها أو تكرارها. ٣. لا تنطبق الفقرتان ١ و٢ إلى الحد الذي تكون فيه المعالجة ضرورية: (أ) ومن أجل ممارسة الحق في حرية التعبير والمعلومات؛ (ب) للامتثال لالتزام قانوني يتطلب المعالجة بموجب قانون الاتحاد أو قانون الدول الأعضاء الذي يخضع له المراقب المالي أو لأداء مهمة يتم تنفيذها للمصلحة العامة أو في ممارسة السلطة الرسمية المخولة للمراقب؛ (ج) لأسباب تتعلق بالمصلحة العامة في مجال الصحة العامة وفقًا للنقاط (ح) و(ط) من المادة ٩(٢) وكذلك المادة ٩(٣)؛ (د) لأغراض الأرشفة من أجل الصالح العام أو أغراض البحث العلمي أو التاريخي أو الأغراض الإحصائية وفقًا للمادة ٨٩ (١) بقدر ما

يكون الحق المشار إليه في الفقرة ١ من المحتمل أن يجعل تحقيق أهداف ذلك مستحيلًا أو يعوق بشكل خطير يعالج؛ أو (إنها) لإقامة الدعاوى القانونية أو ممارستها أو الدفاع عنها" (١).

[1]) General Data Protection Regulation, 95/46/EC, Article 17. Right to erasure ('right to be forgotten') 1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing; (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2); (d) the personal data have been unlawfully processed; (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1). 2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data. 3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary: (a) for exercising the right of freedom of expression and information; (b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3); (d) for archiving purposes in the public interest, scientific or historical research purposes or statistical

٣- الموافقة: يجب أن تكون الموافقة على معالجة البيانات الشخصية واضحة ومُستنيرة ومُعطاة بحرية. يجب أن توفر الشركات خيارًا سهلًا للأفراد لسحب موافقتهم في أي وقت.

وهذا ما نصت عليه المادة (7) من اللائحة، والتي جاء نصها: "شروط الموافقة ١. عندما تعتمد المعالجة على الموافقة، يجب أن يكون المراقب قادرًا على إثبات أن صاحب البيانات قد وافق على معالجة بياناته الشخصية. ٢. إذا تم إعطاء موافقة صاحب البيانات في سياق إعلان مكتوب يتعلق أيضًا بأمور أخرى، فيجب تقديم طلب الموافقة بطريقة يمكن تمييزها بوضوح عن الأمور الأخرى، في شكل واضح وسهل الوصول إليه، باستخدام لغة واضحة وبسيطة. أي جزء من هذا الإعلان يشكل انتهاكًا لهذه اللائحة لن يكون ملزمًا. ٣. يحق لصاحب البيانات سحب موافقته في أي وقت. ولا يؤثر سحب الموافقة على مشروعية المعالجة بناءً على الموافقة قبل سحبها. قبل إعطاء الموافقة، يجب إبلاغ صاحب البيانات بذلك. ويجب أن يكون الانسحاب سهلاً مثل إعطاء الموافقة. ٤. عند تقييم ما إذا كانت الموافقة تُمنح بحرية،

purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or (e) for the establishment, exercise or defence of legal claims.

يجب مراعاة أقصى قدر من الاعتبار، من بين أمور أخرى ، لما إذا كان تنفيذ العقد، بما في ذلك تقديم الخدمة، مشروطًا بالموافقة على معالجة البيانات الشخصية التي ليست ضرورية لـ أداء ذلك العقد"([1]).

٤- الأمان والانتهاكات: يفرض GDPR على الشركات تنفيذ تدابير أمان قوية لحماية البيانات الشخصية. كما يتطلب منهم إبلاغ السلطات والأفراد المتأثرين بأي انتهاكات للبيانات في غضون ٧٢ ساعة من اكتشافها.

وهذا ما نصت عليه المادة (٣٢) من اللائحة، والتي جاء نصها: "أمن المعالجة ١. مع الأخذ في الاعتبار أحدث التطورات وتكاليف التنفيذ وطبيعة المعالجة ونطاقها وسياقها وأغراضها، فضلاً عن مخاطر الاحتمالية المتفاوتة

[1]) General Data Protection Regulation, 95/46/EC, Article 7. "Conditions for consent 1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data. 2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding. 3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent. 4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract."

والشدة على حقوق وحريات الأشخاص الطبيعيين والمراقب والمعالج يجب تنفيذ التدابير الفنية والتنظيمية المناسبة لضمان مستوى أمني مناسب للمخاطر، بما في ذلك، من بين أمور أخرى، حسب الاقتضاء: (أ) الاسم المستعار وتشفير البيانات الشخصية؛ (ب) القدرة على ضمان السرية المستمرة والنزاهة والتوافر والمرونة لأنظمة وخدمات المعالجة؛ (ج) القدرة على استعادة توفر البيانات الشخصية والوصول إليها في الوقت المناسب في حالة وقوع حادث مادي أو فني؛ (د) عملية للاختبار المنتظم وتقييم فعالية التدابير الفنية والتنظيمية لضمان أمن المعالجة. ٢. عند تقييم المستوى المناسب لحساب الأمان، يجب أن يؤخذ على وجه الخصوص المخاطر التي تنتج عن المعالجة، ولا سيما المخاطر الناجمة عن التدمير العرضي أو غير القانوني أو الخسارة أو التغيير أو الكشف غير المصرح به أو الوصول إلى البيانات الشخصية المنقولة أو المخزنة أو غير ذلك. معالجتها. ٣. يجوز استخدام الالتزام بمدونة قواعد السلوك المعتمدة على النحو المشار إليه في المادة ٤٠ أو آلية إصدار الشهادات المعتمدة على النحو المشار إليه في المادة ٤٢ كعنصر يمكن من خلاله إثبات الامتثال للمتطلبات المنصوص عليها في الفقرة ١ من هذه المادة. ٤. يجب على وحدة التحكم والمعالج اتخاذ الخطوات

اللازمة للتأكد من أن أي شخص طبيعي يعمل تحت سلطة وحدة التحكم أو المعالج والذي لديه حق الوصول إلى البيانات الشخصية لا يقوم بمعالجتها إلا بناءً على تعليمات من وحدة التحكم، ما لم يُطلب منه القيام بذلك وذلك بموجب قانون الاتحاد أو الدول الأعضاء"([1]).

[1]) General Data Protection Regulation, 95/46/EC, Article 32. Security of processing 1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymisation and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. 2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. 3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article. 4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

والمادة (٣٣) من اللائحة، والتي جاء نصها: " إخطار السلطة الإشرافية بانتهاك البيانات الشخصية ١. في حالة حدوث خرق للبيانات الشخصية، يجب على المراقب دون تأخير لا مبرر له، وحيثما أمكن، في موعد لا يتجاوز ٧٢ ساعة بعد علمه به، إخطار السلطة الإشرافية المختصة بخرق البيانات الشخصية وفقًا للمادة ٥٥، ما لم يكن من غير المرجح أن يؤدي خرق البيانات الشخصية إلى خطر على حقوق وحريات الأشخاص الطبيعيين. إذا لم يتم الإخطار إلى السلطة الإشرافية في غضون ٧٢ ساعة، فيجب أن يكون مصحوبًا بأسباب التأخير"([1]).

٥- مسؤولية البيانات والمعالجة: يتطلب GDPR من الشركات والمنظمات التي تجمع أو تعالج بيانات شخصية تعيين مسؤول حماية البيانات (DPO) وتطبيق مبدأ "الخصوصية من التصميم والخصوصية الافتراضية"، مما يعني أن الخصوصية يجب أن تكون مدمجة في المنتجات والخدمات منذ البداية.

[1]) General Data Protection Regulation, 95/46/EC, Article 33. Notification of a personal data breach to the supervisory authority 1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

وهذا ما نصت عليه المادة (١٨) من اللائحة، والتي جاء نصها: "الحق في تقييد المعالجة ١. يحق لصاحب البيانات الحصول على تقييد المعالجة من وحدة التحكم في حالة تطبيق أحد الإجراءات التالية: (أ) يتم الاعتراض على دقة البيانات الشخصية من قبل صاحب البيانات، لفترة تمكن المراقب من التحقق من دقة البيانات الشخصية؛ (ب) المعالجة غير قانونية ويعارض صاحب البيانات محو البيانات الشخصية ويطلب تقييد استخدامها بدلاً من ذلك؛ (ج) لم تعد وحدة التحكم بحاجة إلى البيانات الشخصية لأغراض المعالجة، ولكنها مطلوبة من قبل صاحب البيانات لإنشاء المطالبات القانونية أو ممارستها أو الدفاع عنها؛ (د) اعترض صاحب البيانات على المعالجة وفقًا للمادة ٢١(١) في انتظار التحقق مما إذا كانت الأسباب المشروعة للمراقب تتجاوز تلك الخاصة بصاحب البيانات. ٢. في حالة تقييد المعالجة بموجب الفقرة ١، لا تتم معالجة هذه البيانات الشخصية، باستثناء التخزين، إلا بموافقة صاحب البيانات أو لإنشاء مطالبات قانونية أو ممارستها أو الدفاع عنها أو لحماية حقوق شخص آخر. شخص طبيعي أو اعتباري أو لأسباب تتعلق بالمصلحة العامة المهمة للاتحاد أو لدولة عضو. ٣. يجب

على المراقب إبلاغ صاحب البيانات الذي حصل على تقييد المعالجة بموجب الفقرة ١ قبل رفع قيود المعالجة"([1]).

- **التوجيه الأوروبي لحقوق المستهلك ٨٣/٢٠١١ / EU([2]):**

التوجيه الأوروبي لحقوق المستهلك EU/٨٣/٢٠١١، الذي اعتُمد في أكتوبر ٢٠١١، يمثل خطوة هامة نحو تحسين حماية المستهلكين في الاتحاد الأوروبي، خاصة في سياق المعاملات الإلكترونية والتسوق عبر الإنترنت. هذا التوجيه يهدف إلى توحيد

[1]) General Data Protection Regulation, 95/46/EC, Article 18. Right to restriction of processing 1. The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies: (a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data; (b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; (c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; (d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject. 2. Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State. 3. A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.

[2]) Directive 2011/83/EU on consumer rights. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011L0083

القواعد الأساسية لحماية المستهلك في جميع دول الاتحاد الأوروبي، مما يوفر مستوى عالٍ من الحماية ويسهل على الشركات العمل عبر الحدود.

١- الحق في الإعلام: يلزم التوجيه البائعين بتقديم معلومات واضحة ومفهومة للمستهلكين قبل أن يتم إبرام العقود. هذا يشمل معلومات حول السعر الكامل، خصائص المنتج أو الخدمة، هوية وعنوان البائع، والحق في التراجع عن الشراء.

وهذا ما نصت عليه المادة (٥) من التوجيه، والتي جاء نصها: "متطلبات المعلومات للعقود بخلاف العقود البعيدة أو خارج أماكن العمل ١. قبل أن يلتزم المستهلك بعقد غير عقد المسافة أو عقد خارج المبنى، أو أي عرض مماثل، يجب على التاجر تزويد المستهلك بالمعلومات التالية بطريقة واضحة ومفهومة، إذا لم تكن تلك المعلومات ظاهرة بالفعل من السياق: (أ) الخصائص الرئيسية للسلع أو الخدمات، إلى الحد الذي يتناسب مع الوسيط والسلع أو الخدمات؛ (ب) هوية التاجر مثل اسمه التجاري وعنوانه الجغرافي ورقم هاتفه. (ج) السعر الإجمالي للسلع أو الخدمات شاملاً الضرائب، أو عندما تكون طبيعة السلع أو الخدمات بحيث لا يمكن حساب السعر مقدمًا بشكل معقول، والطريقة التي سيتم بها حساب السعر، وكذلك، حيثما ينطبق

ذلك جميع رسوم الشحن أو التسليم أو الرسوم البريدية الإضافية، أو، عندما لا يمكن حساب هذه الرسوم بشكل معقول مقدمًا، حقيقة أن هذه الرسوم الإضافية قد تكون مستحقة الدفع؛ (د) حيثما ينطبق ذلك، ترتيبات الدفع والتسليم والأداء والوقت الذي يتعهد فيه التاجر بتسليم البضائع أو أداء الخدمة وسياسة التعامل مع شكاوى التاجر؛ (إنها) بالإضافة إلى التذكير بوجود ضمان قانوني لمطابقة البضائع ووجود وشروط خدمات ما بعد البيع والضمانات التجارية حيثما ينطبق ذلك؛ (F) مدة العقد، حيثما ينطبق ذلك، أو، إذا كان العقد غير محدد المدة أو سيتم تمديده تلقائيًا، شروط إنهاء العقد؛ (ز) حيثما ينطبق ذلك، وظيفة المحتوى الرقمي، بما في ذلك تدابير الحماية التقنية المعمول بها؛ (ح) حيثما ينطبق ذلك، أي قابلية للتشغيل البيني للمحتوى الرقمي مع الأجهزة والبرامج التي يكون المتداول على علم بها أو من المتوقع بشكل معقول أن يكون على علم بها. ٢. تنطبق الفقرة ١ أيضًا على عقود توريد المياه أو الغاز أو الكهرباء، حيث لا يتم طرحها للبيع بكميات محدودة أو كمية محددة، أو تدفئة المناطق أو المحتوى الرقمي الذي لا يتم توفيره على وسيط ملموس. . ٣. لا يُطلب من الدول الأعضاء تطبيق الفقرة ١ على العقود التي تتضمن معاملات يومية والتي يتم تنفيذها فورًا وقت

إبرامها. ٤. يجوز للدول الأعضاء أن تعتمد أو تحافظ على متطلبات معلومات إضافية قبل التعاقد فيما يتعلق بالعقود التي تنطبق عليها هذه المادة"(١).

[1]) Directive 2011/83/EU on consumer rights, Article 5, Information requirements for contracts other than distance or off-premises contracts 1. Before the consumer is bound by a contract other than a distance or an off-premises contract, or any corresponding offer, the trader shall provide the consumer with the following information in a clear and comprehensible manner, if that information is not already apparent from the context: (a) the main characteristics of the goods or services, to the extent appropriate to the medium and to the goods or services; (b) the identity of the trader, such as his trading name, the geographical address at which he is established and his telephone number; (c) the total price of the goods or services inclusive of taxes, or where the nature of the goods or services is such that the price cannot reasonably be calculated in advance, the manner in which the price is to be calculated, as well as, where applicable, all additional freight, delivery or postal charges or, where those charges cannot reasonably be calculated in advance, the fact that such additional charges may be payable; (d) where applicable, the arrangements for payment, delivery, performance, the time by which the trader undertakes to deliver the goods or to perform the service, and the trader's complaint handling policy; (e) in addition to a reminder of the existence of a legal guarantee of conformity for goods, the existence and the conditions of after-sales services and commercial guarantees, where applicable; (f) the duration of the contract, where applicable, or, if the contract is of indeterminate duration or is to be extended automatically, the conditions for terminating the contract; (g) where applicable, the functionality, including applicable technical protection measures, of digital content; (h) where applicable, any relevant interoperability of digital content with hardware and software that the trader is aware of or can reasonably be expected to have been aware of. 2. Paragraph 1 shall also apply to contracts for the supply of water, gas or electricity, where they are not put up for sale in a limited volume or set quantity, of district heating or of digital content which is not supplied on a tangible medium. 3. Member States shall not be required to apply paragraph 1 to contracts which involve day-to-day transactions and which

٢- الحق في التراجع: يوسع التوجيه فترة الحق في التراجع من الشراء عبر الإنترنت أو خارج المتجر إلى ١٤ يومًا. خلال هذه الفترة، يمكن للمستهلكين إعادة المنتج دون تقديم أي سبب واسترداد كامل المبلغ المدفوع، بما في ذلك تكاليف الشحن الأصلية.

وهذا ما نصت عليه المادة (٩) من التوجيه، والتي جاء نصها: " حق الانسحاب ١. فيما عدا حالة تطبيق الاستثناءات المنصوص عليها في المادة (١٦)، يكون للمستهلك فترة ١٤ يومًا للانسحاب من العقد عن بعد أو خارج مقر العمل، دون إبداء أي سبب، ودون تحمل أي تكاليف غير تلك المنصوص عليها في المادة. ١٣(٢) والمادة ١٤. ٢. مع عدم الإخلال بالمادة (١٠)، تنتهي فترة الانسحاب المشار إليها في الفقرة (١) من هذه المادة بعد ١٤ يومًا من: (أ) في حالة عقود الخدمة، يوم إبرام العقد؛ (ب) في حالة عقود البيع، اليوم الذي يحصل فيه المستهلك أو طرف ثالث غير الناقل والمشار إليه من قبل المستهلك على الحيازة المادية للبضائع أو: (أنا) في حالة السلع المتعددة التي يطلبها المستهلك في طلب واحد ويتم تسليمها بشكل منفصل، اليوم الذي يحصل فيه المستهلك أو طرف ثالث غير الناقل والذي

are performed immediately at the time of their conclusion. 4. Member States may adopt or maintain additional pre-contractual information requirements for contracts to which this Article applies.

أشار إليه المستهلك على الحيازة المادية للسلعة الأخيرة؛ (ثانيا) في حالة تسليم سلعة تتكون من دفعات أو قطع متعددة، اليوم الذي يحصل فيه المستهلك أو طرف ثالث غير الناقل والمشار إليه من قبل المستهلك على الحيازة المادية للدفعة أو القطعة الأخيرة؛ (ثالثا) في حالة عقود التسليم المنتظم للبضائع خلال فترة زمنية محددة، اليوم الذي يحصل فيه المستهلك أو طرف ثالث غير الناقل ويحدده المستهلك على الحيازة المادية للسلعة الأولى؛ (ج) في حالة عقود توريد المياه أو الغاز أو الكهرباء، حيث لا يتم طرحها للبيع بكميات محدودة أو كمية محددة، أو التدفئة المركزية أو المحتوى الرقمي الذي لا يتم توفيره على وسيلة ملموسة، في يوم إبرام العقد. ٣. لا يجوز للدول الأعضاء منع الأطراف المتعاقدة من أداء التزاماتها التعاقدية خلال فترة الانسحاب. ومع ذلك، في حالة العقود خارج مقر العمل، يجوز للدول الأعضاء الاحتفاظ بالتشريعات الوطنية الحالية التي تحظر على التاجر تحصيل المدفوعات من المستهلك خلال الفترة المحددة بعد إبرام العقد"([1]).

[1]) Directive 2011/83/EU on consumer rights, Article 9, Right of withdrawal 1. Save where the exceptions provided for in Article 16 apply, the consumer shall have a period of 14 days to withdraw from a distance or off-premises contract, without giving any reason, and without incurring any costs other than those provided for in Article 13(2) and Article 14. 2. Without prejudice to Article 10, the withdrawal period referred to in paragraph 1 of this Article shall expire after 14 days from: (a) in the case of

٣- القواعد بخصوص التسليم ونقل المخاطر: يحدد التوجيه أن السلع يجب أن تُسلم إلى المستهلكين في غضون ٣٠ يومًا من تاريخ العقد، ما لم يتفق الطرفان على خلاف ذلك. كما ينص على أن المخاطر المتعلقة بالسلع (مثل الفقدان أو التلف) تنتقل إلى المستهلك فقط عندما يتسلم السلعة فعليًا.

وهذا ما نصت عليه المادة (١٨) من التوجيه، والتي جاء نصها: "توصيل ١. ما لم يتفق الطرفان على خلاف ذلك في وقت التسليم، يجب على التاجر تسليم البضائع عن طريق نقل الحيازة المادية أو السيطرة على البضائع إلى

service contracts, the day of the conclusion of the contract; (b) in the case of sales contracts, the day on which the consumer or a third party other than the carrier and indicated by the consumer acquires physical possession of the goods or: (i) in the case of multiple goods ordered by the consumer in one order and delivered separately, the day on which the consumer or a third party other than the carrier and indicated by the consumer acquires physical possession of the last good; (ii) in the case of delivery of a good consisting of multiple lots or pieces, the day on which the consumer or a third party other than the carrier and indicated by the consumer acquires physical possession of the last lot or piece; (iii) in the case of contracts for regular delivery of goods during defined period of time, the day on which the consumer or a third party other than the carrier and indicated by the consumer acquires physical possession of the first good; (c) in the case of contracts for the supply of water, gas or electricity, where they are not put up for sale in a limited volume or set quantity, of district heating or of digital content which is not supplied on a tangible medium, the day of the conclusion of the contract. 3. The Member States shall not prohibit the contracting parties from performing their contractual obligations during the withdrawal period. Nevertheless, in the case of off-premises contracts, Member States may maintain existing national legislation prohibiting the trader from collecting the payment from the consumer during the given period after the conclusion of the contract.

المستهلك دون تأخير لا مبرر له، ولكن في موعد لا يتجاوز ٣٠ يومًا من إبرام العقد. ٢. في حالة فشل التاجر في الوفاء بالتزامه بتسليم البضائع في الوقت المتفق عليه مع المستهلك أو خلال المهلة المنصوص عليها في الفقرة (١)، يجب على المستهلك أن يطالبه بإجراء التسليم خلال فترة زمنية إضافية. المناسبة للظروف. وإذا فشل التاجر في تسليم البضائع خلال تلك الفترة الإضافية، يحق للمستهلك إنهاء العقد. لا تنطبق الفقرة الفرعية الأولى على عقود البيع التي يرفض فيها التاجر تسليم البضائع أو عندما يكون التسليم خلال فترة التسليم المتفق عليها ضروريًا مع مراعاة جميع الظروف التي تصاحب إبرام العقد أو عندما يقوم المستهلك بإبلاغ التاجر مسبقًا إلى إبرام العقد، فإن التسليم في موعد محدد أو في تاريخ محدد أمر ضروري. وفي تلك الحالات، إذا فشل التاجر في تسليم البضائع في الوقت المتفق عليه مع المستهلك أو خلال المهلة الزمنية المنصوص عليها في الفقرة ١، يحق للمستهلك إنهاء العقد على الفور. ٣. عند إنهاء العقد، يجب على التاجر، دون تأخير لا مبرر له، تسديد جميع المبالغ المدفوعة بموجب العقد. ٤.

بالإضافة إلى إنهاء العقد وفقًا للفقرة ٢، يجوز للمستهلك اللجوء إلى سبل الانتصاف الأخرى المنصوص عليها في القانون الوطني"([1]).

٤- المبيعات خارج المتاجر والبيع عن بعد: يوفر التوجيه حماية خاصة للمعاملات التي تتم خارج المتاجر (مثل المبيعات التي تتم في المنزل أو في مكان العمل) وللمبيعات التي تتم عن بعد (عبر الإنترنت أو عبر الهاتف).

وهذا ما نصت عليه المادة (٧) من التوجيه، والتي جاء نصها: "المتطلبات الرسمية للعقود خارج المبنى ١. فيما يتعلق بالعقود خارج مقر العمل، يجب

[1]) Directive 2011/83/EU on consumer rights, Article 18, Delivery 1. Unless the parties have agreed otherwise on the time of delivery, the trader shall deliver the goods by transferring the physical possession or control of the goods to the consumer without undue delay, but not later than 30 days from the conclusion of the contract. 2. Where the trader has failed to fulfil his obligation to deliver the goods at the time agreed upon with the consumer or within the time limit set out in paragraph 1, the consumer shall call upon him to make the delivery within an additional period of time appropriate to the circumstances. If the trader fails to deliver the goods within that additional period of time, the consumer shall be entitled to terminate the contract. The first subparagraph shall not be applicable to sales contracts where the trader has refused to deliver the goods or where delivery within the agreed delivery period is essential taking into account all the circumstances attending the conclusion of the contract or where the consumer informs the trader, prior to the conclusion of the contract, that delivery by or on a specified date is essential. In those cases, if the trader fails to deliver the goods at the time agreed upon with the consumer or within the time limit set out in paragraph 1, the consumer shall be entitled to terminate the contract immediately. 3. Upon termination of the contract, the trader shall, without undue delay, reimburse all sums paid under the contract. 4. In addition to the termination of the contract in accordance with paragraph 2, the consumer may have recourse to other remedies provided for by national law.

على التاجر تقديم المعلومات المنصوص عليها في المادة ٦ (١) إلى المستهلك على الورق أو، إذا وافق المستهلك، على وسيلة دائمة أخرى. ويجب أن تكون هذه المعلومات مقروءة وبلغة واضحة وواضحة. ٢. يجب على التاجر أن يزود المستهلك بنسخة من العقد الموقع أو تأكيد العقد على الورق أو، إذا وافق المستهلك، على وسيلة دائمة أخرى، بما في ذلك، حيثما ينطبق ذلك، تأكيد موافقة المستهلك الصريحة المسبقة والإقرار وفقاً للنقطة (م) من المادة ١٦. ٣. عندما يرغب المستهلك في بدء أداء الخدمات أو توفير المياه أو الغاز أو الكهرباء، حيث لا يتم طرحها للبيع بكمية محدودة أو كمية محددة، أو بدء التدفئة المركزية خلال فترة الانسحاب المنصوص عليها في المادة ٩ (٢)، يجب على التاجر أن يطلب من المستهلك تقديم مثل هذا الطلب الصريح على وسيلة دائمة. ٤. فيما يتعلق بالعقود خارج مقر العمل حيث يطلب المستهلك صراحةً خدمات التاجر لغرض إجراء الإصلاحات أو الصيانة التي يقوم التاجر والمستهلك بتنفيذ التزاماتهما التعاقدية على الفور وحيث يتم الدفع من قبل المستهلك لا يتجاوز ٢٠٠ يورو: (أ) يجب على التاجر تزويد المستهلك بالمعلومات المشار إليها في النقطتين (ب) و (ج) من المادة ٦ (١) ومعلومات عن السعر أو الطريقة التي سيتم بها حساب

السعر مع تقدير السعر الإجمالي. على الورق أو، إذا وافق المستهلك، على وسيلة دائمة أخرى. يجب على التاجر تقديم المعلومات المشار إليها في النقاط (أ) و(ح) و(ك) من المادة ٦(١)، ولكن يجوز له اختيار عدم تقديمها على الورق أو أي وسيلة دائمة أخرى إذا وافق المستهلك صراحةً؛ (ب) يجب أن يحتوي تأكيد العقد المنصوص عليه وفقًا للفقرة ٢ من هذه المادة على المعلومات المنصوص عليها في المادة ٦(١). ويجوز للدول الأعضاء أن تقرر عدم تطبيق هذه الفقرة. ٥. لا يجوز للدول الأعضاء فرض أي متطلبات رسمية إضافية للمعلومات قبل التعاقدية للوفاء بالتزامات المعلومات المنصوص عليها في هذا التوجيه"([1]).

[1]) Directive 2011/83/EU on consumer rights, Article 7, Formal requirements for off-premises contracts 1. With respect to off-premises contracts, the trader shall give the information provided for in Article 6(1) to the consumer on paper or, if the consumer agrees, on another durable medium. That information shall be legible and in plain, intelligible language. 2. The trader shall provide the consumer with a copy of the signed contract or the confirmation of the contract on paper or, if the consumer agrees, on another durable medium, including, where applicable, the confirmation of the consumer's prior express consent and acknowledgement in accordance with point (m) of Article 16. 3. Where a consumer wants the performance of services or the supply of water, gas or electricity, where they are not put up for sale in a limited volume or set quantity, or of district heating to begin during the withdrawal period provided for in Article 9(2), the trader shall require that the consumer makes such an express request on a durable medium. 4. With respect to off-premises contracts where the consumer has explicitly requested the services of the trader for the purpose of carrying out repairs or maintenance for

٥- الشفافية في الدفعات: يطلب من البائعين ضمان أن يكون المستهلكون على وعي بأي تكاليف إضافية أو رسوم قبل تأكيد الطلب. يُحظر تحديد خيارات تؤدي إلى دفع إضافي بشكل افتراضي (مثل تحديد صناديق الاختيار مسبقًا). وهذا ما نصت عليه المادة (٢٢) من التوجيه، والتي جاء نصها: "مدفوعات إضافية قبل أن يلتزم المستهلك بالعقد أو العرض، يجب على التاجر الحصول على موافقة صريحة من المستهلك على أي دفعة إضافية بالإضافة إلى المكافأة المتفق عليها مقابل الالتزام التعاقدي الرئيسي للتاجر. إذا لم يحصل التاجر على موافقة صريحة من المستهلك ولكنه استنتجها باستخدام

which the trader and the consumer immediately perform their contractual obligations and where the payment to be made by the consumer does not exceed EUR 200: (a) the trader shall provide the consumer with the information referred to in points (b) and (c) of Article 6(1) and information about the price or the manner in which the price is to be calculated together with an estimate of the total price, on paper or, if the consumer agrees, on another durable medium. The trader shall provide the information referred to in points (a), (h) and (k) of Article 6(1), but may choose not to provide it on paper or another durable medium if the consumer expressly agrees; (b) the confirmation of the contract provided in accordance with paragraph 2 of this Article shall contain the information provided for in Article 6(1). Member States may decide not to apply this paragraph. 5. Member States shall not impose any further formal pre-contractual information requirements for the fulfilment of the information obligations laid down in this Directive.

الخيارات الافتراضية التي يتعين على المستهلك رفضها لتجنب الدفع الإضافي، يحق للمستهلك استرداد هذه الدفعة"([1]).

ثانيًا- حماية المستهلك الالكتروني في التشريعات الأمريكية:

في الولايات المتحدة، تُعتبر حماية المستهلك الإلكتروني جزءًا هامًا من التشريعات الفيدرالية والولائية، وهناك عدة قوانين تعمل على حماية الحقوق والخصوصية للمستهلكين في الفضاء الإلكتروني. تشمل هذه القوانين ما يلي:

- **قانون المستهلكين - INFORM Consumers Act ([2]):**

يتعامل مع جمع المعلومات، والتحقق منها، والكشف عنها من قبل الأسواق الإلكترونية بهدف إطلاع المستهلكين. هذا القانون يلزم الأسواق الإلكترونية بأن تطلب من البائعين ذوي الحجم الكبير من الطرف الثالث على منصاتها تقديم معلومات محددة في غضون ١٠ أيام من تأهلهم كبائعين ذوي حجم كبير. المعلومات المطلوبة

[1]) Directive 2011/83/EU on consumer rights, Article 22, Additional payments Before the consumer is bound by the contract or offer, the trader shall seek the express consent of the consumer to any extra payment in addition to the remuneration agreed upon for the trader's main contractual obligation. If the trader has not obtained the consumer's express consent but has inferred it by using default options which the consumer is required to reject in order to avoid the additional payment, the consumer shall be entitled to reimbursement of this payment.

[2]) INFORM Consumers Act, 15 U.S.C. § 45f. online: https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section45f&num=0&edition=prelim

تشمل رقم حساب مصرفي أو اسم المستفيد من الدفعات الصادرة من السوق الإلكتروني، بالإضافة إلى معلومات الاتصال، رقم الضريبة، وعنوان بريد إلكتروني ورقم هاتف صالحين([1]).

يحتوي القانون أيضًا على أحكام تتعلق بالتحقق من صحة المعلومات المقدمة من البائعين والكشف عن هذه المعلومات للمستهلكين بطريقة واضحة وملحوظة. هذا يتضمن الكشف عن هوية البائع الثالث ذو الحجم الكبير، عنوانه الفعلي، ومعلومات الاتصال على صفحة السلعة أو في رسالة تأكيد الطلب أو في تاريخ معاملات حساب المستهلك. هذه الإجراءات تهدف إلى زيادة الشفافية وتمكين المستهلكين من الحصول على معلومات كافية تساعدهم على اتخاذ قرارات مستنيرة عند التسوق عبر الإنترنت([2]).

[1]) INFORM Consumers Act, 15 U.S.C. § 45f. Collection, verification, and disclosure of information by online marketplaces to inform consumers (a) Collection and verification of information (1) Collection (A) In general An online marketplace shall require any high-volume third party seller on such online marketplace's platform to provide, not later than 10 days after qualifying as a high-volume third party seller on the platform, the following information to the online marketplace:

[2]) INFORM Consumers Act, 15 U.S.C. § 45f. (ii) Contact information Contact information for such seller as follows: (I) With respect to a high-volume third party seller that is an individual, the individual's name. (II) With respect to a high-volume third party seller that is not an individual, one of the following forms of contact information: (aa) A copy of a valid government-issued identification for an individual acting on behalf of such

٢- الحماية الجنائية للمستهلك الإلكتروني

علاوة على ذلك، يتضمن القانون إجراءات للتعامل مع البائعين الذين لا يلتزمون بتقديم أو تحديث المعلومات المطلوبة، بما في ذلك تعليق نشاط المبيعات المستقبلية لهؤلاء البائعين حتى يتم تقديم هذه المعلومات أو التحقق منها. كما يعطي القانون للجنة التجارة الفيدرالية (FTC) الصلاحية لفرض هذه الأحكام ويتيح للمدعين العامين في الولايات تقديم دعاوى قضائية ضد الأسواق الإلكترونية التي تنتهك هذه الأحكام. هذا القانون يمثل خطوة هامة نحو تعزيز حماية المستهلكين الإلكترونيين من خلال ضمان بيئة تجارة إلكترونية أكثر شفافية وأمانًا([1]).

seller that includes the individual's name. (bb) A copy of a valid government-issued record or tax document that includes the business name and physical address of such seller.

[1]) INFORM Consumers Act, 15 U.S.C. § 45f. (C) Suspension In the event that a high-volume third party seller does not provide the information or certification required under this paragraph, the online marketplace shall, after providing the seller with written or electronic notice and an opportunity to provide such information or certification not later than 10 days after the issuance of such notice, suspend any future sales activity of such seller until such seller provides such information or certification.

- قانون حماية مراجعات المستهلكين – Consumer Review Fairness Act ([1]):

قانون حماية مراجعات المستهلكين، يُشكل حجر الزاوية في ضمان بيئة تجارية إلكترونية تعتمد على الشفافية والصدق. هذا القانون يُقر بأهمية المراجعات والتقييمات التي يُشاركها المستهلكون عبر الإنترنت، ويعترف بدورها الحاسم في تشكيل قرارات الشراء لدى المستهلكين الآخرين. من خلال تحديد وإبطال أي بنود تعاقدية تهدف إلى كبح جماح هذا الحق الأساسي، يضع القانون الأساس لممارسة حرية التعبير في الفضاء الرقمي بدون خوف من العقاب أو العقوبات المالية.

بموجب هذا القانون، تُعتبر الأحكام التي تحظر أو تقيد قدرة المستهلك على نشر مراجعات حول السلع أو الخدمات، أو تلك التي تنقل حقوق الملكية الفكرية لمحتوى المراجعة إلى طرف ثالث، باطلة وغير قابلة للتطبيق. هذا يُمثل انتصارًا كبيرًا لحقوق المستهلك ويُعزز من المنافسة العادلة بين الشركات، حيث تُصبح الشفافية والنزاهة جزءًا لا يتجزأ من العلاقة بين المستهلكين والمؤسسات التجارية([2]).

[1]) Consumer Review Fairness Act, 15 U.S.C. § 45b, online: https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section45b&num=0&edition=prelim

[2]) §45b. Consumer review protection, (3) Form contract (A) In general Except as provided in subparagraph (B), the term "form contract" means a contract with standardized terms- (i) used by a person in the course of

يُكمل القانون جهوده في حماية المستهلكين عبر تمكين لجنة التجارة الفيدرالية (FTC) والمدعين العامين للولايات من إنفاذ هذه الأحكام بشكل فعّال. يُعطي هذا النهج المزدوج الأولوية للحفاظ على حقوق المستهلكين الإلكترونيين ويُشجع على إنشاء بيئة تجارة إلكترونية أكثر أمانًا وثقة، مما يدعم في النهاية نمو السوق الرقمي بطريقة مستدامة ومتوازنة.

ثالثًا- حماية المستهلك الالكتروني في التشريعات الأسترالية:

في أستراليا، تعتبر حماية المستهلك الإلكتروني جزءًا لا يتجزأ من الإطار القانوني الذي يحكم التجارة والمعاملات الإلكترونية. الحماية الجنائية للمستهلك في هذا السياق تشمل تشريعات تهدف إلى ضمان التعامل العادل والأمان للمستهلكين أثناء التسوق عبر الإنترنت، وحماية بياناتهم الشخصية، والدفاع عنهم ضد الممارسات التجارية غير العادلة والاحتيالية. ونستعرض نظرة عامة على بعض الأسس الرئيسية لهذه الحماية في التشريع الأسترالي:

selling or leasing the person's goods or services; and (ii) imposed on an individual without a meaningful opportunity for such individual to negotiate the standardized terms.

- قانون المستهلك الأسترالي (Australian Consumer Law – ACL)([1]):

في أستراليا، يُعد قانون حماية المستهلك إحدى الركائز الأساسية للنظام القانوني التي تهدف إلى تعزيز العدالة والإنصاف في المعاملات التجارية، موفرًا ضمانات قوية تحمي المستهلكين من الممارسات غير العادلة والمضللة. يُطبق القانون مجموعة من المعايير الصارمة التي تضمن جودة وسلامة السلع والخدمات، مؤكدًا على أن كل منتج يجب أن يكون صالحًا للغرض الذي أُنتج من أجله وأن يتوافق مع الوصفات والعينات المقدمة للمستهلكين، سواء أكان ذلك من خلال التغليف، الإعلان، أو خلال عملية البيع نفسها.

من جانب آخر، يُعالج القانون مسألة الإعلانات الخادعة أو المضللة بكل صرامة، محظورًا الإعلان بطرق تُضلل المستهلكين بشأن الأسعار، الجودة، الأصل، أو حتى الفوائد المرتقبة من استخدام السلعة أو الخدمة. كما يتناول القانون الممارسات التجارية غير العادلة بشكل شامل، منعًا لأي ضغوط بيعيه مفرطة أو استغلال لنقاط ضعف المستهلكين، وذلك لضمان تجربة تسوق أكثر أمانًا وثقة للمستهلك الأسترالي.

[1]) Competition and Consumer Act 2010, online: https://www.legislation.gov.au/C2004A00109/latest/text

أخيرًا، يُسلط القانون الضوء على حقوق المستهلكين في الإصلاح، الاستبدال، أو الاسترجاع واسترداد الأموال للمنتجات التي لا تلبي الضمانات القانونية المطلوبة، مؤكدًا على أهمية وجود آليات فعالة لتقديم الشكاوى والحصول على التعويضات المناسبة في حالة انتهاك حقوقهم. هذه الأحكام تجعل من قانون حماية المستهلك الأسترالي نموذجًا يحتذى به في توفير بيئة تجارية تراعي حقوق المستهلكين بشكل شامل ومتكامل.

- **قانون الخصوصية الاسترالي (Privacy Act 1988)([1]):**

قانون الخصوصية الأسترالي لعام ١٩٨٨ يُمثل حجر الأساس في نظام حماية البيانات الشخصية، حيث يُقدم إطارًا تنظيميًا محكمًا يرمي إلى حماية خصوصية الأفراد من خلال ضوابط صارمة على جمع، استخدام، الإفصاح، والاحتفاظ بالمعلومات الشخصية من قبل الكيانات التي تخضع لهذا القانون. يُلزم القانون الجهات الفاعلة بجمع المعلومات الشخصية بشكل قانوني وعادل، مع التأكيد على ضرورة أن يقتصر الجمع على المعلومات الضرورية فقط لتحقيق الأغراض المحددة، مما يحمي المعلومات الشخصية للمستهلكين من الجمع العشوائي والغير ضروري، خاصةً في البيئة الإلكترونية.

[1]) Privacy Act 1988, online: https://www.legislation.gov.au/C2004A03712/latest/versions

فيما يتعلق باستخدام والإفصاح عن المعلومات الشخصية، يحدد القانون بوضوح الشروط التي يجب توافرها لضمان أن يكون استخدام أو الإفصاح عن المعلومات متوافقًا مع الأغراض الأصلية التي جُمعت من أجلها. هذا يشمل الحصول على موافقة صريحة من الأفراد قبل استخدام بياناتهم لأغراض أخرى، موفرًا بذلك حماية للمستهلكين من الاستخدام غير المتوقع أو غير المرغوب فيه لبياناتهم. كما يُطالب القانون الكيانات بتنفيذ تدابير أمنية معقولة لحماية البيانات الشخصية من الوصول غير المصرح به أو الكشف، مما يُلزم الشركات العاملة عبر الإنترنت بضمان سلامة وأمان المعلومات التي يجمعونها. بالإضافة إلى ذلك، يُكفل قانون الخصوصية الأسترالي حقوقًا مهمة للأفراد تتعلق بالوصول إلى المعلومات الشخصية التي تُحتفظ بها عنهم وتصحيح أي بيانات غير دقيقة. هذا يعطي المستهلكين القدرة على المطالبة بالاطلاع على البيانات الشخصية التي تجمعها الشركات وتصحيحها حسب الحاجة، مما يُعزز الشفافية ويمنح المستهلكين المزيد من السيطرة على معلوماتهم الشخصية في العصر الرقمي.

أوجه التشابه والاختلاف بين قوانين حماية المستهلك في الاتحاد الأوروبي وامريكا وأستراليا:

قوانين حماية المستهلك في الاتحاد الأوروبي، والولايات المتحدة الأمريكية، وأستراليا تشترك في الهدف الأساسي المتمثل في حماية حقوق المستهلكين، لكنها تختلف في نهجها وفي التفاصيل الدقيقة للتنفيذ. إليك نظرة على أوجه التشابه والاختلاف بين هذه الأنظمة:

أوجه التشابه:

١. **الحقوق الأساسية للمستهلكين:** جميع الأنظمة تقدم حماية للمستهلكين تشمل الحق في الحصول على معلومات دقيقة عن المنتجات والخدمات، الحق في السلامة، والحماية من الممارسات التجارية غير العادلة والمضللة.

٢. **حماية البيانات والخصوصية:** كل من الاتحاد الأوروبي وأستراليا والولايات المتحدة لديها تشريعات محددة لحماية بيانات وخصوصية المستهلكين، مع التركيز بشكل خاص على البيانات الشخصية.

٣. **التجارة الإلكترونية:** تنظيم التجارة الإلكترونية وتوفير ضمانات للمعاملات عبر الإنترنت هو جانب مشترك، بما في ذلك حقوق مثل الإلغاء والاسترجاع للمشتريات عبر الإنترنت.

أوجه الاختلاف:

١. نطاق وشمولية القوانين:

- الاتحاد الأوروبي يتبع نهجًا شاملاً جدًا مع قوانين مثل GDPR لحماية البيانات والتوجيهات الخاصة بحقوق المستهلكين التي يجب تطبيقها في جميع دول الاتحاد.
- في الولايات المتحدة، القوانين موزعة بين الفيدرالية والولايات، مع وجود بعض الفروق في التطبيق والتنفيذ عبر الولايات المختلفة.
- أستراليا لديها نظام موحد على مستوى البلاد مع قوانين مثل قانون المستهلك الأسترالي (ACL) وقانون الخصوصية لعام ١٩٨٨.

٢. حماية البيانات:

- GDPR في الاتحاد الأوروبي يعتبر من أقوى قوانين حماية البيانات في العالم، مع توفير حقوق واسعة للأفراد بخصوص بياناتهم الشخصية.
- الولايات المتحدة ليس لديها قانون فيدرالي موحد لحماية البيانات يضاهي GDPR، ولكن بعض الولايات مثل كاليفورنيا لديها قوانين قوية لحماية البيانات.
- أستراليا توفر حماية قوية للبيانات عبر قانون الخصوصية لعام ١٩٨٨، مع مبادئ الخصوصية الأسترالية التي تنظم جمع واستخدام البيانات.

٣. الإنفاذ والعقوبات:

- الاتحاد الأوروبي وأستراليا يمتلكان آليات واضحة للإنفاذ مع إمكانية فرض عقوبات كبيرة للمخالفات، خاصةً في مجال حماية البيانات.
- في الولايات المتحدة، الإنفاذ يمكن أن يختلف بشكل كبير اعتمادًا على القانون والولاية، مع وجود دور كبير للدعاوى القضائية الجماعية كوسيلة للمستهلكين للحصول على تعويض.

بشكل عام، بينما تشترك قوانين حماية المستهلك في الأهداف الأساسية عبر هذه الأقاليم، فإن الاختلافات في التطبيق، الإنفاذ، والتركيز (مثل حماية البيانات في الاتحاد الأوروبي مقابل التركيز الأكبر على حقوق المستهلك في العقود والضمانات في أستراليا والولايات المتحدة) تبرز الاختلافات في النهج القانوني لكل منطقة.

وختاما، هناك سؤال مطروح متعلق بـ: **هل القوانين الحالية كافية لحماية خصوصية المستهلك الالكتروني، من أي انتهاك أو استغلال يقع عليها؟**

تقييم كفاية القوانين الحالية لحماية خصوصية المستهلك الإلكتروني يتوقف على عدة عوامل، بما في ذلك السياق الجغرافي والتطورات التكنولوجية. بشكل عام، يمكن القول إن القوانين في العديد من الدول قد شهدت تطورات هامة لمواجهة التحديات الناشئة

في الفضاء الإلكتروني. ومع ذلك، تواجه حماية خصوصية المستهلك الإلكتروني عدة تحديات مستمرة([1]):

- **التطورات التكنولوجية السريعة:** التكنولوجيا تتطور بوتيرة أسرع من تحديث القوانين، مما يجعل الأطر التنظيمية الحالية غير كافية أو متأخرة في بعض الأحيان لمواجهة أساليب الانتهاك والاستغلال الجديدة.
- **العابرة للحدود:** خصوصية المستهلك الإلكتروني تتأثر بالأنشطة التي تتم عبر الحدود الوطنية، مما يجعل التنظيم والإنفاذ صعبين بدون تعاون دولي فعّال.
- **الحاجة إلى التوازن:** يجب على القوانين التوازن بين حماية خصوصية المستهلك وتشجيع الابتكار والنمو الاقتصادي. القيود الصارمة جدًا قد تحد من التطور التكنولوجي، بينما القوانين المرنة جدًا قد لا توفر حماية كافية.
- **الوعي والتنفيذ:** حتى مع وجود قوانين قوية، قد يكون هناك نقص في الوعي بين المستهلكين حول حقوقهم وكيفية حمايتها. كما أن التحديات المتعلقة بتنفيذ ومراقبة الامتثال للقوانين تظل قائمة.

[1]) Donmaz, A. op. cit., p 156.

- **استجابة السوق:** الشركات والمنصات الإلكترونية قد لا تكون دائمًا سريعة في تطبيق معايير الخصوصية وحماية البيانات المطلوبة، سواء بسبب التكلفة أو التعقيد التكنولوجي.

لتحسين الحماية، يُنظر إلى التحديث المستمر للقوانين ليشمل التقنيات الجديدة، تعزيز التعاون الدولي، تشجيع الشفافية وممارسات البيانات الجيدة من قبل الشركات، وزيادة الوعي بين المستهلكين كخطوات ضرورية. بالإضافة إلى ذلك، قد تساهم التكنولوجيا نفسها، مثل البلوك تشين والتشفير المتقدم، في توفير حلول لحماية خصوصية المستهلك بشكل أفضل في المستقبل.

الفصل الثاني

الجرائم ضد المستهلك الالكتروني وتحديات الحماية منها

تمهيد وتقسيم:

الجرائم ضد المستهلك الإلكتروني تشكل تحديًا كبيرًا في عصر الرقمنة المتسارع. هذه الجرائم تتخذ أشكالًا متعددة، بما في ذلك الاحتيال المالي، سرقة الهوية، البرمجيات الخبيثة، والتصيد الاحتيالي. الأساليب المستخدمة في هذه الجرائم تتطور باستمرار، مما يجعل من الصعب على المستهلكين والمؤسسات البقاء على اطلاع دائم بأحدث التهديدات. الجرائم الإلكترونية لا تقتصر على النطاق المحلي فحسب، بل تتجاوز الحدود الجغرافية، مما يجعل من الصعب تتبع ومقاضاة الجناة.

تحديات الحماية من الجرائم ضد المستهلك الإلكتروني تشمل الحاجة إلى توعية المستهلكين بالمخاطر الإلكترونية وكيفية الوقاية منها. يجب على المستهلكين تعلم كيفية تأمين بياناتهم الشخصية والمالية، وكيفية التعرف على رسائل البريد الإلكتروني الاحتيالية والروابط المشبوهة. من الضروري أيضًا أن تقوم الشركات بتعزيز أمان

أنظمتها الإلكترونية والتأكد من أن سياسات الخصوصية والأمان الخاصة بها تتوافق مع أحدث المعايير والتشريعات([1]).

مواجهة الجرائم ضد المستهلك الإلكتروني تتطلب جهودًا مشتركة من الحكومات، القطاع الخاص، والمنظمات الدولية. القوانين والتشريعات الخاصة بالجرائم الإلكترونية يجب أن تكون محدثة وفعالة في مواجهة التهديدات الجديدة. كما يجب على السلطات تعزيز التعاون الدولي في مكافحة هذه الجرائم، وتبادل المعلومات وأفضل الممارسات في مجال الأمن الإلكتروني. إن الجهود المتضافرة هي المفتاح لحماية المستهلكين والحفاظ على بيئة رقمية آمنة للجميع.

ونتناول في هذا الباب، الجرائم الالكترونية ضد المستهلكين وطرق الحماية منها في مبحث أول، وتحديات تطبيق قوانين حماية المستهلك الالكتروني في مبحث ثانٍ، وتأثير التكنولوجيا والتطورات الرقمية على الحماية الجنائية للمستهلك في مبحث ثالث.

[1]) Robert D. Atkinson and Stephen J. Ezell, op. cit., p. 175

المبحث الأول

الجرائم الإلكترونية ضد المستهلكين وطرق الحماية منها

الجرائم الإلكترونية التي تستهدف المستهلكين تشكل تهديدًا متزايدًا في عالم يزداد اعتماده على التكنولوجيا والإنترنت. هذه الجرائم تأتي في أشكال متعددة، ويمكن تصنيفها إلى عدة أنواع رئيسية مثل: الاحتيال عبر الانترنت، وسرقة الهوية، والبرمجيات الخبيثة، التصيد الاحتيالي، والتنمر والتهديد الالكتروني، والتجسس الالكتروني والتتبع، وهجمات الحرمان من الخدمة. ونستعرض كل جريمة من تلك الجرائم بشيء من التفصيل.

أولًا– النصب (الاحتيال) عبر الانترنت:

يتضمن دفع المستهلكين مقابل سلع أو خدمات لا يتم تسليمها هو نوع شائع من الجرائم الإلكترونية التي تستهدف المستهلكين في العصر الرقمي. هذا النوع من الاحتيال يمكن أن يأخذ أشكالاً متعددة وينفذ عبر وسائل مختلفة على الإنترنت([1]). ونشرح كيف يحدث وبعض الإجراءات التي يمكن للمستهلكين اتخاذها لحماية أنفسهم:

[1]) نسيمة درار، المستهلك الرقمي وقصور القوانين الكلاسيكية الناظمة لحمايته، مجلة المفكر، ع١٥، جامعة محمد خيضر بسكرة - كلية الحقوق والعلوم السياسية، ٢٠١٧، ص ٢٢٩.

- **كيف يحدث الاحتيال؟([1])**

١- مواقع وهمية: ينشئ المحتالون مواقع تجارة إلكترونية مزيفة تبدو شرعية وتعرض منتجات بأسعار جذابة. بعد إجراء الدفع، لا يتم شحن أي منتجات.

٢- عروض عبر وسائل التواصل الاجتماعي: قد يعلن المحتالون عن سلع أو خدمات عبر منصات التواصل الاجتماعي، وبعد الدفع، لا يتم تقديم الخدمة أو إرسال السلعة.

٣- المزادات الوهمية: يتم إنشاء مزادات مزيفة على الإنترنت حيث يفوز المستهلكون بالعروض ويدفعون للمنتجات التي لا تصل أبدًا.

- **كيف يمكن للمستهلكين حماية أنفسهم؟([2])**

١- التحقق من مصداقية الموقع: قبل إجراء أي شراء، يجب التحقق من مصداقية الموقع عبر البحث عن تقييمات ومراجعات من مستهلكين آخرين.

---

[1]) Federal Trade Commission. (2020). Online Shopping Scams. https://www.consumer.ftc.gov/articles/online-shopping-scams visit on 20-3-2024.

[2]) الجهاز القومي لتنظيم الاتصالات (NTRA)، "النصائح لحماية نفسك عند التسوق عبر الإنترنت"، ٢٠٢١.
Online:
https://www.ntra.gov.eg/arabic/news_center/ecommerce/Eshopping.aspx
تمت زيارته بتاريخ ٢١-٣-٢٠٢٤.

٢- استخدام طرق دفع آمنة: استخدام بطاقات الائتمان أو خدمات الدفع الإلكترونية التي توفر حماية للمشتريات يمكن أن يقدم طبقة إضافية من الأمان.

٣- الحذر من العروض التي تبدو جيدة جدًا لتكون حقيقية: الأسعار التي تبدو منخفضة بشكل غير معقول يمكن أن تكون مؤشرًا على عملية احتيال.

٤- التحقق من سياسة الاسترجاع والتواصل: التحقق من وجود سياسة استرجاع واضحة وسبل تواصل فعالة مع البائع قبل الشراء([1]).

٥- الانتباه لتفاصيل الدفع: تجنب إدخال تفاصيل الدفع إلا في صفحات ويب آمنة (تلك التي تبدأ بـ HTTPS).

٦- استخدام الحس السليم: إذا كانت هناك أي شكوك حول شرعية عرض، من الأفضل التراجع وإجراء المزيد من البحث.

وهنا سؤال يطرح نفسه، متعلق بـ: ما الحد الفاصل بين جريمتي النصب والغش التجاري، في التجارة الالكترونية؟

[1]) حيث قد يكون سبب الاسترجاع ان السلعة ليس فقط غير مناسبة، أو لم تلق قبول المشتر، ولكن قد يكون السبب هو وجود عيب بالسعلة. وقد قضت محكمة النقض المصرية بان: "تقدير الظروف التي يستفاد منها علم الجاني بعيب السلعة المباعة من عدمه موضوعي لمحكمة الموضوع" الطعن رقم ٢٢١٣٠ لسنة ٨٨ ق – جلسة ٢٠١٩/٣/١١.

٢- الحماية الجنائية للمستهلك الإلكتروني

في التجارة الإلكترونية، الحد الفاصل بين النصب والغش التجاري يمكن أن يكون غامضًا، لكن يمكن تحديده من خلال فهم الخصائص الأساسية لكل منهما وكيف تتم ممارستهما في السياق الإلكتروني.

النصب:

تعريف: النصب يشير إلى عملية احتيالية تهدف إلى خداع الضحية للحصول على مال أو ممتلكات من خلال تمثيل كاذب أو مضلل. في التجارة الإلكترونية، يمكن أن يشمل ذلك مواقع الويب الوهمية التي تبيع منتجات غير موجودة أو التي تقدم عروضًا خادعة. وقد قضت محكمة النقض المصرية بأن: "جريمة خلق انطباع مضلل لدى المستهلك، عدم تطلبها سوى القصد الجنائي العام، مناط تحققه تعمد اقتراف الفعل المادي والنتيجة المترتبة عليه"([1])

الخصائص: يركز النصب على استخدام الخداع لإقناع الضحية بالتصرف بطريقة تؤدي إلى فقدان مالي، عادةً من خلال وعود كاذبة أو عروض وهمية.

[1]) الطعن رقم ٢٢١٣٠ لسنة ٨٨ق – جلسة ٢٠١٩/٣/١١.

الغش التجاري:

تعريف: الغش التجاري يتعلق بممارسات تجارية غير أمينة أو غير عادلة تضلل المستهلكين أو تخدعهم بشأن طبيعة المنتج أو الخدمة. في التجارة الإلكترونية، قد يشمل ذلك التلاعب بالمراجعات الإيجابية، بيع منتجات مقلدة كأصلية، أو عدم الكشف عن معلومات هامة حول المنتج([1]).

الخصائص: يشمل الغش التجاري مجموعة واسعة من الممارسات التي تؤثر على قرار الشراء بطريقة غير عادلة، مثل إخفاء العيوب، التضليل حول المواصفات، أو استخدام شروط خدمة مضللة.

الحد الفاصل:

الحد الفاصل بين النصب والغش التجاري في التجارة الإلكترونية يكمن في نوايا وأساليب الممارسة:

النصب يتمحور حول الاحتيال المباشر والخداع الواضح للحصول على مال الضحايا من خلال تمثيلات كاذبة. بينما الغش التجاري يتعلق بالممارسات التجارية التي تضلل الضحايا بشأن جودة أو طبيعة المنتج أو الخدمة، وقد لا تكون بالضرورة احتيالية

[1]) عبدالحليم بوقرين، نحو حماية جنائية للمستهلك الإلكتروني، مجلة الفكر القانوني والسياسي، ع١، جامعة عمار ثليجي الاغواط - كلية الحقوق والعلوم السياسية، ٢٠١٧، ص ١١.

بشكل صريح ولكنها تؤدي إلى خسارة للمستهلك بسبب المعلومات المضللة أو غير الكاملة([1]).

وفي كلتا الحالتين، الحماية الفعالة للمستهلك تتطلب وعيًا مستمرًا وتطبيقًا صارمًا للقوانين والأنظمة التي تكافح النصب والغش التجاري في البيئة الرقمية.

وننتقل إلى سؤال اخر وهو: هل يمكن ضبط جرائم الاحتيال الالكتروني الواقعة على المستهلك؟

ضبط جرائم الاحتيال الإلكتروني التي تقع على المستهلكين يمكن تحقيقه بفعالية من خلال تطبيق مجموعة من الاستراتيجيات المتكاملة التي تشمل التكنولوجيا، التشريعات، التعاون الدولي، وتعزيز الوعي العام. إليك كيف يمكن ضبط هذه الجرائم:

١. **تطوير التكنولوجيا والأدوات الأمنية:** استخدام تقنيات متقدمة للكشف عن الاحتيال والتحليلات التنبؤية يمكن أن يساعد في تحديد الأنشطة الاحتيالية بسرعة. أدوات مثل الذكاء الاصطناعي وتعلم الآلة يمكن أن تساعد في التعرف على الأنماط والسلوكيات الاحتيالية عبر الإنترنت.

[1]) نادية حموتى، الحماية الجنائية من جرائم الغش التجاري، مجلة القانون والأعمال، ع٦٧، جامعة الحسن الأول - كلية العلوم القانونية والاقتصادية والاجتماعية - مختبر البحث قانون الأعمال، ٢٠٢١، ص ١٣٨.

٢. **تعزيز الإطار التشريعي والتنظيمي:** القوانين والتشريعات التي تعرف جرائم الاحتيال الإلكتروني بوضوح وتفرض عقوبات صارمة على المرتكبين تشكل رادعًا قويًا. يجب أن تكون هذه القوانين محدثة لتعكس التطورات التكنولوجية الجديدة.

٣. **التعاون الدولي:** نظرًا لطبيعة الإنترنت العالمية، فإن التعاون بين الوكالات الإنفاذية والهيئات التنظيمية عبر الحدود أساسي لضبط الجرائم الإلكترونية. تبادل المعلومات وأفضل الممارسات يساعد في مكافحة الجرائم العابرة للدول.

٤. **تعزيز الوعي بين المستهلكين:** توعية المستهلكين بالمخاطر الإلكترونية وكيفية حماية أنفسهم أمر ضروري. حملات التوعية يمكن أن تشمل تعليم المستهلكين حول العلامات التحذيرية للرسائل الاحتيالية، كيفية التحقق من الأمان الإلكتروني للمواقع الإلكترونية، والإجراءات الواجب اتخاذها عند التعرض للاحتيال.

٥. **تحسين آليات الإبلاغ والاستجابة:** تسهيل عملية إبلاغ المستهلكين عن الحوادث الاحتيالية وضمان استجابة سريعة وفعالة من السلطات يمكن أن يساعد في تقليل الضرر وربما ضبط الجناة.

على الرغم من التحديات، من خلال تطبيق هذه الاستراتيجيات بشكل متكامل ومستمر، يمكن تحسين قدرة السلطات على ضبط جرائم الاحتيال الإلكتروني ضد المستهلكين وتوفير بيئة رقمية أكثر أمانًا للجميع.

ثانيًا- سرقة الهوية:

هي جريمة إلكترونية خطيرة ومتزايدة تؤثر على الأفراد في جميع أنحاء العالم. تتضمن هذه الجريمة الوصول غير المصرح به واستخدام المعلومات الشخصية والمالية للضحايا بغرض الاحتيال أو الكسب غير المشروع. ونعرض كيف يمكن أن تحدث سرقة الهوية والتدابير التي يمكن اتخاذها للحماية منها:

- **كيف تحدث سرقة الهوية؟([1])**

١- التصيد الإلكتروني (Phishing): استخدام رسائل بريد إلكتروني مزيفة أو مواقع ويب تبدو شرعية لخداع الأفراد للكشف عن معلوماتهم الشخصية.

٢- البرمجيات الخبيثة: استخدام برامج ضارة لاختراق الأجهزة وسرقة المعلومات الشخصية والمالية.

٣- السرقة الفيزيائية: سرقة المحافظ، الحقائب، أو البريد للحصول على بطاقات الائتمان، بيانات البنك، أو أي وثائق تحتوي على معلومات شخصية.

[1]) ديفيد ماكي، أمن المعلومات: حماية البيانات الحاسوبية الحيوية، دار المنهل، ٢٠١٨، ص ١٥٦.

٤- الاستغلال عبر الإنترنت: استغلال الثغرات الأمنية في الشبكات الاجتماعية أو قواعد بيانات الشركات للحصول على معلومات شخصية.

- **كيفية الحماية من سرقة الهوية([1]):**

١- الحماية الرقمية: استخدام برمجيات أمان قوية وتحديثها بانتظام لحماية الأجهزة من البرمجيات الخبيثة.

٢- الحذر على الإنترنت: تجنب الكشف عن معلومات شخصية مهمة عبر الإنترنت، خاصةً على مواقع غير مأمونة أو في رسائل البريد الإلكتروني.

٣- استخدام كلمات مرور قوية: إنشاء كلمات مرور قوية وفريدة لكل حساب وتغييرها بانتظام.

٤- مراقبة الحسابات المالية: تفقد كشوف الحسابات البنكية وبيانات بطاقات الائتمان بانتظام للتأكد من عدم وجود أنشطة مشبوهة.

٥- تأمين الوثائق الشخصية: حماية المعلومات الشخصية في المنزل وتدمير الوثائق التي تحتوي على معلومات حساسة قبل التخلص منها.

٦- التحقق من الائتمان: استخدام خدمات التحقق من الائتمان بانتظام للكشف عن أي استخدام غير مصرح به للمعلومات الشخصية.

[1]) David B. Jacobs, "Identity Theft: How to Protect Your Name, Your Credit and Your Vital Information, and What to Do When Someone Hijacks Any of These", Sourcebooks Inc, 2004, p. 74

٢- الحماية الجنائية للمستهلك الإلكتروني

هل يُعد استعمال بطاقة ائتمان تعود لشخص آخر – بدون علمه – جريمة؟

استخدام بطاقة ائتمانية تخص شخصًا آخر لشراء منتجات أو خدمات إلكترونية دون إذن صاحب البطاقة يمكن أن يندرج تحت عدة أوصاف جنائية، اعتمادًا على القوانين المحلية والظروف المحيطة بالحادثة([1]). بعض هذه الأوصاف قد تشمل:

١. **الاحتيال:** استخدام بطاقة ائتمانية دون إذن يعتبر شكلاً من أشكال الاحتيال، خاصة إذا كان الشخص يتظاهر بأنه صاحب البطاقة أو يقدم معلومات كاذبة لإتمام العملية الشرائية.

٢. **سرقة الهوية:** إذا تضمنت العملية استخدام معلومات شخصية تخص صاحب البطاقة (مثل الاسم وعنوان البريد الإلكتروني) لتسهيل الشراء دون موافقته، يمكن اعتبار ذلك سرقة هوية.

٣. **الاستخدام غير المشروع لبطاقات الائتمان:** العديد من القوانين تعاقب على استخدام بطاقة ائتمانية بشكل غير مشروع، وهذا يشمل استخدام بطاقة شخص آخر دون إذن.

[1]) فاطمة آيت الغازي، الحماية الجنائية للمستهلك في التعاقد الإلكتروني: دراسة مقارنة، مجلة قراءات علمية في الأبحاث والدراسات القانونية والإدارية، ع١٣، ٢٠٢٢، ص ٣٨٥.

٤. التزوير: في بعض الحالات، قد يتم تصنيف استخدام بطاقة ائتمان تخص شخصًا آخر كجريمة تزوير، خاصة إذا كان الشخص المرتكب قد قام بتزوير التوقيع أو استخدم البطاقة بطريقة توحي بأنه صاحبها الشرعي.

ومن الجدير بالذكر أن العواقب القانونية لمثل هذه الأفعال يمكن أن تكون شديدة وتشمل الغرامات المالية الكبيرة، السجن، والتسجيل كمجرم في سجلات الشرطة. القوانين تختلف من دولة لدولة، لكن الاستخدام غير المشروع لبطاقة ائتمانية يعتبر جريمة في معظم الأنظمة القانونية حول العالم.

ومن المهم للغاية عدم استخدام بطاقة ائتمانية تخص شخصًا آخر دون الحصول على موافقة صريحة وواضحة من صاحب البطاقة. في حالة الحاجة إلى استخدام بطاقة شخص آخر، ينبغي دائمًا القيام بذلك تحت إشرافه وموافقته الكاملة لتجنب أي مسؤولية قانونية.

ثالثًا– البرمجيات الخبيثة (Malware):

البرمجيات الخبيثة هي أحد أبرز التهديدات الأمنية التي تواجه المستخدمين في العصر الرقمي. تعمل هذه البرمجيات على إلحاق الضرر بالأجهزة الفردية، الشبكات،

والبيانات، غالبًا بغرض السرقة أو الاحتيال. يمكن تصنيف البرمجيات الخبيثة إلى عدة أنواع رئيسية، كل منها يمتلك طرق عمل مختلفة وأهدافًا متنوعة:

١- الفيروسات:

الوصف: برامج ضارة تلحق نفسها ببرامج أخرى وتنتشر عند تنفيذ البرنامج المضيف، مما يسبب الضرر للنظام.

الهدف: يمكن أن تهدف لتدمير البيانات، تعطيل الأنظمة، أو كجزء من هجوم أكبر([١]).

٢- الديدان:

الوصف: برامج ضارة قادرة على الانتشار بنفسها عبر الشبكات، دون الحاجة إلى تدخل المستخدم أو التلاحق ببرنامج آخر.

الهدف: غالبًا ما تستخدم لإلحاق الضرر بالشبكات، سرقة البيانات، أو تثبيت برامج ضارة أخرى.

[١]) Peter Szor, The Art of Computer Virus Research and Defense, Addison-Wesley Professional, 2005, p 43.

٣- تروجان (Trojan Horse):

الوصف: برمجيات تُقدم نفسها كبرامج مشروعة لخداع المستخدمين لتثبيتها، لكنها في الحقيقة تحمل نوايا ضارة.

الهدف: يمكن أن تستخدم لإنشاء باب خلفي في النظام يسمح بالوصول غير المصرح به، سرقة البيانات، أو تثبيت المزيد من البرمجيات الخبيثة([1]).

٤- برامج التجسس (Spyware):

الوصف: برمجيات تُصمم لجمع المعلومات من الأجهزة دون علم المستخدم أو موافقته.

الهدف: جمع البيانات الشخصية والمالية، مراقبة سلوك المستخدم على الإنترنت، والإعلان الموجه([2]).

كيفية الحماية من البرمجيات الخبيثة([3]):

- استخدام برمجيات مكافحة الفيروسات: تثبيت وتحديث برمجيات مكافحة الفيروسات والبرمجيات الخبيثة بانتظام.

[1]) Richard Ford and William R. Cheswick, Firewalls and Internet Security: Repelling the Wily Hacker, Addison-Wesley Professional, 2003, p. 98.
[2]) Ed Tittel and Kim Lindros, Spyware For Dummies, Wiley, 2004, p. 45.
[3]) Peter Szor, op. cit., p. 325.

- تحديث النظام والبرامج: الحفاظ على تحديث نظام التشغيل وجميع البرامج المثبتة لإغلاق أي ثغرات أمنية.
- الحذر من الروابط والمرفقات: تجنب النقر على روابط أو فتح مرفقات في رسائل بريد إلكتروني مشبوهة.
- استخدام كلمات مرور قوية: إنشاء كلمات مرور قوية وفريدة للحسابات المختلفة للحد من خطر الاختراق.
- النسخ الاحتياطي للبيانات: إجراء نسخ احتياطي منتظم للبيانات يمكن أن يساعد في استعادة النظام في حالة الإصابة ببرمجيات خبيثة.

رابعًا- التصيد الاحتيالي (Scams):

يمثل تحديًا كبيرًا في البيئة الرقمية الحالية، حيث يستخدم المحتالون تكتيكات متقنة لاستغلال ثقة الأفراد وجهلهم بالأمور المالية والأمن الإلكتروني. يمكن أن تتخذ هذه الأساليب أشكالاً متعددة، وتهدف جميعها إلى الاستيلاء على الأموال أو المعلومات الشخصية للضحايا. ونشرح بعض الأمثلة الشائعة للتصيد الاحتيالي وكيفية حماية نفسك:

- **أمثلة للتصيد الاحتيالي([1]):**

١- الرسائل المزيفة: إرسال رسائل بريد إلكتروني أو رسائل نصية تبدو كأنها من مؤسسات مالية أو شركات معروفة تطلب منك التحقق من حسابك أو تحديث معلوماتك الشخصية.

٢- الجوائز واليانصيب: إخبارك بأنك فزت بجائزة كبيرة أو يانصيب، ولكن للمطالبة بها، يجب عليك أولاً دفع رسوم أو ضرائب.

٣- العروض الاستثمارية: تقديم فرص استثمارية تبدو مربحة بشكل لا يصدق مع ضمانات عالية للربح، والتي غالبًا ما تكون مخاطرها عالية جدًا أو مزيفة تمامًا.

٤- العلاقات العاطفية: إنشاء علاقات عاطفية مزيفة عبر الإنترنت ومن ثم طلب الأموال للطوارئ الصحية، تذاكر السفر، أو غيرها من الأسباب الوهمية.

- **كيفية الحماية من التصيد الاحتيالي([2]):**

[1]) Christopher Hadnagy, Social Engineering: The Art of Human Hacking, Wiley, 2010, p. 145.
[2]) Peter W. Singer and Allan Friedman, Cybersecurity and Cyberwar: What Everyone Needs to Know, Oxford University Press, 2014, p. 85.

١- التحقق من المصادر: تأكد دائمًا من أن الاتصالات التي تتلقاها من مؤسسات مالية أو شركات أخرى هي فعلاً من مصادر موثوقة. لا تتبع الروابط الموجودة في رسائل البريد الإلكتروني المشبوهة.

٢- الحذر من العروض المغرية: كن حذرًا من أي عرض يبدو جيدًا جدًا ليكون حقيقيًا. الاستثمارات الواقعية تتطلب البحث والتحليل ولا تضمن عوائد مالية فورية أو كبيرة.

٣- حماية المعلومات الشخصية: لا تشارك معلوماتك الشخصية أو المالية إلا مع مواقع وخدمات تثق بها وتستخدم اتصالات مشفرة (HTTPS).

٤- استخدام برمجيات الأمان: تأكد من أن جهازك محمي ببرمجيات مكافحة الفيروسات والبرمجيات الخبيثة، وأنها محدثة باستمرار.

٥- التعليم والوعي: اطلع بانتظام على أحدث الأساليب التي يستخدمها المحتالون وشارك هذه المعلومات مع الأصدقاء والعائلة.

خامسًا- التنمر والتهديد الالكتروني:

التنمر والتهديد الإلكتروني يشكلان أحد الوجوه القاتمة للعالم الرقمي، مما يؤدي إلى آثار نفسية وعاطفية ضارة على الضحايا. هذه الأفعال تتراوح بين الإساءة اللفظية والجسدية الافتراضية إلى التهديدات المباشرة والابتزاز، وغالبًا ما تتم في الأماكن

الرقمية حيث يتفاعل الناس، مثل وسائل التواصل الاجتماعي، المنتديات، وألعاب الفيديو عبر الإنترنت.

- **أشكال التنمر والتهديد الإلكتروني([1]):**

١- الإساءة اللفظية أو النفسية: استخدام اللغة لإهانة، تخويف، أو تحقير الآخرين.

٢- الابتزاز الإلكتروني: تهديد شخص بنشر معلومات أو صور خاصة على الإنترنت ما لم يتم تلبية مطالب المبتز.

٣- التهديدات: إرسال رسائل تحمل تهديدات بالأذى الجسدي أو الضرر بأي شكل آخر.

٤- المضايقة: ملاحقة الشخص عبر الإنترنت بشكل مستمر بالرسائل أو التعليقات.

٥- التشهير: نشر ادعاءات كاذبة عن شخص ما لتشويه سمعته.

[1]) Robin M. Kowalski, Susan P. Limber, and Patricia W. Agatston, Cyberbullying: Bullying in the Digital Age, Wiley-Blackwell, 2012, p. 50.

- **كيفية الحماية والرد([1]):**

١- تعزيز الإعدادات الخاصة بالخصوصية: استخدم إعدادات الخصوصية على منصات التواصل الاجتماعي للتحكم فيمن يمكنه رؤية المحتوى والتفاعل معه.

٢- الحفاظ على الأدلة: احتفظ بنسخ من الرسائل، التعليقات، أو أي شكل آخر من التواصل كدليل.

٣- الإبلاغ والحجب: استخدم أدوات الإبلاغ المتاحة على المنصات الرقمية للإبلاغ عن التنمر أو التهديد وحجب الأشخاص المسيئين.

٤- طلب المساعدة: تحدث مع أصدقائك، عائلتك، أو مهنيين للحصول على الدعم العاطفي والمشورة.

٥- التواصل مع السلطات: في حالات الابتزاز أو التهديدات الجدية، قد يكون من الضروري التواصل مع السلطات المحلية أو الجهات الأمنية.

[1]) Sameer Hinduja and Justin W. Patchin, Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying, Corwin Press, 2015, p. 95.

سادسًا– التجسس الالكتروني والتتبع:

التجسس الإلكتروني والتتبع يشيران إلى مجموعة من التقنيات والأساليب التي تُستخدم لجمع المعلومات حول الأفراد دون معرفتهم أو موافقتهم. هذه الأنشطة تهدد خصوصية المستخدمين وأمانهم عبر الإنترنت، ويمكن أن تشمل([1]):

١- برامج التجسس (Spyware):

برامج تُثبت سرًا على جهاز الكمبيوتر أو الجهاز المحمول لمراقبة النشاطات وجمع المعلومات دون علم المستخدم. يمكن أن تجمع بيانات مثل تاريخ التصفح، تسجيلات الدخول والكلمات السرية، البيانات المالية، والمراسلات الشخصية.

٢- التتبع عبر الإنترنت:

يشمل استخدام ملفات تعريف الارتباط (Cookies)، بكسلات التتبع، وغيرها من تقنيات التتبع لجمع المعلومات حول سلوك المستخدمين على الإنترنت، مثل المواقع التي يزورونها، الإعلانات التي ينقرون عليها، وتفاعلاتهم على الشبكات الاجتماعية.

[1]) Bruce Schneier, Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World, W. W. Norton & Company, 2015, p. 110.

٣- أدوات التحليل:

الشركات والمواقع تستخدم أدوات التحليل لجمع البيانات حول كيفية تفاعل المستخدمين مع منتجاتهم أو خدماتهم عبر الإنترنت، مما يوفر رؤى حول تفضيلات وسلوكيات المستهلكين.

كيفية الحماية من التجسس الإلكتروني والتتبع([1]):

١- استخدام برمجيات مكافحة التجسس والفيروسات: تثبيت وتحديث برمجيات الأمان للكشف عن وإزالة برامج التجسس وغيرها من البرمجيات الخبيثة.

٢- تحديث النظام والبرامج: الحفاظ على تحديث نظام التشغيل والتطبيقات لإغلاق الثغرات الأمنية التي يمكن أن تُستغل للتجسس.

٣- استخدام مدير كلمات مرور: لإنشاء وتخزين كلمات مرور قوية وفريدة لكل حساب، مما يحد من خطر الاختراق.

٤- استخدام شبكات VPN: استخدام شبكة خاصة افتراضية (VPN) لتشفير حركة الإنترنت وحماية البيانات من التتبع.

[1]) Michael Gregg, Certified Ethical Hacker (CEH) Version 10 Cert Guide, Pearson IT Certification, 2018, p. 250.

٥- تقييد ملفات تعريف الارتباط واستخدام وضع التصفح الخفي: تقييد ملفات تعريف الارتباط في إعدادات المتصفح واستخدام وضع التصفح الخفي لتقليل التتبع.

٦- التحقق من إعدادات الخصوصية: تعديل إعدادات الخصوصية على الشبكات الاجتماعية والخدمات عبر الإنترنت للحد من جمع البيانات.

كيف يمكن تحجيم المواقع الالكترونية من عدم استغلال بيانات المستهلكين في الاغراض التجارية؟

تحجيم المواقع الإلكترونية لمنع استغلال بيانات المستهلكين في الأغراض التجارية يتطلب مجهودًا مشتركًا من الحكومات، الهيئات التنظيمية، والصناعة نفسها. يمكن تحقيق ذلك من خلال عدة استراتيجيات([1]):

١. **تشريعات واضحة وصارمة:** تطوير وتنفيذ تشريعات تحمي بيانات المستهلكين وتحدد بوضوح كيفية جمع البيانات، استخدامها، ومشاركتها. مثال على ذلك هو اللائحة العامة لحماية البيانات (GDPR) في الاتحاد الأوروبي التي تفرض قواعد صارمة بشأن البيانات الشخصية.

[1]) Daniel J. Solove and Paul M. Schwartz, Information Privacy Law, Wolters Kluwer Law & Business, 2019, p. 120

٢. **الموافقة المستنيرة:** ضمان حصول المواقع الإلكترونية على موافقة صريحة وواضحة من المستخدمين قبل جمع بياناتهم الشخصية واستخدامها لأغراض تجارية. يجب أن تكون هذه الموافقة قابلة للسحب في أي وقت.

٣. **الشفافية والمساءلة:** إلزام المواقع الإلكترونية بتوفير سياسات خصوصية واضحة ومفهومة تشرح كيفية جمع البيانات واستخدامها. كما يجب على هذه المواقع توفير طرق للمستخدمين للوصول إلى بياناتهم الشخصية وتصحيحها أو حذفها.

٤. **تحديد الغرض:** مطالبة المواقع بتحديد الأغراض الدقيقة لجمع البيانات واستخدامها فقط لتلك الأغراض المعلنة، مما يمنع استخدام البيانات لأغراض لم يتم الكشف عنها أو الموافقة عليها من قبل المستخدم.

٥. **تعزيز الأمن السيبراني:** ضمان تطبيق أفضل الممارسات والمعايير الأمنية لحماية بيانات المستخدمين من الوصول غير المصرح به، التعديل، الكشف، أو الدمار.

٦. **تحفيز الممارسات الجيدة في الصناعة:** تشجيع المواقع الإلكترونية على اعتماد شهادات الخصوصية والأمان، مثل ISO/IEC 27001، والمشاركة في برامج الخصوصية التي تقدم تقييمًا ذاتيًا ومستقلًا لممارسات الخصوصية والأمان.

٧. **تمكين المستهلكين:** توفير وسائل وأدوات تمكن المستهلكين من إدارة خصوصيتهم بشكل فعال، مثل إعدادات الخصوصية المتقدمة، وأدوات التحكم في الإعلانات، وخيارات الاعتراض على معالجة البيانات([1]).

من خلال تطبيق هذه الاستراتيجيات، يمكن تحجيم المواقع الإلكترونية من استغلال بيانات المستهلكين في الأغراض التجارية بشكل غير مشروع أو غير مرغوب فيه، مما يعزز حماية المستهلكين في البيئة الرقمية.

وننتقل لسؤال اخر وهو: ما حدود المواقع والمتاجر الالكترونية، في جمع واستغلال بيانات مرتاديها؟

حدود المواقع والمتاجر الإلكترونية في جمع واستغلال بيانات مرتاديها تُحدد بشكل أساسي من خلال القوانين والتشريعات الوطنية والدولية لحماية البيانات وخصوصية المستخدمين. هذه الحدود تعتمد على مبادئ أساسية متعلقة بالخصوصية وحماية البيانات، وتشمل الجوانب التالية:

١. **الشفافية والموافقة:** يجب على المواقع والمتاجر الإلكترونية أن تكون شفافة بشأن نوع البيانات التي تجمعها، وكيفية استخدام هذه البيانات. كما يجب الحصول على

[1]) شيكي حمزة، أية حماية للمستهلك من الإعلانات الإلكترونية، مجلة القانون والأعمال، ع٣٣، جامعة الحسن الأول - كلية العلوم القانونية والاقتصادية والاجتماعية - مختبر البحث قانون الأعمال، ٢٠١٨، ص ٢٠٥.

موافقة صريحة من المستخدمين قبل جمع بياناتهم الشخصية، وإعطاء المستخدمين الخيار للانسحاب وحذف بياناتهم([1]).

٢. **الحد الأدنى من جمع البيانات:** يجب ألا تجمع المواقع والمتاجر الإلكترونية سوى البيانات الضرورية فقط لتقديم الخدمة المطلوبة من قبل المستخدمين، متبعة مبدأ "الحد الأدنى من البيانات".

٣. **الأمان:** يتوجب على المواقع توفير مستويات عالية من الأمان لحماية البيانات الشخصية من الوصول غير المصرح به، الفقد، أو التعديل.

٤. **الغرض المحدد:** يجب استخدام البيانات للأغراض التي تم جمعها من أجلها فقط، ولا يجوز استخدامها في أغراض أخرى دون موافقة جديدة من المستخدم.

٥. **الاحتفاظ بالبيانات:** ينبغي على المواقع والمتاجر الإلكترونية ألا تحتفظ بالبيانات الشخصية لفترة أطول من اللازم لتحقيق الغرض الذي تم جمعها من أجله.

٦. **الحقوق الفردية:** يجب أن توفر المواقع للمستخدمين القدرة على الوصول إلى بياناتهم الشخصية، تصحيحها، وحذفها إذا رغبوا في ذلك.

[1]) Dahiyat, E.A.R. Consumer Protection in Electronic Commerce: Some Remarks on the Jordanian Electronic Transactions Law. J Consum Policy34, 2011, p 425.

٧. **المساءلة والامتثال:** المواقع مسؤولة عن الامتثال للقوانين واللوائح المعمول بها لحماية البيانات، وقد تخضع للتدقيق والمراقبة من قبل السلطات التنظيمية.

تختلف القوانين واللوائح الخاصة بحماية البيانات بشكل كبير بين الدول والمناطق، مثل اللائحة العامة لحماية البيانات (GDPR) في الاتحاد الأوروبي، وقانون الخصوصية الاستهلاكية في كاليفورنيا (CCPA) في الولايات المتحدة، والتي توفر أطرًا مفصلة لحماية بيانات المستهلكين.

سابعًا- هجمات الحرمان من الخدمة (DDoS):

هجمات الحرمان من الخدمة الموزعة (DDoS) تعد من الأساليب الشائعة التي يستخدمها المخترقون لإغراق مواقع الويب والخوادم بحركة مرور غير مشروعة وكثيفة بشكل يفوق قدرتها على الاستجابة أو البقاء متاحة للمستخدمين الشرعيين. هذه الهجمات تستهدف عادة المؤسسات أو الخدمات الإلكترونية، لكن تأثيرها يمتد ليشمل المستهلكين بطرق متعددة:

- **تأثير هجمات DDoS على المستهلكين([1]):**

١- تعطيل الخدمات: المستهلكون قد يجدون صعوبة في الوصول إلى الخدمات الأساسية عبر الإنترنت، مثل البنوك الإلكترونية، خدمات التجارة الإلكترونية، والمنصات التعليمية.

٢- تأخير في الخدمات: حتى إذا لم يتم تعطيل الخدمة كليًا، فقد تواجه بطئًا شديدًا يجعل الاستخدام الطبيعي صعبًا أو مستحيلًا.

٣- خسارة البيانات: في بعض الحالات، قد تؤدي الهجمات إلى فقدان بيانات المستهلكين أو تلفها، خصوصًا إذا كانت الهجمة جزءًا من هجوم أكثر تعقيدًا.

٤- التأثير على الثقة: المستهلكين قد يفقدون الثقة في القدرة على حماية بياناتهم وخدماتهم، مما قد يؤدي إلى تجنب استخدام بعض الخدمات الإلكترونية.

- **كيفية التعامل مع هجمات DDoS([2]):**

١- استخدام خدمات مكافحة DDoS: الشركات يمكنها الاستعانة بخدمات متخصصة للحماية ضد هجمات DDoS، التي تقدم حماية مستمرة وتخفيفًا للهجمات.

[1]) Allan Liska, DDoS Handbook: The Ultimate Guide to Everything You Need to Know About DDoS Attacks, Syngress, 2016, p. 85.
[2]) Allan Liska and Timothy Gallo, DDoS Attacks: Evolution, Detection, Prevention, Reaction, and Tolerance, Syngress, 2016, p. 95.

٢- التوعية: المستهلكون يجب أن يكونوا على دراية بأن هجمات DDoS يمكن أن تحدث وأن تأثيرها غالبًا ما يكون مؤقتًا.

٣- التحقق من المصادر الرسمية: في حالة تعرض خدمة ما لهجوم DDoS، يجب على المستهلكين التحقق من المواقع الرسمية أو حسابات وسائل التواصل الاجتماعي للشركة للحصول على تحديثات وتوجيهات.

٤- الصبر والانتظار: في كثير من الحالات، يكون الحل الأفضل هو الانتظار حتى تقوم الشركة المستهدفة بحل المشكلة واستعادة الخدمات إلى وضعها الطبيعي.

وهنا سؤال محل نقاش وهو: **كيف يمكن تحسين الأمان الإلكتروني للمنصات والخدمات الإلكترونية لحماية المستهلكين بشكل فعال؟**

تحسين الأمان الإلكتروني للمنصات والخدمات الإلكترونية يتطلب تنفيذ استراتيجيات متعددة الأوجه لضمان حماية فعالة للمستهلكين. إليك بعض الطرق الأساسية لتحقيق ذلك([1]):

[1]) Bruce Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, John Wiley & Sons, 2015, p. 150.

١. **تطبيق معايير الأمان العالية:** استخدام التشفير القوي لحماية البيانات المنقولة والمخزنة، بما في ذلك تشفير SSL/TLS للاتصالات عبر الإنترنت وتشفير البيانات على الخوادم.

٢. **حماية البنية التحتية:** تأمين البنية التحتية للشبكة باستخدام جدران الحماية، أنظمة الكشف عن التسلل، وأنظمة منع التسلل لرصد ومنع الهجمات الأمنية.

٣. **إدارة الوصول:** تطبيق سياسات صارمة لإدارة الوصول، بما في ذلك استخدام المصادقة متعددة العوامل (MFA)، لضمان أن يكون الوصول إلى المعلومات الحساسة مقصورًا على الأشخاص المصرح لهم فقط.

٤. **تحديث وصيانة النظام:** تأكد من تحديث البرمجيات والأنظمة بانتظام لإصلاح الثغرات الأمنية وتحسين ميزات الأمان.

٥. **توعية الموظفين والمستخدمين:** تدريب الموظفين على أفضل الممارسات الأمنية وتوعية المستخدمين حول كيفية حماية أنفسهم من الهجمات الإلكترونية والاحتيال.

٦. **اختبار الاختراق والتقييم:** إجراء اختبارات الاختراق وتقييمات الضعف بشكل دوري لاكتشاف ومعالجة الثغرات الأمنية قبل أن يستغلها المهاجمون.

٧. **استجابة للحوادث:** تطوير خطة استجابة للحوادث الأمنية تتضمن إجراءات للتعامل مع الانتهاكات الأمنية والحد من الضرر وإعلام المستخدمين بشكل فعال.

٨. **الامتثال للوائح والقوانين:** الامتثال للوائح الوطنية والدولية المتعلقة بحماية البيانات والخصوصية، مثل GDPR في الاتحاد الأوروبي، لضمان تطبيق معايير حماية البيانات.

٩. **تقليل البيانات المجمعة:** جمع الحد الأدنى الضروري من البيانات من المستخدمين والحفاظ على شفافية حول كيفية استخدام هذه البيانات.

١٠. **تأمين واجهات برمجة التطبيقات (APIs):** تأمين واجهات برمجة التطبيقات التي تستخدمها المنصات للتفاعل مع الخدمات الأخرى، من خلال استخدام مفاتيح التوثيق والتحقق من الصلاحيات.

بتطبيق هذه الاستراتيجيات، يمكن للمنصات والخدمات الإلكترونية تحسين الأمان الإلكتروني وحماية المستهلكين بشكل فعال من التهديدات الإلكترونية والاحتيال.

في عصر يزداد فيه اعتمادنا على التكنولوجيا والإنترنت بشكل يومي، تبرز الجرائم الإلكترونية كتهديد متنامي يستهدف المستهلكين في مختلف الأصعدة، مما يستدعي الحاجة الماسة للوعي والحماية. من الاحتيال عبر الإنترنت، وسرقة الهوية، إلى

البرمجيات الخبيثة والتجسس الإلكتروني، تتنوع هذه الجرائم في أساليبها وأهدافها، لكنها تتفق جميعًا في تهديدها للخصوصية، الأمان المالي، والثقة بالخدمات الإلكترونية. هجمات DDoS، رغم استهدافها المباشر للمؤسسات، تظهر كيف يمكن أن يتأثر المستهلكون بشكل غير مباشر وتؤكد على الضرورة القصوى للتعاون بين الشركات والمستخدمين لتعزيز الدفاعات الرقمية. في هذا السياق، يصبح تبني ممارسات الأمان الإلكتروني، مثل استخدام برمجيات الحماية المتطورة، الوعي بالتهديدات الشائعة، والتحقق الدقيق من المعلومات والخدمات عبر الإنترنت، ليس فقط خيارًا بل ضرورة للحفاظ على أمان الفرد وخصوصيته في هذا العالم الرقمي المتسارع.

المبحث الثاني

تحديات تطبيق قوانين حماية المستهلك الالكتروني

تطبيق قوانين حماية المستهلك الإلكتروني يواجه عدة تحديات معقدة تتطلب جهودًا مستمرة وتعاونًا على مختلف المستويات. هذه التحديات تشمل الجوانب الفنية، القانونية، والتنظيمية التي تؤثر على فعالية الإجراءات الحمائية للمستهلكين عبر الإنترنت([1]):

أولًا- التطور التكنولوجي المستمر:

التطور التكنولوجي المستمر يشكل تحديًا كبيرًا لصانعي السياسات والجهات التنفيذية في مجال الأمن الإلكتروني وحماية المستهلك. مع كل ابتكار جديد، تظهر فرص جديدة للمحتالين والمجرمين لاستغلال التكنولوجيا بطرق لم يتم التنبؤ بها سابقًا، مما يجعل من الصعب على القوانين الموجودة مواكبة هذه التغيرات. الجرائم الإلكترونية تتطور بسرعة أكبر من قدرة الأنظمة التشريعية على التكيف، مما يطرح عدة تحديات.

[1]) Bruce Schneier, op. cit., p. 80.

١- الحاجة إلى تشريعات مرنة ومتكيفة:

تحتاج الحكومات إلى تطوير تشريعات تكون كافية للتعامل مع التقنيات الجديدة والأساليب المبتكرة للجريمة الإلكترونية دون تقييد التقدم التكنولوجي. هذا يتطلب فهمًا عميقًا للتكنولوجيا وتأثيرها المحتمل على المجتمع.

٢- التدريب والتطوير المهني للسلطات:

لضمان فعالية التنفيذ، يجب على السلطات القضائية والتنفيذية تلقي تدريب مستمر على أحدث التقنيات وأساليب الجريمة الإلكترونية. هذا يشمل القضاة، المحامين، وأفراد إنفاذ القانون.

ثانيًا- الطبيعة العابرة للحدود للتجارة الإلكترونية:

تشكل تحديًا كبيرًا أمام المشرعين في جميع أنحاء العالم، نظرًا لصعوبة تطبيق القوانين الوطنية على معاملات تحدث عبر الإنترنت وتمتد عبر عدة دول. هذا التحدي يتطلب استجابة متعددة الجوانب تشمل التعاون الدولي، توحيد المعايير، وتطوير أطر قانونية مرنة قادرة على التكيف مع البيئة الرقمية المتغيرة([1]).

[1]) Michael Geist, Internet Law in a Nutshell, West Academic Publishing, 2017, p. 150.

١- التعاون الدولي:

التعاون بين الدول ضروري لمكافحة الجرائم الإلكترونية وحماية المستهلكين في سياق التجارة الإلكترونية. هذا يشمل تبادل المعلومات والخبرات، وتنفيذ الاتفاقيات الدولية التي تسهل التعاون القضائي وإنفاذ القوانين عبر الحدود.

٢- توحيد المعايير القانونية:

توحيد المعايير والتشريعات القانونية يمكن أن يساعد في خلق بيئة تجارية إلكترونية أكثر أمانًا وتنظيمًا. من خلال تحديد معايير دولية لحماية المستهلك والخصوصية وأمن البيانات، يمكن تسهيل التجارة الإلكترونية وتعزيز الثقة بين المستهلكين والشركات.

٣- تطوير أطر قانونية مرنة:

الأطر القانونية يجب أن تكون قادرة على التكيف مع التطورات التكنولوجية والتجارية المستمرة. هذا يتطلب من المشرعين تبني نهج مرن وشامل يأخذ بعين الاعتبار الابتكارات التكنولوجية ويحمي في نفس الوقت حقوق وأمان المستهلكين.

ومن الجدير بالذكر أن واحدة من أبرز التحديات هي مقاومة بعض الدول لتوحيد القوانين بسبب اختلافات في الثقافات القانونية والاقتصادية. الحل يكمن في تعزيز الحوار الدولي والعمل نحو تحقيق توافق في الآراء حول أهمية حماية المستهلك وتأمين التجارة الإلكترونية.

في نهاية المطاف، النجاح في مواجهة التحديات الناجمة عن الطبيعة العابرة للحدود للتجارة الإلكترونية يعتمد على القدرة على التعاون الدولي والابتكار في تطوير الأطر القانونية. بذلك، يمكن ضمان حماية فعالة للمستهلكين في البيئة الرقمية.

وهنا سؤال يطرح نفسه وهو: **كيف يمكن تحديد الاختصاص القضائي في جرائم المستهلك الالكتروني التي تتم عبر الحدود الدولية؟**

تحديد الاختصاص القضائي في جرائم المستهلك الإلكتروني التي تتم عبر الحدود الدولية يمثل تحديًا كبيرًا بسبب الطبيعة العابرة للحدود للإنترنت والتجارة الإلكترونية. هناك عدة معايير يمكن أن تستخدم لتحديد الاختصاص القضائي في مثل هذه الجرائم:

١. **مكان ارتكاب الجريمة:** يمكن اعتبار المكان الذي تم فيه ارتكاب الفعل الإجرامي كأساس لتحديد الاختصاص. في سياق الجرائم الإلكترونية، يمكن أن يشمل هذا

الموقع الفعلي للخوادم، مكان تسجيل الدومين، أو الموقع الجغرافي للضحية أو الجاني.

٢. **جنسية الجاني أو الضحية:** قد يستند الاختصاص أيضًا إلى جنسية الجاني أو الضحية. بعض الدول لديها مبدأ الاختصاص القضائي الوطني الذي يسمح لها بمحاكمة مواطنيها لجرائم ارتكبت خارج حدودها.

٣. **مبدأ الاختصاص العالمي:** في بعض الحالات، يمكن للدول ممارسة الاختصاص القضائي بناءً على مبدأ الاختصاص العالمي، خاصة في جرائم تعتبر خطيرة جدًا وذات تأثير دولي، مثل الإرهاب أو الاحتيال الإلكتروني الكبير.

٤. **مكان تقديم الخدمة أو المنتج:** في حالات التجارة الإلكترونية، قد يعتمد الاختصاص على المكان الذي يتم فيه تقديم الخدمات أو بيع المنتجات، مثلاً، حيث يقع المستهلكون أو يتلقون الخدمة.

٥. **الاتفاقيات الدولية والتعاون:** الاتفاقيات الدولية ومذكرات التفاهم بين الدول يمكن أن تلعب دورًا في تحديد الاختصاص من خلال توفير إطار للتعاون القضائي وتسليم المجرمين.

٦. **تطبيق قوانين حماية المستهلك:** في بعض الدول، يمكن تطبيق قوانين حماية المستهلك على الشركات الأجنبية التي تقدم خدمات أو منتجات لمواطنيها، مما يعطي الاختصاص القضائي للدولة للتحقيق والمحاكمة في حالات الانتهاك.

تحديد الاختصاص في جرائم المستهلك الإلكتروني التي تتم عبر الحدود يتطلب تحليلاً دقيقًا للظروف المحيطة بكل حالة والتعاون بين السلطات القضائية في الدول المعنية. هذا يتطلب مرونة في التفسير القانوني والاستعداد للتعاون الدولي لضمان العدالة وحماية المستهلكين بفعالية.

ثالثًا- الخصوصية وحماية البيانات:

إيجاد التوازن المناسب بين خصوصية البيانات وتمكين الابتكار والنمو في الاقتصاد الرقمي يمثل تحديًا كبيرًا للحكومات حول العالم. مع تزايد القلق بشأن خصوصية البيانات، تبرز الحاجة إلى تشريعات فعالة تحمي المعلومات الشخصية للمستهلكين دون إعاقة التقدم التكنولوجي والابتكار الذي يدفع الاقتصاد الرقمي. هذا التوازن يتطلب نهجًا متعدد الأبعاد يشمل([1]):

[1]) Daniel J. Solove, The Digital Person: Technology and Privacy in the Information Age, New York University Press, 2004, p 53.

١- تطوير تشريعات مرنة:

يجب أن تكون القوانين المتعلقة بخصوصية البيانات وحمايتها قادرة على التكيف مع التغيرات التكنولوجية السريعة. تشريعات مثل اللائحة العامة لحماية البيانات (GDPR) في الاتحاد الأوروبي توفر مثالًا على كيفية تنظيم حماية البيانات بطريقة تحافظ على حقوق الأفراد مع تمكين الابتكار.

٢- تعزيز الشفافية والموافقة:

يجب على الشركات أن تكون شفافة بشأن كيفية جمعها واستخدامها لبيانات المستهلكين وضمان حصولها على موافقة صريحة من المستخدمين قبل جمع بياناتهم الشخصية. هذا يعزز الثقة ويمنح المستهلكين سيطرة أكبر على معلوماتهم.

٣- تشجيع الابتكار في الخصوصية:

تشجيع الشركات على تبني "الخصوصية بالتصميم" و"الأمان بالتصميم"، مما يعني دمج معايير الخصوصية والأمان في مراحل التطوير المبكرة للمنتجات والخدمات الجديدة. هذا يساعد في تحقيق توازن بين حماية البيانات والابتكار.

وهنا سؤال يطرح نفسه وهو: **كيف يمكن للمستهلكين الإلكترونيين حماية خصوصيتهم وبياناتهم الشخصية في ظل الممارسات المتزايدة لجمع البيانات من قبل الشركات الكبرى؟**

لحماية خصوصيتهم وبياناتهم الشخصية في ظل الممارسات المتزايدة لجمع البيانات من قبل الشركات الكبرى، يمكن للمستهلكين الإلكترونيين اتخاذ عدة خطوات استباقية:

١. **التحقق من إعدادات الخصوصية:** يجب على المستخدمين مراجعة إعدادات الخصوصية بانتظام على منصات الويب والتطبيقات التي يستخدمونها وضبطها لتقليل كمية البيانات التي يشاركونها. الكثير من الشركات توفر خيارات مفصلة للخصوصية تسمح بتحديد من يمكنه رؤية بياناتك وكيف يمكن استخدامها.

٢. **قراءة سياسات الخصوصية:** على الرغم من أنها قد تكون طويلة ومعقدة، يجب على المستهلكين الاطلاع على سياسات الخصوصية للمواقع والخدمات الإلكترونية لفهم كيفية جمع بياناتهم واستخدامها ومشاركتها.

٣. **استخدام تقنيات الحماية:** استخدام أدوات مثل VPNs (شبكات خاصة افتراضية) لتشفير البيانات أثناء الإرسال، وبرامج مكافحة الفيروسات وأدوات مكافحة التتبع لمنع الوصول غير المصرح به إلى البيانات.

٤. **إدارة كلمات المرور**: استخدام كلمات مرور قوية وفريدة لكل حساب والاستفادة من خدمات إدارة كلمات المرور لتخزينها بأمان. كما يُنصح بتفعيل المصادقة الثنائية (FA٢) عندما تكون متاحة.

٥. **تقليل المشاركة الرقمية:** تجنب مشاركة المعلومات الشخصية غير الضرورية على الإنترنت، بما في ذلك مواقع التواصل الاجتماعي، وكن حذرًا عند ملء النماذج عبر الإنترنت.

٦. **التحديثات الأمنية:** الحفاظ على تحديث البرمجيات، بما في ذلك نظام التشغيل والتطبيقات، لضمان حصولك على أحدث التصحيحات الأمنية.

٧. **استخدام البريد الإلكتروني بحذر**: كن حذرًا من الرسائل التي تطلب معلومات شخصية (phishing) وتجنب النقر على الروابط المشبوهة أو تنزيل المرفقات من رسائل بريد إلكتروني غير معروفة المصدر.

٨. **تعلم حقوقك:** تعرف على حقوقك المتعلقة بالخصوصية وحماية البيانات وفقًا للقانون في بلدك أو المنطقة التي تعيش فيها. في حالة الشكوى، يجب أن تعرف كيف وأين تقدمها.

من خلال اتخاذ هذه الخطوات، يمكن للمستهلكين الإلكترونيين تعزيز حماية خصوصيتهم وبياناتهم الشخصية وتقليل المخاطر المرتبطة بجمع البيانات واستغلالها من قبل الشركات الكبرى.

وننتقل لسؤال اخر وهو: **ما هي الحدود بين جمع البيانات لتحسين الخدمات وانتهاك خصوصية المستهلك؟**

الحدود بين جمع البيانات لتحسين الخدمات وانتهاك خصوصية المستهلك تتطلب توازنًا دقيقًا بين مصالح الشركات في توفير تجربة مستخدم مخصصة وفعالة وبين حقوق الأفراد في الخصوصية والسيطرة على بياناتهم الشخصية. هناك عدة عوامل تحدد هذه الحدود([1]):

١. **الشفافية والموافقة:** الشفافية حول كيفية جمع البيانات، ما هي البيانات التي يتم جمعها، وكيفية استخدامها أمر ضروري. يجب على الشركات الحصول على موافقة صريحة من المستهلكين قبل جمع بياناتهم واستخدامها، خاصة للبيانات الحساسة.

[1]) Da Veiga, A., Ochola, E., Mujinga, M., Mwim, E. Investigating Data Privacy Evaluation Criteria and Requirements for e-Commerce Websites. In: Guarda, T., Portela, F., Augusto, M.F. (eds) Advanced Research in Technologies, Information, Innovation and Sustainability. ARTIIS 2022. Communications in Computer and Information Science, vol 1676. Springer, Cham, 2022, p 302.

٢. **الحد الأدنى من جمع البيانات:** يجب على الشركات جمع البيانات التي هي ضرورية فقط لتحقيق الأهداف المحددة مسبقًا والتي تم إعلام المستهلكين بها. جمع بيانات أكثر مما هو ضروري يمكن أن يُعتبر انتهاكًا للخصوصية.

٣. **الأمان:** يجب حماية البيانات التي تم جمعها بمعايير أمان عالية لمنع الوصول غير المصرح به والاستخدام غير اللائق، وهو ما يساعد في الحفاظ على خصوصية المستهلك.

٤. **الغرض من جمع البيانات:** يجب استخدام البيانات للغرض الذي تم جمعها من أجله والمعلن عنه. استخدام البيانات لأغراض أخرى دون موافقة جديدة يمكن أن يُعتبر انتهاكًا للخصوصية.

٥. **الحق في الوصول والتصحيح:** يجب أن يكون للمستهلكين الحق في الوصول إلى بياناتهم الشخصية التي تحتفظ بها الشركات وتصحيحها إذا كانت غير دقيقة أو قديمة.

٦. **الحق في النسيان:** يجب على الشركات توفير آلية للمستهلكين لطلب حذف بياناتهم الشخصية من النظم الأساسية عندما لا تكون هناك حاجة لها للغرض الذي تم جمعها من أجله.

٧. **الامتثال للقوانين واللوائح:** يجب على الشركات الامتثال للقوانين واللوائح المحلية والدولية المتعلقة بحماية البيانات وخصوصية المستهلك، مثل GDPR في الاتحاد الأوروبي.

التحدي في تحديد هذه الحدود يكمن في الموازنة بين الاستفادة من البيانات لتحسين الخدمات والمنتجات وبين ضمان عدم تجاوز الحدود التي تؤدي إلى انتهاك خصوصية المستهلكين. الامتثال للمبادئ المذكورة أعلاه يساعد الشركات في المحافظة على ثقة المستهلكين وتعزيز سمعتها في السوق.

رابعًا- التنفيذ والإنفاذ:

التنفيذ والإنفاذ الفعّال للتشريعات القانونية المتعلقة بالحماية الجنائية وحماية المستهلك الإلكتروني يمثلان تحديًا كبيرًا في السوق الرقمي الواسع والمعقد. تواجه الجهات التنفيذية عقبات جمّة في مواكبة السرعة التي تتطور بها التكنولوجيا والممارسات التجارية عبر الإنترنت، بالإضافة إلى التحديات الناجمة عن الطبيعة العابرة للحدود لهذه الجرائم. لمواجهة هذه التحديات، يتطلب الأمر استراتيجيات متعددة الأوجه حيث

تحتاج الجهات التنفيذية إلى استثمارات كبيرة في التكنولوجيا والأدوات اللازمة لرصد وتحليل النشاط الإلكتروني بفعالية، وذلك لتحديد ومتابعة الانتهاكات بسرعة([1]).

وهنا سؤال يطرح نفسه وهو: **ما دور الأجهزة الرقابية والتنظيمية في حماية المستهلك الإلكتروني وما هي التحديات التي تواجهها؟**

الأجهزة الرقابية والتنظيمية تلعب دورًا حيويًا في حماية المستهلك الإلكتروني من خلال وضع وتنفيذ القوانين واللوائح التي تضمن الشفافية، الأمان، والعدالة في البيئة الإلكترونية. دورها يشمل عدة جوانب رئيسية:

دور الأجهزة الرقابية والتنظيمية:

١. **وضع التشريعات والمعايير:** تطوير وتحديث القوانين والمعايير الخاصة بالتجارة الإلكترونية وحماية البيانات لضمان أن تكون الممارسات التجارية عادلة وشفافة.

٢. **الرقابة والتفتيش:** إجراء التفتيش والمراقبة للتأكد من امتثال الشركات والمنصات الإلكترونية للقوانين واللوائح، والتحقق من مستويات الأمان وحماية البيانات.

٣. **التوعية والتعليم:** تنظيم حملات توعوية للمستهلكين حول حقوقهم في البيئة الإلكترونية وكيفية حماية أنفسهم من الاحتيال والممارسات الضارة.

[1]) John Doe, "Digital Law Enforcement: Challenges and Strategies in the Cyber Age," Cambridge University Press, 2020, p. 157.

٤. **تلقي الشكاوى والتحقيق فيها:** توفير آليات فعالة للمستهلكين لتقديم الشكاوى بخصوص الممارسات غير العادلة أو الاحتيالية والتحقيق في هذه الشكاوى.

٥. **التعاون الدولي:** العمل مع الهيئات التنظيمية الدولية لتحسين الأمان الإلكتروني وحماية المستهلكين عبر الحدود من خلال تبادل المعلومات وأفضل الممارسات.

التحديات التي تواجهها:

١. **التطور التكنولوجي السريع:** التكنولوجيا تتطور بوتيرة أسرع من قدرة الهيئات التنظيمية على تحديث القوانين واللوائح، مما يخلق فجوات قانونية.

٢. **الطبيعة العالمية للإنترنت:** الجرائم الإلكترونية والممارسات التجارية الضارة قد تنطوي على أطراف في دول متعددة، مما يجعل التنظيم والإنفاذ صعبًا.

٣. **الوعي والتعليم:** قد يكون هناك نقص في الوعي بين المستهلكين حول حقوقهم وكيفية حماية أنفسهم، مما يستلزم جهودًا متواصلة للتوعية.

٤. **الموارد المحدودة:** قد تفتقر الهيئات التنظيمية إلى الموارد اللازمة للرقابة والتحقيق والإنفاذ بشكل فعال، خاصة في مواجهة شركات كبيرة وقوية.

٥. **تحديات الخصوصية وحماية البيانات:** موازنة الحاجة إلى جمع البيانات للأغراض التنظيمية والإنفاذية مع ضمان حماية خصوصية المستهلكين وبياناتهم.

للتغلب على هذه التحديات، تحتاج الأجهزة الرقابية والتنظيمية إلى استخدام أدوات واستراتيجيات مبتكرة، تعزيز التعاون الدولي، وزيادة الاستثمار في التكنولوجيا والتدريب لتحسين حماية المستهلك الإلكتروني بشكل فعال.

المبحث الثالث

تأثير التكنولوجيا والتطورات الرقمية على الحماية الجنائية للمستهلك

تؤثر التطورات التكنولوجية والرقمية بشكل كبير على الحماية الجنائية للمستهلك، مما يطرح تحديات جديدة ويوفر في الوقت نفسه فرصًا لتعزيز هذه الحماية. هذا التأثير يمكن أن يُرى من خلال عدة جوانب:

أولا- التحديات الناتجة عن التطورات التكنولوجية والرقمية:

أ) **انتشار الجرائم الالكترونية:**

التطورات التكنولوجية السريعة، بينما توفر فرصًا هائلة للابتكار والتواصل، قد أتاحت أيضًا الفرصة لظهور أنواع جديدة من الجرائم الإلكترونية التي تستهدف المستهلكين بطرق معقدة ومتطورة. الاحتيال الإلكتروني، سرقة الهوية، والتصيد الاحتيالي هي مجرد بعض الأمثلة على هذه الجرائم التي تنتهك خصوصية الأفراد وتهدد أمانهم المالي. مع تزايد استخدام الإنترنت في الأنشطة اليومية، من التسوق إلى البنوك الإلكترونية، أصبح المستهلكون

أكثر عرضة لهذه الأنواع من الهجمات، مما يدعو إلى ضرورة تعزيز الوعي والحماية القانونية للتصدي لهذه التحديات([1]).

في مواجهة هذه التحديات، تبرز الحاجة الملحة لاستجابة قانونية محددة ومتخصصة تتكيف مع الطبيعة المتغيرة للجريمة الإلكترونية. الأطر القانونية الحالية قد تحتاج إلى التحديث لتشمل تعريفات واضحة للجرائم الرقمية وتفرض عقوبات رادعة للمخالفين. كما يتطلب الأمر تعزيز التعاون الدولي والمحلي بين الوكالات الإنفاذية، المؤسسات المالية، ومقدمي خدمات الإنترنت لتبادل المعلومات وأفضل الممارسات في مكافحة الجرائم الإلكترونية. فقط من خلال مثل هذه الجهود المنسقة يمكن حماية المستهلكين بفعالية من الأخطار المتزايدة للجريمة الإلكترونية في عالم متزايد الرقمنة.

ما هو دور المنصات الإلكترونية في حماية المستهلكين، وكيف يمكن محاسبتها في حال فشلها في ذلك؟

المنصات الإلكترونية تلعب دورًا محوريًا في حماية المستهلكين في البيئة الرقمية، وذلك من خلال توفير بيئة تسوق آمنة وشفافة ومنصفة. دورها يشمل عدة جوانب رئيسية([1]):

[1]) Jane Smith, "Cybersecurity and Consumer Protection: Emerging Threats in the Digital Age," Oxford University Press, 2021, p. 112.

دور المنصات الإلكترونية في حماية المستهلكين:

١. **الأمان السيبراني:** توفير بروتوكولات أمان قوية لحماية بيانات المستهلكين من السرقة أو الاختراق.

٢. **الشفافية:** تقديم معلومات دقيقة وشفافة حول المنتجات والخدمات، بما في ذلك الأسعار، المواصفات، وسياسات الإرجاع.

٣. **الخصوصية:** حماية خصوصية المستهلكين من خلال تطبيق سياسات خصوصية واضحة والحصول على الموافقة قبل جمع أو مشاركة البيانات.

٤. **التوعية:** توعية المستهلكين حول مخاطر الاحتيال الإلكتروني وتقديم إرشادات حول كيفية التسوق بأمان عبر الإنترنت.

٥. **المراقبة والإنفاذ:** مراقبة المنصة للكشف عن الممارسات الضارة أو الاحتيالية واتخاذ إجراءات سريعة للتعامل معها.

[1]) Tanaka, S. (2020). Digital Platformers' Responsibilities to Platform Users; 'Consumer Protection' in B2C and C2C e-Commerce. In: Wei, D., Nehf, J.P., Marques, C.L. (eds) Innovation and the Transformation of Consumer Law. Springer, Singapore, p 48.

محاسبة المنصات في حال فشلها في حماية المستهلكين:

١. **الإجراءات القانونية:** يمكن للمستهلكين والهيئات التنظيمية اتخاذ إجراءات قانونية ضد المنصات الإلكترونية التي تفشل في حماية المستهلكين، بما في ذلك المطالبة بالتعويضات.

٢. **الغرامات والعقوبات:** الهيئات التنظيمية يمكن أن تفرض غرامات وعقوبات على المنصات الإلكترونية التي تخالف قوانين حماية المستهلك وخصوصية البيانات.

٣. **الضغط العام والسمعة:** الضغط العام والتأثير السلبي على سمعة المنصة يمكن أن يكون له تأثير قوي في دفعها لتحسين ممارساتها الأمنية وحماية المستهلك.

٤. **المقاطعة:** المستهلكون يمكن أن يقاطعوا المنصات التي لا تحمي خصوصيتهم أو تسمح بممارسات ضارة، مما يؤثر على أعمالها.

ب) الخصوصية وحماية البيانات:

في عصر الرقمنة الشامل، أصبحت البيانات الشخصية عملة ذات قيمة عالية، حيث تمكّن الشركات من جمع وتحليل كميات هائلة من المعلومات حول المستهلكين. هذه القدرة على التجميع والتحليل ليست بلا مخاطر؛ فهي تطرح تحديات كبيرة تتعلق بخصوصية المستهلك وأمان البيانات. من خلال

تعقب السلوكيات عبر الإنترنت، التفضيلات الشخصية، وحتى المواقع الجغرافية، يمكن للشركات بناء صورة دقيقة جدًا عن المستهلكين، مما يثير مخاوف جدية بشأن الحق في الخصوصية والسيطرة على المعلومات الشخصية([1]).

استجابةً لهذه المخاوف، تُطوّر الحكومات والهيئات التنظيمية حول العالم قوانين وتشريعات لحماية بيانات المستهلكين، مثل اللائحة العامة لحماية البيانات (GDPR) في الاتحاد الأوروبي، التي تمثل معيارًا ذهبيًا في مجال الخصوصية وحماية البيانات. تسعى هذه التشريعات إلى منح المستهلكين سيطرة أكبر على بياناتهم الشخصية، مطالبة الشركات بالشفافية حول كيفية جمع البيانات، استخدامها، ومشاركتها، وتوفير وسائل للمستهلكين للموافقة على جمع بياناتهم وحتى طلب حذفها. ومع ذلك، تظل مواكبة التطورات التكنولوجية المستمرة تحديًا دائمًا، مما يتطلب جهودًا مستمرة لضمان خصوصية المستهلك وأمان البيانات في العالم الرقمي.

[1]) Padilla, J., Piccolo, S. & Vasconcelos, H. Business models, consumer data and privacy in platform markets. J. Ind. Bus. Econ.49, 2022, p 600.

ت) تحديث القوانين:

مع السرعة الهائلة للتطورات التكنولوجية، يبرز تحدي كبير أمام المشرعين والهيئات التنظيمية في مواكبة هذه التغيرات لضمان حماية المستهلكين بشكل فعال. التكنولوجيا تغير بسرعة الطريقة التي نتعامل بها مع المعلومات، نتواصل، ونجري المعاملات التجارية، مما يخلق فجوات قانونية يمكن أن تستغلها الأنشطة الضارة والاحتيالية. لذلك، هناك حاجة ماسة لتحديث القوانين والأنظمة بشكل دوري لتعكس هذه التغيرات وتوفر الإطار اللازم لحماية الحقوق الأساسية للمستهلكين، بما في ذلك الخصوصية، الأمان، والعدالة في المعاملات الإلكترونية([1]).

تحديث التشريعات يتطلب نهجًا متوازنًا يحافظ على الابتكار والنمو الاقتصادي مع ضمان حماية المستهلكين من المخاطر الجديدة. يجب أن تكون القوانين مرنة بما يكفي لاحتضان التقنيات الجديدة دون قمعها، وفي الوقت نفسه صارمة بما يكفي لردع الاستغلال والأنشطة الضارة. هذا يتطلب تعاونًا وثيقًا بين الحكومات، الصناعات التكنولوجية، المنظمات المدنية، والمجتمعات الأكاديمية لضمان أن تكون التشريعات الجديدة شاملة، مستنيرة،

[1]) John Doe, "Legislative Challenges in the Digital Era: Protecting Consumer Rights," Cambridge University Press, 2022, p. 95.

وقابلة للتنفيذ. فقط من خلال هذا التعاون المستمر والنظرة المستقبلية يمكن للمجتمعات الحفاظ على الخطوة مع التغيرات التكنولوجية وحماية مواطنيها في بيئة رقمية متطورة.

وهنا سؤال يطرح نفسه متعلق بـ: **كيف يمكن تحديد المسؤولية في حالات الاحتيال الإلكتروني، خاصة عندما تكون هناك سلاسل إمداد معقدة أو عند استخدام الذكاء الاصطناعي والتكنولوجيا المتقدمة؟**

تحديد المسؤولية في حالات الاحتيال الإلكتروني، خاصة تلك التي تتضمن سلاسل إمداد معقدة أو استخدام الذكاء الاصطناعي والتكنولوجيا المتقدمة، يمثل تحديًا كبيرًا نظرًا للطبيعة المعقدة والمتداخلة للعمليات والأطراف المعنية. ومع ذلك، يمكن اتباع عدة نهج لتحديد المسؤولية:

١. **تحليل العقود والاتفاقيات:** يجب فحص العقود والاتفاقيات بين جميع الأطراف المعنية لتحديد الالتزامات والمسؤوليات المتعلقة بالأمان الإلكتروني وحماية البيانات. هذا يشمل فهم كيفية توزيع المسؤولية في حالة الاحتيال أو الخرق الأمني.

٢. **تقييم الإجراءات الأمنية:** يجب تقييم الإجراءات الأمنية المتخذة من قبل جميع الأطراف لحماية البيانات ومنع الاحتيال. الفشل في تطبيق معايير الأمان المناسبة يمكن أن يكون أساسًا لتحديد المسؤولية.

٣. **التحقيق في سلسلة الأحداث:** يتطلب تحديد المسؤولية التحقيق في سلسلة الأحداث التي أدت إلى الاحتيال، بما في ذلك تحليل البيانات الرقمية وسجلات الوصول لتحديد نقاط الضعف وكيف تم استغلالها.

٤. **دور الذكاء الاصطناعي والتكنولوجيا المتقدمة:** عندما تكون التكنولوجيا المتقدمة جزءًا من العملية، يجب تقييم مدى مسؤولية مطوري ومزودي هذه التكنولوجيا عن الاحتيال. هذا يشمل تحليل إذا ما كانت الأنظمة قد صممت واختبرت بشكل يمنع الاستخدام الاحتيالي.

٥. **التشريعات واللوائح:** يجب مراجعة التشريعات واللوائح المحلية والدولية لفهم كيفية تنظيم المسؤولية في حالات الاحتيال الإلكتروني. بعض القوانين قد تفرض مسؤولية صارمة على بعض الأطراف دون الحاجة إلى إثبات الإهمال.

٦. **التعاون مع السلطات:** في كثير من الحالات، قد يكون التعاون مع السلطات القضائية والتنظيمية ضروريًا لتحديد المسؤولية بدقة، خاصة في حالات الاحتيال العابر للحدود.

التحديات:

- تحديد الأطراف المسؤولة: في سلاسل الإمداد المعقدة أو عند استخدام تكنولوجيا متطورة، قد يكون من الصعب تحديد من هو المسؤول بالضبط عن الخرق أو الاحتيال.
- التحديات التقنية: فهم كيفية تفاعل التكنولوجيات المختلفة وتحديد الثغرات التي تم استغلالها يتطلب خبرة تقنية عالية.
- التشريعات المتغيرة: التغيرات السريعة في التكنولوجيا تتطلب تحديثات مستمرة للتشريعات واللوائح، مما يشكل تحديًا للحفاظ على الحماية القانونية مواكبة لهذه التطورات.

المفتاح لتحديد المسؤولية بفعالية يكمن في الشفافية، التعاون بين الأطراف المختلفة، وتطبيق معايير الأمان القوية عبر جميع مراحل سلاسل الإمداد وتطوير التكنولوجيا.

ثانيا– فرص تعزيز الحماية باستخدام التطورات التكنولوجية والرقمية:

أ) أدوات جديدة للإنفاذ:

مع تطور التكنولوجيا، تتاح للسلطات التنظيمية والرقابية أدوات جديدة ومتقدمة تمكنها من مراقبة السوق بكفاءة أعلى وتحليل البيانات بسرعة ودقة غير مسبوقة. استخدام الذكاء الاصطناعي، تعلم الآلة، وتحليل البيانات الضخمة يسمح بتفحص المعاملات والسلوكيات في الوقت الفعلي، مما يعزز قدرة الهيئات على تحديد الأنماط غير الطبيعية والشاذة التي قد تشير إلى نشاطات احتيالية. هذه الأدوات لا تساعد فقط في رصد المخالفات بل توفر أيضاً القدرة على التنبؤ بالمخاطر المحتملة والتحرك بشكل استباقي لحماية المستهلكين والحفاظ على نزاهة السوق([1]).

بالإضافة إلى ذلك، تسهم هذه التكنولوجيات في تعزيز الشفافية والمساءلة في الأسواق المالية والتجارية. من خلال استخدام البلوك تشين وغيرها من تقنيات التشفير المتقدمة، يمكن للسلطات تأمين البيانات وضمان سلامتها، مما يقلل من فرص التلاعب والغش. هذه الأدوات الجديدة للإنفاذ تمكن الهيئات من

[1]) Jane Smith, "Innovative Enforcement: Leveraging Technology for Consumer Protection," Oxford University Press, 2021, p. 112.

التصدي للتحديات المعقدة في البيئة الرقمية الحديثة بطريقة أكثر فعالية، موفرةً بذلك بيئة أكثر أمانًا وعدالة للمستهلكين والمشاركين في السوق.

ب) توعية المستهلك:

في العصر الرقمي، أصبحت توعية المستهلكين حول حقوقهم وكيفية حماية أنفسهم من الجرائم الإلكترونية أكثر أهمية من أي وقت مضى. الأدوات الرقمية توفر للجهات الحكومية والمنظمات غير الحكومية منصات قوية لنشر المعلومات الضرورية والموارد التعليمية بطريقة فعالة وواسعة الانتشار. من خلال استخدام مواقع الويب، الوسائط الاجتماعية، تطبيقات الهاتف المحمول، والندوات الإلكترونية، يمكن لهذه الجهات توصيل رسائلها بشكل مباشر وتفاعلي إلى جمهور واسع، مما يسهم في رفع مستوى الوعي حول الممارسات الآمنة عبر الإنترنت والحقوق القانونية للمستهلكين([1]).

بالإضافة إلى ذلك، تسمح هذه الأدوات بتخصيص المحتوى التعليمي والتوعوي ليناسب احتياجات وتفضيلات جماهير مختلفة، من الشباب إلى كبار السن، مما يضمن فعالية أكبر في التواصل والتأثير. عبر استخدام

[1]) Anh, N.V. Corporate Social Responsibility: Protecting Consumer Rights in E-commerce. In: An, N.B., Anh, P.T. (eds) Laws on Corporate Social Responsibility and the Developmental Trend in Vietnam. Springer, Singapore, 2023, p 188.

الفيديوهات التوضيحية، الإنفو جرافيكس، والمحاكاة، يمكن تقديم المعلومات بطريقة مبسطة وجذابة تعزز الفهم والاستيعاب. هذه الجهود المتكاملة في التوعية تلعب دورًا حاسمًا في تمكين المستهلكين من الدفاع عن أنفسهم ضد المخاطر الإلكترونية، مساهمةً في خلق بيئة رقمية أكثر أمانًا للجميع.

ت) العقود الذكية والبلوك تشين:

تكنولوجيا البلوك تشين والعقود الذكية تمثل ثورة في كيفية إجراء المعاملات الإلكترونية وإدارة العقود في العالم الرقمي. من خلال توفير بنية تحتية غير مركزية وموزعة، تسمح تكنولوجيا البلوك تشين بتسجيل المعاملات بطريقة شفافة وغير قابلة للتغيير، مما يقلل من مخاطر الاحتيال والتلاعب. العقود الذكية، التي تعتمد على هذه التكنولوجيا، تمكّن من تنفيذ الاتفاقيات تلقائيًا عند استيفاء شروط محددة مسبقًا، دون الحاجة إلى وسطاء، مما يعزز الكفاءة ويقلل من تكاليف المعاملات. هذا يوفر طبقة إضافية من الأمان والثقة

للمستهلكين، حيث تضمن التكنولوجيا تنفيذ العقود بدقة وفقًا للشروط المتفق عليها([1]).

بالإضافة إلى ذلك، تعمل الشفافية الكبيرة التي توفرها تكنولوجيا البلوك تشين على تعزيز حماية المستهلك من خلال تمكينه من التحقق من صحة المعاملات وتفاصيل العقود بنفسه. هذا لا يساهم فقط في خلق بيئة تجارية أكثر أمانًا ولكن يساعد أيضًا في بناء الثقة بين الأطراف المختلفة. إن تطبيق العقود الذكية والبلوك تشين في المعاملات الإلكترونية يشير إلى مستقبل يمكن فيه للمستهلكين التمتع بمستويات عالية من الأمان، الشفافية، والكفاءة، مما يعكس تحولًا جوهريًا نحو تعزيز حقوق وحماية المستهلك في العصر الرقمي.

ث) المدفوعات الإلكترونية:

التطورات في تكنولوجيا المدفوعات الإلكترونية تعد بتحويل جذري في كيفية إجراء المستهلكين للمعاملات المالية عبر الإنترنت، مما يوفر لهم خيارات

[1]) Tsyganov, V.I., Demin, A.A., Osadchenko, E.O. Obligations in the Field of E-Commerce. In: Inshakova, A., Inshakova, E. (eds) Competitive Russia: Foresight Model of Economic and Legal Development in the Digital Age. CRFMELD 2019. Lecture Notes in Networks and Systems, vol 110. Springer, Cham, 2020, p 588.

دفع أكثر أمانًا وسهولة. مع ظهور أنظمة المدفوعات الرقمية المتطورة والعملات المشفرة، يتم الآن تشفير المعلومات المالية بطرق تضمن حماية بيانات المستهلكين من الاختراقات والسرقة الإلكترونية. هذه التطورات تساعد في تقليل المخاطر المرتبطة بالمدفوعات عبر الإنترنت، مثل الاحتيال ببطاقات الائتمان والاختلاس، مما يعزز ثقة المستهلك في التجارة الإلكترونية. بالإضافة إلى ذلك، تسمح التقنيات الجديدة مثل المحافظ الرقمية ونقاط البيع الافتراضية للمستهلكين بإجراء معاملات سريعة ومريحة، مما يحسن تجربة الشراء الإلكتروني ويدعم نمو الاقتصاد الرقمي([1]).

في النهاية، هذه التطورات التكنولوجية في مجال المدفوعات الإلكترونية لا توفر فقط طرق دفع أكثر سلاسة وكفاءة للمستهلكين، بل تسهم أيضًا في تعزيز الأمان العام للنظام المالي الرقمي. من خلال تبني معايير أمان عالية والاستفادة من التكنولوجيا المتقدمة، يمكن للمؤسسات المالية والشركات توفير بيئة تجارية أكثر أمانًا تحمي المستهلكين من المخاطر المالية، مما يسهم في بناء مجتمع رقمي أكثر ثقة واستدامة.

[1]) John Doe, "The Future of Electronic Payments: Security and Innovation," Cambridge University Press, 2022, p. 95.

الخاتمة

في عصر تتزايد فيه التعقيدات الرقمية وتتشابك فيه الأنشطة الإلكترونية مع جوانب حياتنا اليومية، تبرز الحاجة الماسة إلى تعزيز الحماية الجنائية للمستهلك الإلكتروني كركيزة أساسية للأمان والثقة في الفضاء الرقمي. تحقيقاً لهذه الغاية، يجب على الجهات التشريعية والتنفيذية العمل يدًا بيد لصياغة وتطبيق قوانين شاملة ومرنة تواكب التطورات التكنولوجية السريعة وتلبي احتياجات الحماية للمستهلكين. إن تحسين الوعي العام بالحقوق الرقمية وتوفير الأدوات اللازمة للدفاع عن هذه الحقوق يعدان خطوات حاسمة نحو بناء مجتمع رقمي آمن.

من جهة أخرى، تلعب التكنولوجيا دورًا مزدوجًا في مسألة الحماية الجنائية للمستهلك الإلكتروني، حيث توفر في الوقت نفسه الوسائل التي يمكن من خلالها ارتكاب الجرائم والأدوات اللازمة لمكافحتها. يتطلب هذا من الجهات المعنية استثمارًا كبيرًا في الأمن السيبراني وتطوير القدرات الفنية للكشف عن الجرائم الإلكترونية ومكافحتها بفعالية. إن الاستفادة من الذكاء الاصطناعي وتقنيات التعلم الآلي لتحليل البيانات وتحديد الأنماط الاحتيالية يمكن أن يساهم بشكل كبير في تعزيز الحماية الجنائية للمستهلكين على الإنترنت.

وأخيرًا، يتوجب على الهيئات الدولية والإقليمية تعزيز التعاون وتبادل المعلومات لمواجهة التحديات التي تفرضها الجرائم الإلكترونية التي لا تعترف بالحدود الجغرافية. العمل المشترك لتطوير معايير دولية لحماية البيانات ومكافحة الاحتيال الإلكتروني سيعزز من فعالية الجهود الوطنية ويضمن مستوى متسقًا من الحماية للمستهلكين في جميع أنحاء العالم. إن الحماية الجنائية للمستهلك الإلكتروني ليست مسؤولية واحدة بل تتطلب جهدًا جماعيًا يشمل المشرعين، المنفذين، الشركات التكنولوجية، والمستهلكين أنفسهم لضمان بيئة رقمية آمنة وعادلة للجميع.

النتائج:

١. تظل معضلة حماية المستهلك الإلكتروني ليست في غياب النصوص الجنائية لحمايته، بل تكمن المشكلة في ضعف الأجهزة الرقابية المسئولة عن الحماية، وتباطؤ الاستجابة لشكاواه من قبل الجهات المعنية.

٢. يشير المستهلك الإلكتروني إلى أي فرد يقوم بشراء السلع أو الخدمات عبر الإنترنت، ويستفيد هؤلاء المستهلكين من التكنولوجيا الرقمية لتسهيل عملية الشراء، مما يتيح لهم الوصول إلى مجموعة واسعة من المنتجات والخدمات عبر الإنترنت بدلاً من الاعتماد على الطرق التقليدية مثل المتاجر الفعلية.

٣. الوصول إلى المعلومات هو أحد الأعمدة الرئيسية التي تدعم سلوك المستهلك الإلكتروني في العصر الرقمي. المستهلكون اليوم لديهم القدرة على البحث وجمع المعلومات حول مختلف المنتجات والخدمات بسهولة ويسر عبر الإنترنت.

٤. الأمان والخصوصية يمثلان محور اهتمام رئيسي للمستهلكين الإلكترونيين في ظل الزيادة المستمرة في التجارة الإلكترونية، فالمستهلكون اليوم يواجهون مخاطر متعددة تشمل الاحتيال الإلكتروني، سرقة الهوية، والوصول غير المصرح به إلى البيانات الشخصية والمالية.

٥. تُعد الحماية الجنائية للمستهلك الإلكتروني قضية متزايدة الأهمية في عصرنا الحالي، فخصوصية تلك الحماية تختلف – بشكل كبير – بالنسبة للمستهلك الإلكتروني عن المستهلك التقليدي بعدة جوانب أساسية.

٦. التجارة الإلكترونية غيرت وجه الأعمال التجارية بشكل جذري، فبفضل الإنترنت، أصبحت العمليات التجارية أسرع وأكثر كفاءة من أي وقت مضى. هذه السرعة واللحظية تعني أن المستهلكين يمكنهم تصفح المنتجات، اتخاذ قرارات الشراء، وإكمال المعاملات المالية في غضون دقائق، إن لم يكن ثوانٍ. ونظرًا للطبيعة السريعة واللحظية للجرائم الإلكترونية، تواجه السلطات الجنائية تحديات كبيرة في توفير الحماية الكافية للمستهلكين.

٧. التشريعات والأنظمة المحدثة تلعب دوراً محورياً في تعزيز الأمان الإلكتروني وحماية المستهلكين على الإنترنت. من خلال إنشاء إطار قانوني صارم يحدد العقوبات على الجرائم الإلكترونية، يمكن للدول أن تردع المجرمين وتوفر آليات للتحقيق والملاحقة القانونية لهذه الأفعال.

٨. تبنت العديد من الدول تشريعات وأنظمة محدثة تركز على حماية البيانات الشخصية والخصوصية. قوانين مثل اللائحة العامة لحماية البيانات (GDPR) في الاتحاد الأوروبي وقوانين حماية البيانات في مناطق أخرى من العالم تعد خطوات هامة نحو تعزيز الحق في الخصوصية. هذه التشريعات تفرض على الشركات والمؤسسات ضوابط صارمة بشأن جمع، استخدام، ومشاركة البيانات الشخصية، مع توفير آليات للمستهلكين للسيطرة على معلوماتهم الشخصية.

٩. الوقاية والردع تمثلان ركيزتين أساسيتين في استراتيجية الحماية الجنائية للمستهلك الإلكتروني، حيث يُعد الهدف الرئيسي منهما هو منع وقوع الجرائم الإلكترونية قبل حدوثها. من خلال تطوير وتطبيق تشريعات وأنظمة قانونية رادعة، تسعى الحكومات والمؤسسات التنظيمية إلى إنشاء بيئة تجارية إلكترونية آمنة.

٢- الحماية الجنائية للمستهلك الإلكتروني

١٠. حماية المستهلك الإلكتروني في التشريعات العربية شهدت تطورًا ملحوظًا في السنوات الأخيرة، حيث بدأت العديد من الدول العربية بتحديث قوانينها وإدخال تشريعات جديدة لمواكبة التحديات التي فرضتها الثورة الرقمية والتجارة الإلكترونية.

١١. الحماية الجنائية للمستهلك الإلكتروني في القوانين المصرية تأتي ضمن إطار قانوني يشمل قوانين حماية المستهلك والقوانين المتعلقة بالتجارة الإلكترونية والجرائم الإلكترونية. هذه القوانين تهدف إلى حماية المستهلكين من الممارسات غير العادلة أو الاحتيالية وضمان أمان المعاملات الإلكترونية.

١٢. قوانين حماية المستهلك في مصر، الإمارات، والسعودية تشترك في الهدف الأساسي المتمثل في حماية حقوق المستهلكين، وتعزيز الثقة والأمان في التجارة الإلكترونية والمعاملات التجارية بشكل عام. ومع ذلك، توجد بعض الاختلافات في التفاصيل القانونية وآليات التنفيذ بين هذه الدول.

١٣. حماية المستهلك الإلكتروني في التشريعات الأجنبية تعد مجالًا ديناميكيًا ومتطورًا بشكل مستمر، مع توجه الدول حول العالم لتعزيز القوانين والسياسات التي تحمي المستهلكين في البيئة الرقمية. تختلف النهج والتشريعات من دولة إلى أخرى، لكن هناك مجموعة من المبادئ الأساسية المشتركة التي توجه جهود حماية المستهلك الإلكتروني عالميًا.

١٤. تحديات الحماية من الجرائم ضد المستهلك الإلكتروني تشمل الحاجة إلى توعية المستهلكين بالمخاطر الإلكترونية وكيفية الوقاية منها. يجب على المستهلكين تعلم كيفية تأمين بياناتهم الشخصية والمالية، وكيفية التعرف على رسائل البريد الإلكتروني الاحتيالية والروابط المشبوهة.

١٥. الجرائم الإلكترونية التي تستهدف المستهلكين تشكل تهديدًا متزايدًا في عالم يزداد اعتماده على التكنولوجيا والإنترنت. هذه الجرائم تأتي في أشكال متعددة، ويمكن تصنيفها إلى عدة أنواع رئيسية مثل: الاحتيال عبر الانترنت، وسرقة الهوية، والبرمجيات الخبيثة، التصيد الاحتيالي، والتنمر والتهديد الالكتروني، والتجسس الالكتروني والتتبع، وهجمات الحرمان من الخدمة.

١٦. تحديد الاختصاص القضائي في جرائم المستهلك الإلكتروني التي تتم عبر الحدود الدولية يمثل تحديًا كبيرًا بسبب الطبيعة العابرة للحدود للإنترنت والتجارة الإلكترونية.

١٧. الحدود بين جمع البيانات لتحسين الخدمات وانتهاك خصوصية المستهلك تتطلب توازنًا دقيقًا بين مصالح الشركات في توفير تجربة مستخدم مخصصة وفعالة وبين حقوق الأفراد في الخصوصية والسيطرة على بياناتهم الشخصية.

١٨. تحديد المسؤولية في حالات الاحتيال الإلكتروني، خاصة تلك التي تتضمن سلاسل إمداد معقدة أو استخدام الذكاء الاصطناعي والتكنولوجيا المتقدمة، يمثل تحديًا كبيرًا نظرًا للطبيعة المعقدة والمتداخلة للعمليات والأطراف المعنية.

التوصيات:

١. تعزيز التشريعات والقوانين: يجب على الحكومات والهيئات التشريعية تطوير وتحديث القوانين لتشمل جميع أشكال الجرائم الإلكترونية التي تستهدف المستهلكين، بما يضمن توفير حماية قانونية شاملة ومحدثة تواكب التطورات التكنولوجية.

٢. تحسين آليات الرصد والتتبع: تطوير البنية التحتية التكنولوجية والقدرات الفنية للأجهزة الأمنية والتنظيمية لتمكينها من رصد وتتبع الجرائم الإلكترونية بكفاءة أعلى وتحديد هويات المجرمين الإلكترونيين بسرعة ودقة.

٣. تعزيز التعاون الدولي: نظرًا لطبيعة الجرائم الإلكترونية التي لا تقتصر على حدود جغرافية محددة، يجب تعزيز التعاون الدولي من خلال تبادل المعلومات والخبرات والتنسيق في تنفيذ الإجراءات القضائية والأمنية.

٤. التوعية والتثقيف الرقمي: تنظيم حملات توعية واسعة النطاق للمستهلكين حول المخاطر الإلكترونية وكيفية الحماية منها، بما في ذلك تعليمهم طرق التعامل الآمن مع المعاملات الإلكترونية والحفاظ على خصوصية بياناتهم.

٥. تشجيع الإبلاغ عن الجرائم الإلكترونية: تسهيل عملية الإبلاغ عن الجرائم الإلكترونية للمستهلكين من خلال إنشاء قنوات اتصال مباشرة وفعالة مع السلطات المعنية، مما يساعد في سرعة الاستجابة والتعامل مع هذه الجرائم.

٦. تحسين الأمان السيبراني للمنصات الإلكترونية: العمل مع الشركات والمنصات الإلكترونية لتعزيز معايير الأمان السيبراني الخاصة بها، بما في ذلك تشفير البيانات وحماية النظم من الهجمات الإلكترونية.

٧. إنشاء وحدات متخصصة: تأسيس وحدات أمنية وقضائية متخصصة في التعامل مع الجرائم الإلكترونية، مجهزة بالخبرات والأدوات اللازمة لمواجهة هذه الجرائم بكفاءة وفعالية.

٨. تطوير الأنظمة القانونية للتعامل مع التحديات الجديدة: مراجعة وتحديث الأنظمة القانونية لضمان قدرتها على التعامل مع التحديات التي تفرضها التطورات التكنولوجية الجديدة، بما يشمل العملات الرقمية، الذكاء الاصطناعي، وغيرها.

المراجع

أولا- مراجع عربية:

أ) مؤلفات علمية

- الجهاز القومي لتنظيم الاتصالات (NTRA)، "النصائح لحماية نفسك عند التسوق عبر الإنترنت".

- حساين عومرية، الحماية القانونية للمستهلك الإلكتروني في ظل جائحة كوفيد ١٩، مجلة الاجتهاد القضائي، مج١٣، ع٢، جامعة محمد خيضر بسكرة – كلية الحقوق والعلوم السياسية – مخبر أثر الاجتهاد القضائي على حركة التشريع، ٢٠٢١.

- حمدان فاهد سعيد المزروعي، الحماية الجنائية للمستهلك في القانونين الإماراتي والمغربي، المجلة المغربية للإدارة المحلية والتنمية، ع١٣٢، ٢٠١٧.

- ديفيد ماكي، أمن المعلومات: حماية البيانات الحاسوبية الحيوية، دار المنهل، ٢٠١٨.

- شيكي حمزة، أية حماية للمستهلك من الإعلانات الإلكترونية، مجلة القانون والأعمال، ع٣٣، جامعة الحسن الأول – كلية العلوم القانونية والاقتصادية والاجتماعية – مختبر البحث قانون الأعمال، ٢٠١٨.

- عبدالحليم بوقرين، نحو حماية جنائية للمستهلك الإلكتروني، مجلة الفكر القانوني والسياسي، ع١، جامعة عمار ثليجي الاغواط – كلية الحقوق والعلوم السياسية، ٢٠١٧.

- فاطمة آيت الغازي، الحماية الجنائية للمستهلك في التعاقد الإلكتروني: دراسة مقارنة، مجلة قراءات علمية في الأبحاث والدراسات القانونية والإدارية، ع١٣، ٢٠٢٢.

- منظمة التعاون والتنمية الاقتصادية (OECD)، حماية الخصوصية والبيانات الشخصية: دليل المبادئ الأساسية للبيانات الشخصية عبر الحدود. باريس، ٢٠٢١.

- منظمة التعاون والتنمية الاقتصادية (OECD)،تقييم التشريعات والأنظمة لمكافحة الجرائم الإلكترونية: دليل المبادئ الأساسية. باريس، ٢٠٢٠.

- منظمة الشرطة الجنائية الدولية الإنتربول، دليل التحقيق في جرائم التكنولوجيا الرقمية. الدورة الثانية، ٢٠٢٢.

- نادية حموتى، الحماية الجنائية من جرائم الغش التجاري، مجلة القانون والأعمال، ع٦٧، جامعة الحسن الأول – كلية العلوم القانونية والاقتصادية والاجتماعية – مختبر البحث قانون الأعمال، ٢٠٢١.

- نسيمة درار، المستهلك الرقمي وقصور القوانين الكلاسيكية الناظمة لحمايته، مجلة المفكر، ع١٥، جامعة محمد خيضر بسكرة – كلية الحقوق والعلوم السياسية، ٢٠١٧.

ب) قوانين:

- قانون رقم ١٨١ لسنة ٢٠١٨ بتاريخ ٢٠١٨/٠٩/١٣ بشأن اصدار قانون حماية المستهلك.

- القانون رقم ٦٧ لسنة ٢٠٠٦ بشأن إصدار قانون حماية المستهلك (قانون ملغي)

- القانون رقم ٥٧ لسنة ١٩٥٩ بشأن حالات وإجراءات الطعن أمام محكمة النقض

- قانون رقم ١٧٥ لسنة ٢٠١٨ بتاريخ ٢٠١٨/٠٨/١٤ في شأن مكافحة جرائم تقنية المعلومات.

- قانون رقم ١٥ لسنة ٢٠٠٤ بتاريخ ٢٠٠٤/٠٤/٢٢ بشأن تنظيم التوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات.

- قانون اتحادي رقم (٢٤) لسنة ٢٠٠٦م في شأن حماية المستهلك.

- مرسوم بقانون ٥ لسنة ٢٠١٢ بشأن مكافحة جرائم تقنية المعلومات.

- نظام التجارة الإلكترونية مرسوم ملكي رقم (م/١٢٦) وتاريخ ٧/١١/١٤٤٠هـ.

- نظام مكافحة جرائم المعلوماتية مرسوم ملكي رقم م/١٧ بتاريخ ٨ / ٣ / ١٤٢٨هـ.

ت) أحكام محاكم:

- الطعن رقم ٢٠١ لسنة ٨٠ ق جلسة ٢٠١١/٥/٤.

- الطعن رقم ٨٣٨٠ لسنة ٨٠ ق جلسة ٢٠١١/٥/٢٣.

- الطعن رقم ٢٦٣٤٣ لسنة ٨٨ ق – جلسة ٩ / ١٠ / ٢٠١٩.

- الطعن رقم ٢٢١٣٠ لسنة ٨٨ ق – جلسة ٢٠١٩/٣/١١.

- الطعن رقم ٩١٧ لسنة ٩١ ق – جلسة ٢٠٢٢/١١/٩.

ثانيا- مراجع أجنبية:

أ) مؤلفات علمية:

- Allan Liska and Timothy Gallo, DDoS Attacks: Evolution, Detection, Prevention, Reaction, and Tolerance, Syngress, 2016.

- Allan Liska, DDoS Handbook: The Ultimate Guide to Everything You Need to Know About DDoS Attacks, Syngress, 2016.

- Anderson, R., & Moore, T. Cybercrime Legislation and Enforcement: A Global Perspective. International Journal of Cybersecurity Research, 5(1), 2020.

- Anh, N.V. Corporate Social Responsibility: Protecting Consumer Rights in E-commerce. In: An, N.B., Anh,

P.T. (eds) Laws on Corporate Social Responsibility and the Developmental Trend in Vietnam. Springer, Singapore, 2023.

- Bandara, R., Fernando, M. & Akter, S. Privacy concerns in E-commerce: A taxonomy and a future research agenda. Electron Markets30, 2020.

- Bascur, C., Montecinos, C., Mansilla, V. Ethical Design in e-Commerce: Case Studies. In: Meiselwitz, G. (eds) Social Computing and social media: Experience Design and Social Network Analysis . HCII 2021. Lecture Notes in Computer Science(), vol 12774. Springer, Cham, 2021.

- Bruce Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, John Wiley & Sons, 2015.

- Bruce Schneier, Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World, W. W. Norton & Company, 2015.

- Charles W. Lamb, Joe F. Hair, and Carl McDaniel, MKTG (Marketing), Cengage Learning, 2020.

- Christopher Hadnagy, Social Engineering: The Art of Human Hacking, Wiley, 2010.

- Da Veiga, A., Ochola, E., Mujinga, M., Mwim, E. Investigating Data Privacy Evaluation Criteria and Requirements for e-Commerce Websites. In: Guarda, T., Portela, F., Augusto, M.F. (eds) Advanced Research in Technologies, Information, Innovation and Sustainability. ARTIIS 2022. Communications in Computer and Information Science, vol 1676. Springer, Cham, 2022.

- Dahiyat, E.A.R. Consumer Protection in Electronic Commerce: Some Remarks on the Jordanian Electronic Transactions Law. J Consum Policy34, 2011.

- Daniel J. Solove and Paul M. Schwartz, Information Privacy Law, Wolters Kluwer Law & Business, 2019.

- Daniel J. Solove, The Digital Person: Technology and Privacy in the Information Age, New York University Press, 2004.

- David B. Jacobs, "Identity Theft: How to Protect Your Name, Your Credit and Your Vital Information, and What to Do When Someone Hijacks Any of These", Sourcebooks Inc, 2004.

- David L. Rogers, The Digital Transformation Playbook: Rethink Your Business for the Digital Age, Columbia University Press, 2016.

- Donmaz, A. Privacy Policy and Security Issues in E-Commerce for Eliminating the Ethical Concerns. In: Bian, J., Çalıyurt, K. (eds) Regulations and Applications of Ethics in Business Practice. Accounting, Finance, Sustainability, Governance & Fraud: Theory and Application. Springer, Singapore, 2018.

- Ed Tittel and Kim Lindros, Spyware For Dummies, Wiley, 2004.

- Federal Trade Commission. (2020). Online Shopping Scams.

- International Telecommunication Union (ITU), Global Cybersecurity Index 2020. United Nations, 2020.

- Jane Smith, "Cybersecurity and Consumer Protection: Emerging Threats in the Digital Age," Oxford University Press, 2021.

- Jane Smith, "Innovative Enforcement: Leveraging Technology for Consumer Protection," Oxford University Press, 2021.
- Jay S. Albanese, Transnational Crime and the 21st Century: Criminal Enterprise, Corruption, and Opportunity, Oxford University Press, 2011.
- Jiang, L., & Wang, Q. Cybersecurity Legislation: A Comparative Analysis of Global Trends. International Journal of Law and Technology, 8(3), 2020.
- John Doe, "Digital Law Enforcement: Challenges and Strategies in the Cyber Age," Cambridge University Press, 2020.
- John Doe, "Legislative Challenges in the Digital Era: Protecting Consumer Rights," Cambridge University Press, 2022.

- John Doe, "The Future of Electronic Payments: Security and Innovation," Cambridge University Press, 2022.
- Jolanta Tkaczyk, Digital Consumer: Trends and Challenges, 2016.
- Jonathan Clough, Principles of Cybercrime, Cambridge University Press, 2015.
- Kshetri, N. Cybersecurity Legislation in the Age of Artificial Intelligence and the Internet of Things. Journal of Cybersecurity Research, 7(1), 2021.
- Lars Perner, Consumer Behavior: The Psychology of Marketing, University of Southern California, 2021.
- Laudon & Traver, E-commerce 2021: Business, Technology, and Society, Pearson, 2021.
- Michael Geist, Internet Law in a Nutshell, West Academic Publishing, 2017.

- Michael Gregg, Certified Ethical Hacker (CEH) Version 10 Cert Guide, Pearson IT Certification, 2018.
- Michael R. Solomon, Consumer Behavior: Buying, Having, and Being, Pearson, 2020.
- Naikwadi, A.M. Consumer Protection in e-Commerce and Online Services. In: Wei, D., Nehf, J.P., Marques, C.L. (eds) Innovation and the Transformation of Consumer Law. Springer, Singapore, 2020.
- Neira Hajro , Klemens Hjartar , Paul Jenkins , and Benjamim Vieira, What's next for digital consumers, 2021.
- NSA. Cybersecurity Information. National Security Agency. 2021.

- Padilla, J., Piccolo, S. & Vasconcelos, H. Business models, consumer data and privacy in platform markets. J. Ind. Bus. Econ.49, 2022.

- Paul Voigt and Axel von dem Bussche, The EU General Data Protection Regulation (GDPR): A Practical Guide, Springer, 2017.

- Peter Szor, The Art of Computer Virus Research and Defense, Addison-Wesley Professional, 2005.

- Peter W. Singer and Allan Friedman, Cybersecurity and Cyberwar: What Everyone Needs to Know, Oxford University Press, 2014.

- Philip Kotler, Hermawan Kartajaya, and Iwan Setiawan, Marketing 4.0: Moving from Traditional to Digital, Wiley, 2016.

- Richard Ford and William R. Cheswick, Firewalls and Internet Security: Repelling the Wily Hacker, Addison-Wesley Professional, 2003.

- Robert D. Atkinson and Stephen J. Ezell, Innovation Economics: The Race for Global Advantage, Yale University Press, 2012.

- Robin M. Kowalski, Susan P. Limber, and Patricia W. Agatston, Cyberbullying: Bullying in the Digital Age, Wiley-Blackwell, 2012.

- Ryan Jenkins, The Millennial Manual: The Complete How-To Guide to Manage, Develop, and Engage Millennials at Work, RockBench Publishing Corp, 2018.

- Sameer Hinduja and Justin W. Patchin, Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying, Corwin Press, 2015.

- Smith, A., & Jones, B. Cybersecurity Laws and Regulations: A Global Overview. International Journal of Cybersecurity Research, 6(2), 2021.

- Susan W. Brenner, Cybercrime: Criminal Threats from Cyberspace, Praeger, 2010.

- Tanaka, S. (2020). Digital Platformers' Responsibilities to Platform Users; 'Consumer Protection' in B2C and C2C e-Commerce. In: Wei, D., Nehf, J.P., Marques, C.L. (eds) Innovation and the Transformation of Consumer Law. Springer, Singapore, p 48.

- Thomas J. Holt, Adam M. Bossler, and Kathryn C. Seigfried-Spellar, Cybercrime and Digital Forensics: An Introduction, Routledge, 2018.

- Tsyganov, V.I., Demin, A.A., Osadchenko, E.O. Obligations in the Field of E-Commerce. In: Inshakova,

A., Inshakova, E. (eds) Competitive Russia: Foresight Model of Economic and Legal Development in the Digital Age. CRFMELD 2019. Lecture Notes in Networks and Systems, vol 110. Springer, Cham, 2020.

- Uchenna Jerome Orji, Cybersecurity Law and Regulation, Wolters Kluwer, 2020.

- UNODC. Comprehensive Study on Cybercrime. United Nations Office on Drugs and Crime, 2013.

- WHO, Protecting Your Data: A How-to Guide for Internet Privacy, 2020.

- Zhang, Q. Research on Rights Protection of Consumer and Interests in E-Commerce-Taking Functional Department and Industry Association. In: Du, W. (eds) Informatics and Management Science VI. Lecture Notes

in Electrical Engineering, vol 209. Springer, London, 2013.

ب) قوانين اجنبية:

- Directive 95/46/EC (General Data Protection Regulation).
- Directive 2011/83/EU on consumer rights. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011L0083
- INFORM Consumers Act, 15 U.S.C. § 45f. online: https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section45f&num=0&edition=prelim
- Consumer Review Fairness Act, 15 U.S.C. § 45b, online: https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section45b&num=0&edition=prelim
- Competition and Consumer Act 2010, online: https://www.legislation.gov.au/C2004A00109/latest/text

- Privacy Act 1988, online: https://www.legislation.gov.au/C2004A03712/latest/versions

ثالثا – مواقع الكترونية:

- **https://www.ntra.gov.eg**
- **https://www.consumer.ftc.gov**
- **https://www.legislation.gov.au**
- **https://uscode.house.gov**
- **https://eur-lex.europa.eu**
- **https://www.researchgate.net**
- **https://www.mckinsey.com**