تأثير الجريمة الالكترونية على الأمن المعلوماتي

The Impact of Cybercrime on Information Security

معاد الشبكي: كلية الآداب والعلوم الإنسانية بالرباط، المغرب.

Maad Alshabki: Faculty of Arts and Humanities in Rabat, Morocco.

Email: chabki.edu@gmail.com

تاريخ الاستلام: 2025-09-29 تاريخ القبول: 2025-10-19 تاريخ النشر 2025-11-01

الملخص:

يشهد العصر الرقمي تطورا متسارعا وملحوظا في استخدام الوسائط الإلكترونية والأنظمة المعلوماتية، الأمر الذي أفضى إلى ظهور نمط جديد من الجرائم يعرف بـ"الجريمة الإلكترونية". وهذه الجرائم، وإن كانت غير مادية، إلا أن تأثيرها عميق وخطير، كما أصبحت تمارس على نطاق واسع لسهولة توفر أركانها، دون أن يحدها أي نطاق جغرافي. وهي بذلك تشكل خطرا مباشرا على الأفراد والمؤسسات والدول على حد سواء، مستهدفة النظم المعلوماتية وسلامة المعطيات الحساسة، ومهددة بذلك استقرار الفضاء السيبراني.

يعالج هذا المقال الجريمة الإلكترونية من زاوية تأثيرها المباشر على الأمن المعلوماتي، باعتباره إحدى الركائز الجوهرية لحماية المجتمعات الرقمية الحديثة. حيث يبدأ أولا بتحديد المفاهيم التأسيسية ذات الصلة، وعلى رأسها مفهوم الأمن المعلوماتي وخصائصه الجوهرية، ثم يستعرض المنظومة القانونية الوطنية والدولية المؤطرة له، مركزا على القوانين المغربية ذات الصلة والاتفاقيات الدولية التي انخرط فيها المغرب.

كما يتطرق المقال إلى تحليل الأساليب التقنية المستخدمة في ارتكاب الجرائم المعلوماتية، بما في ذلك أدوات الاختراق، والبرمجيات الخبيثة، واستغلال الثغرات البشرية والتقنية. ويركز على خصائص الجريمة الإلكترونية التي تميّزها عن الأفعال التقليدية، لا سيما طابعها العابر للحدود، وسهولة تنفيذها، وصعوبة تعقب مرتكبيها.

ويخلص المقال نهاية إلى أن مكافحة الجريمة الإلكترونية تقتضي مقاربة متعددة الأبعاد، تشمل تطوير الإطار القانوني، وتعزيز القدرات التقنية، وتكثيف التعاون الدولي، فضلا عن نشر ثقافة الأمن الرقمي بين المستخدمين. إن حماية الأمن المعلوماتي لم تعد خيارا، بل أضحت ضرورة سيادية لضمان استقرار الدولة والمجتمع في العصر الرقمي.

الكلمات المفتاحية: الجريمة الإلكترونية، الأمن المعلوماتي، التشريع الرقمي، الاختراق السيبراني، الفضاء الرقمي.

Abstract:

The digital era has brought unprecedented reliance on information systems and electronic networks, which in turn has given rise to a new form of criminal activity known as “cybercrime.” Though intangible, these offenses have far-reaching and serious impacts, targeting individuals, institutions, and states alike. They undermine data security, disrupt information systems, and pose significant threats to national stability in cyberspace.

This article examines cybercrime through the lens of its direct implications for information security, which is a foundational component of digital societal resilience. It begins by clarifying key concepts, particularly the legal and technical dimensions of information security and its core characteristics. It then explores both national and international legal frameworks, with a focus on Moroccan legislation and global conventions in which Morocco participates.

The article further analyzes the tools and techniques employed in committing cybercrimes, including hacking software, malicious programs, and exploitation of both human and technical vulnerabilities. Special attention is given to the unique attributes of cybercrime, such as its borderless nature, ease of execution, and the difficulty of tracing perpetrators.

The study concludes that effectively combating cybercrime demands a multidimensional approach: reinforcing the legal framework, advancing technical capabilities, intensifying international cooperation, and promoting a culture of digital security. In the digital age, safeguarding information security is no longer optional; it is a sovereign necessity to preserve the stability of the state and society.

Keywords: Cybercrime, Information Security, Digital Legislation, Cyber Intrusion, Digital Space.

المقدمة:

شهد العالم في الآونة الأخيرة طفرة معلوماتية هائلة بفضل التطور التكنولوجي، مما أدى إلى تحول نمط إدارة الدولة نحو الصيغة الإلكترونية .فقد أصبحت المعلومة موردًا استراتيجيًا ذو قيمة مالية بالغة، وصار من يمتلكها يتحكم في ميزان القوى ضمن اقتصاد معلوماتي محض .إلى جانب ذلك، برزت ظاهرة البيانات الضخمة واستعمالها كمصدر أساسي لصنع القرار .بيد أن هذه الوفرة المعلوماتية ترافقها مخاطر وتهديدات تستهدف الأفراد والجماعات والمؤسسات على حد سواء.

أضحى كل مستهلك للإنترنت معرضًا للتهديد والخطر في ظل أحكام الاستخدام التي تنص عليها البرمجيات ومحركات البحث، حيث يجد الفرد نفسه مضطرًا للموافقة على مشاركة بياناته مع جهات غير معلومة لأغراض مبهمة .ومن أبرز التهديدات التي تواجه المستخدم الرقمي القرصنة المعلوماتية وسرقة المعطيات والتجسس والاختراق والدخول غير المشروع إلى المواقع الإلكترونية دون إذن، وغيرها من السلوكيات الإجرامية المستحدثة1.

غير أن هذا الواقع الرقمي الجديد لم يكن بمنأى عن المخاطر والتحديات، إذ ظهرت معه أنماط جديدة من الإجرام تتخذ من الوسائل الإلكترونية والأنظمة المعلوماتية وسيلة وأحيانا غاية في حد ذاتها، فيما أصبح يعرف اليوم بـ"الجريمة الإلكترونية" أو "الجريمة السيبرانية". هذه الأخيرة لم تعد جرائم فردية معزولة، بل تحولت إلى ظاهرة عابرة للحدود تمس الأمن العام، والاقتصاد العالمي، والخصوصية الفردية، والسيادة الوطنية، مما جعلها من أخطر التحديات التي تواجه الدول والمؤسسات الأمنية والقانونية في العصر الرقمي.

وعليه، تتميز الجريمة المعلوماتية بجملة من الخصائص التي تميزها عن الجرائم التقليدية، فهي لا تعترف بالحدود الجغرافية، فقد تقع في نطلق جغرافي معين، بينما يتواجد ضحاياها في نطاق آخر، كما أنها سريعة التنفيذ ويصعب تتبع أدلتها لسرعة طمسها واخفاء آثارها، كما أنها ترتكب من طرف أشخاص ذوي مهارات تقنية وذكاء تكنولوجي في التعامل مع الحواسيب والتلاعب بالتقنيات المعلوماتية، ما يضفي عليها تعقيدًا وتحديًا خاصًا في المكافحة[2].

ويقصد بالجريمة الإلكترونية، في أبسط صورها، كل سلوك غير مشروع يرتكب عبر وسائط إلكترونية، يستهدف نظاما معلوماتيا أو بيانات رقمية، سواء بالاختراق أو التلاعب أو الإتلاف أو

---

[1]. مقناني، صبرينة (2020): تأثير الجريمة الالكترونية على المعلومات الرقمية، المجلة الجزائرية للأبحاث والدراسات، المجلد الثالث، العدد التاسع، ص138.

[2]. السحيمي، أمين؛ وبوفرعة، عبد المجيد (2024): الإطار القانوني المغربي للجرائم الالكترونية بين التشريع الوطني والاتفاقيات الدولية، مجلة البحث في العلوم الإنسانية والمعرفية، المجلد 1، العدد 6، السنة الأولى شتنبر، ص235.

الاستغلال غير المشروع. إلا أن خطورتها لا تكمن فقط في طبيعتها التقنية المعقدة، بل في قدرتها على الإضرار المباشر بالأمن المعلوماتي، الذي يشكل بدوره حجر الأساس لاستقرار المجتمعات الحديثة. فالأمن المعلوماتي يعني حماية الأنظمة والشبكات والبيانات من أي تهديد أو هجوم قد يؤدي إلى فقدان الثقة أو تعطيل الخدمات أو تسريب المعطيات الحساسة. ومن ثم، فإن العلاقة بين الجريمة الإلكترونية والأمن المعلوماتي هي علاقة تضاد وجودي، فكل تطور في الجريمة الإلكترونية يقابله تحد جديد في حماية الأمن المعلوماتي.

وفي السياق ذاته، لم يكن المغرب بمنأى عن هذه التحولات، إذ شهد بدوره تزايدا في وتيرة الجرائم الإلكترونية وتنوعا في أساليبها، سواء من حيث استهداف الأفراد عبر الاحتيال الإلكتروني والابتزاز الرقمي، أو المؤسسات عبر الاختراق وسرقة البيانات، وهو ما دفع المشرع المغربي إلى التدخل من خلال سن مجموعة من النصوص القانونية، في مقدمتها القانون رقم 07.03 المتمم لمجموعة القانون الجنائي في ما يخص جرائم المس بنظم المعالجة الآلية للمعطيات[1]، بالإضافة إلى ذلك جاء القانون 09.08 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي[2] ليؤسس لحماية الحقوق الفردية في مواجهة الاستغلال غير المشروع للبيانات، ثم لاحقا القانون رقم 05.20 المتعلق بالأمن السيبراني[3]، الذي يعد نقلة نوعية في التنظيم القانوني للأمن المعلوماتي. وقد أسهم هذا الإطار التشريعي في وضع أسس واضحة لتأمين الفضاء السيبراني الوطني وتعزيز قدرات الدولة في مواجهة التهديدات الرقمية.

وعليه، ففي ظل الانتشار المتسارع للتقنيات الرقمية وتزايد الاعتماد على الأنظمة المعلوماتية في مختلف مناحي الحياة، برزت الجريمة الإلكترونية كأحد أبرز التحديات الأمنية والقانونية التي تهدد استقرار الفضاء الرقمي، وتثير تساؤلات عميقة حول قدرة التشريعات الوطنية والدولية على حماية الأمن المعلوماتي من مخاطر الاختراق، والتخريب، وسرقة المعطيات، والتلاعب بالمعلومات.

---

[1]. القانون رقم 07.03 المتمم لمجموعة القانون الجنائي فيما يتعلق بالجرائم المتعلقة بنظم المعالجة الآلية للمعطيات الصادر بتنفيذه ظهير شريف رقم 1.03.197 بتاريخ 16 رمضان 1424، (11 نونبر 2003)، الجريدة الرسمية عدد 5171، بتاريخ 27 شوال 1424(22 ديسمبر 2003)، ص 4284.

[2]. القانون 09.08 المتعلق بحماية المعطيات الأشخاص الذاتيين للمعطيات ذات الطابع الشخصي، الصادر بتنفيذه ظهير شريف رقم 1.09.15 الصادر بتاري 22 صفر 1430 (18فبراير 2009)، الجريدة الرسمية عدد 5711، بتاريخ 27 صفر 1430 (23 فبراير 2009) ص 552.

[3]. ظهير شريف رقم 1.20.69 صادر في 4 ذي الحجة 1441 الموافق لـ 25 يوليوز 2020، بتنفيذ القانون رقم 05.20 المتعلق بالأمن السيبراني، الجريدة الرسمية عدد 6904 بتاريخ 9 ذو الحجة 1441 الموافق لـ 30 يوليوز 2020 ص 4160.

ومن هذا المنطلق، يمكن صياغة الإشكالية الرئيسية للمقال على النحو الآتي:

إلى أي حد تؤثر الجريمة الإلكترونية في تقويض الأمن المعلوماتي، وما مدى فعالية الإطار القانوني والتقني المغربي في مواجهة هذا التهديد وضمان حماية الفضاء السيبراني الوطني؟

ومن خلال ما سبق التطرق إليه ارتأينا تقسيم هذه الورقة العلمية إلى محورين وهما كالآتي:

- المبحث الأول: مفهوم الأمن المعلوماتي
- المبحث الثاني: الجريمة الإلكترونية وتصدع الأمن المعلوماتي

المبحث الأول: مفهوم الأمن المعلوماتي

يعد الأمن المعلوماتي حجر الزاوية وركيزة أساسية في مجال حماية الرقمنة والفضاء الرقمي، وتسعى الدول في الوقت الحالي إلى إعطائه العناية والحماية الفائقة على غرار الأوجه الأخرى من الأمن الشامل، كالأمن الداخلي والخارجي، والأمن السياسي، والأمن العسكري، والأمن الغذائي...، ولما كانت الجرائم المعلوماتية تنصب على البيانات والمعطيات بكل أنواعها شخصية وغير شخصية، جاء الأمن المعلوماتي بهدف تكريس الأمن الرقمي وتأمين البيئة الرقمية، فما هو إذا تعريف الأمن المعلوماتي وبيان خصائصه **(أولا)** وما هو الإطار التشريعي والمؤسساتي والاستراتيجي للأمن المعلوماتي **(ثانيا)**.

أولا: تعريف الأمن المعلوماتي وبيات خصائصه

سنحاول الوقوف على تعريف الأمن المعلوماتي **(1)**، ثم التطرق لأهم خصاصه **(2)**.

1. تعريف الأمن المعلوماتي

يمكن تعريف أمن المعلومات بأنه مجموعة الإجراءات والتدابير الهادفة إلى حماية المعلومات الحساسة من الولوج أو الاستخدام أو الإفشاء أو التغيير أو التعطيل غير المصرح به. والغاية من ذلك هي ضمان إتاحة المعطيات التنظيمية الهامة للمستخدمين المخوّل لهم فقط، مع الاستمرار في صون سريتها وسلامتها وعدم العبث بها أو انتهاكها.

وبمعنى آخر؛ يشمل الأمن المعلوماتي الإجراءات والتدابير المستخدمة في المجالين الإداري والفني لحماية المصادر البيانية من أجهزة أو برمجيات وبيانات وأفراد من التجاوزات والتدخلات

غير المشروعة التي تقع عن طريق الصدمة أو عمدا عن طريق التسلل، أو كنتيجة لإجراءات خاطئة أو غير الوافية المستخدمة من إدارة هذه المصادر[1].

وعليه، فالمشرع المغربي في إطار قانون 05.20 المتعلق بالأمن السيبراني عمد على غير عادته إلى تعريف الأمن السيبراني، حيث اعتبره في المادة 2 على أنه: "مجموعة من التدابير والإجراءات ومفاهيم الأمن وطرق إدارة المخاطر والأعمال والتكوينات وأفضل الممارسات والتكنولوجيات التي تسمح لنظام معلومات أن يقاوم أحداثا مرتبطة بالفضاء السيبراني، من شأنها أن تمس بتوافر وسلامة وسرية المعطيات المخزنة أو المعالجة أو المرسلة والخدمات ذات الصلة التي يقدمها هذا النظام أو تسمح بالولوج إليه".

من خلال هذا النص التشريعي والتعريف الشامل، نلاحظ أن المشرّع حرص على توسيع مفهوم الأمن المعلوماتي ليشمل مختلف الجوانب ذات الصلة كإدارة المخاطر والموارد والتقنيات الحديثة، تفاديًا لأي لبس مع مفاهيم متقاربة .ونرى أن هذا التوجه من المشرّع أمر مرغوب للحد من التداخل بين المصطلحات المتشابهة في هذا المجال.

ويمكننا القول إن الأمن المعلوماتي هو كل ما تعلق بأمن وسلامة وسرية وصيانة وحماية المعلومة سواء تعلق الأمر بالجانب الإداري والمعاملات التي تتبادل فيها المعلومة أو الجانب التقني والفني أي الوسائل المستخدمة في الأمن والحفظ والصيانة والتخزين والبرمجيات كما لا نستثني من ذلك مراكز تواجد الحاسبات[2].

2. خصائص الأمن المعلوماتي

للأمن المعلوماتي مجموعة من الخصائص، أهمها:

- **الثقة وعدم الثقة:** يسمح بمرور البرامج التي تمتلك بالفعل الثقة من المستخدم، بعد التأكد من أمان استخدامها، إذ يمتلك جدار للحماية خاص بأمن نظم المعلومات، الذي يمنع البرامج الخبيثة واستغلال الثغرات.
- **الحماية من التهديدات الخارجية:** يعمل الأمن المعلوماتي على بناء جدار للحماية والتصدي لكل الهجمات السيبرانية الخارجية والقضاء عليها، وخصوص المخاطر الناتجة عن التعامل العالم الرقمي الخارجي، بداية من الروابط الخبيثة أو مخاطر الرسائل الإلكترونية الخطرة أو

[1]. صدق، دلال؛ وفتال، وحميد ناصر (2008): الأمن المعلوماتي، هيئة التعليم التقني، الأردن: دار اليازوردي العلمية للنشر والتوزيع، ص 12.

[2]. قصعة، سعاد (2020): تحديات الأمن المعلوماتي في مواجهة الجريمة الالكترونية في ظل الاعلام الجديد، مقال منشور في مجلة المعيار، المجلد 24، العدد 50، ص 379.

الفيروسات أو معالجة الضعف في النظام أو الثغرات التي قد يستغلها طرف ثالث في السيطرة والتحكم[1].

- **مراقبة مستمرة ورؤية شاملة:** يهدف الأمن المعلوماتي إلى توفير الحماية للمستخدم طوال الوقت بهدف اكتشاف أي خلل بمجرد وجوده والعمل على سرعة إصلاحه والتخلص منه، ومنعه من إحداث أي ضرر والحفاظ على أمن المعلومات والأمن الخاص بالمستخدم لأطول فترة ممكنة، كما يعمل المن المعلوماتي على توفير للمستخدم رؤية شاملة عن المخاطر السيبرانية التي تواجه ويعمل على التصدي لها واصلاحها وتقديم التوصيات لتجنبها.
- **الحماية من التهديدات الداخلية:** يهدف نظام الأمن المعلوماتي إلى حماية الجهاز من الهجمات السيبرانية الداخلية والقضاء على هذه التهديدات، الناتجة عن عدم الوعي بالمخاطر السيبرانية من المستخدم أو جهله بها، مما يسمح للبرامج الخبيثة من استغلال أمنه الشخصي ومشاركة معطياته الشخصية وكل ما يملك من المعلومات، حينها يقوم الأمن المعلوماتي بسرعة تنبيه الفرد أو المؤسسة بالخطر التي تواجهه ويقوم بمنع حدوث هذا الإجراء في أسرع وقت.
- **التنوع:** يتميز الأمن المعلوماتي بنظام خاص للحماية وذلك عن طريق التصدي للهجمات السيبرانية، كما يوفر حلول مجمعة للتعامل مع هذه التهديدات، إذ لا يمكن للنظام الحماية أن يتصدى لبعض التهديدات ويسمح لأخرى، بل لابد من أن يتصدى للكل أنواع الهجمات الممكنة التي تمس بسلامة وأمن المعلومات.

ثانيا: الإطار التشريعي والمؤسساتي للأمن المعلوماتي

لتحديد الإطار التشريعي والمؤسساتي للأمن المعلوماتي، لا من الوقوف في هذه الفقرة على الإطار التشريعي للأمن المعلوماتي **(1)**، على أن نعالج **(2)** الإطار المؤسساتي للأمن المعلوماتي.

1. الإطار التشريعي للأمن المعلوماتي

سنقوم بالحديث عن الإطار التشريعي للأمن المعلوماتي من خلال التطرق للاتفاقيات والمعاهدات الدولية التي صادق عليها المغرب ثم للقوانين التي أحدثها المشرع المغربي.

[1]– بابكر، إسماعيل، خصائص الأمن السيبراني، مقال منشور على الموقع الالكتروني https://alwatannewssd.com/56117/ تم الاطلاع عليه بتاريخ 2025/10/02، على الساعة 14:00.

1.1. الاتفاقيات والمعاهدات الدولية

تتعدد وتتنوع الاتفاقيات والمعاهدات الدولية التي صادق عليها المغرب والتي تهدف إلى تكريس الأمن المعلوماتي وأهم هذه الاتفاقيات:

1.1.1 : اتفاقية بيرن لحماية المصنفات الأدبية والفنية (9 شتنبر 1886)

تُعد اتفاقية بيرن من أقدم الاتفاقيات الدولية التي تعنى بحماية حقوق المؤلف وملكية الإبداع الفكري. خضعت هذه الاتفاقية عبر تاريخها لعدة مراجعات وتعديلات بهدف مواكبة التطورات – بما فيها ظهور المصنفات الرقمية – وتهدف أحكامها إلى ضمان حماية المؤلفات أيًا كانت وسيلة أو شكل نشرها. وقد انضم المغرب إلى اتفاقية بيرن وغيرها من معاهدات الملكية الفكرية إيمانًا بأهمية حماية الإنتاج الفكري في العصر الرقمي[1].

2.1.1: اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية سنة 2000

تناولت هذه الاتفاقية سبل التعاون القانوني الدولي في مواجهة أشكال الجريمة المنظمة العابرة للحدود، بما فيها الجرائم المعلوماتية .وقد حثّت جميع الدول على إبرام اتفاقيات ثنائية أو متعددة الأطراف لتبادل المعلومات والأدلة الرقمية وتيسير تسليم المجرمين الإلكترونيين، بهدف تعزيز فعالية منع الجرائم الإلكترونية ومكافحتها [2].

3.1.1: اتفاقية بودابست لمكافحة الجرائم المعلوماتية بتاريخ 8 نونبر 2001

تعتبر اتفاقية بودابست أول معاهدة دولية تضع إطارا موحدا لمكافحة الجريمة الإلكترونية، من خلال إرساء سياسة جنائية عالمية تُيسّر تعقّب وملاحقة مرتكبي الجرائم السيبرانية وتنسيق التشريعات الوطنية[3].

---

[1]. انضم المغرب لهذه الاتفاقية بتاريخ 16 يونيو 1917، وصادق على آخر عقد تعديلي لها بباريس 24 يوليوز 1971 وبتاريخ 17 فبراير 1987 (الجريدة الرسمية عدد 1326 الصفحة 517 جريدة رسمية عدد 2019 صفحة 1698 جريدة رسمية عدد 3879 صفحة 220)، كما تعد المملكة المغربية ثاني دولة عربية تنظم لهذه الاتفاقية بعد تونس.

[2]. في هذا الإطار صادق المغرب على هذه الاتفاقية بناء على محضر إبداع وثائق مصادقة المغرب على الاتفاقية المذكورة الموقع بنيويورك في 20 شتنبر 2002، كما تم نشرها في الجريدة الرسمية رقم 5186 الصادرة يوم الخميس 12 فبراير 2004.

[3]. صادق مجلس الحكومة المغربية بتاريخ 20 دجنبر 2012 على مشروع القانون رقم 12–136 الذي يوافق بموجبه على اتفاقية "بودابيست" المتعلقة بالجريمة المعلوماتية، حيث صدر فيما بعد القانون 136.12 الموافق بموجبه على هذه الاتفاقية وكذا على برتوكولها الإضافي الموقع بستراسبورغ بشأن تجريم الأفعال ذات الطبيعة

تميزت اتفاقية بودابست بمنح أولوية كبيرة للإجراءات الجنائية اللازمة للتحقيق في الجرائم المعلوماتية، حيث خُصص نحو نصف موادها للقواعد الإجرائية. ألزمت الدول الأطراف باتخاذ تدابير تشريعية لتوفير أدوات تحقيق فعّالة، مثل حفظ البيانات الإلكترونية العاجل والتعاون الفوري بين السلطات عبر الحدود. وقد أسهمت هذه الاتفاقية في إرساء آليات سريعة لتبادل المعلومات والأدلة بين الدول، مما مكّن من تتبع الجرائم الإلكترونية العابرة للحدود بشكل أكثر كفاءة.

4.1.1: الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

تسعى هذه الاتفاقية إلى تعزيز آليات التعاون بين الدول العربية خاصة فيما يتعلق بالتصدي للجرائم المعلوماتية، وتجنب الأخطار الجانبية لهذه الجرائم، وتعزيز الأمن الرقمي للدول العربية وحماية مصالحها وسلامتها وتحقيق الأمن الرقمي[1].

2.1: القوانين المغربية لتكريس الأمن المعلوماتي

حتى نعالج التجربة التشريعية المغربية التي تسعى إلى تحقيق الأمن المعلوماتي بشكل شمولي، ومن بين هذه القوانين نجد:

1.2.1: القوانين الخاصة المتعلقة بالمعاملات الإلكترونية

تتمثل هذه التشريعات في:

القانون رقم 07.03 المتعلق بمكافحة جرائم المس بنظم المعالجة الآلية للمعطيات

يعد من أهم النصوص التي أضيفت لمجموعة القانون الجنائي المغربي[2] بغية وضع إطار تشريعي ملاءم في مجال مكافحة الجريمة الإلكترونية، إذ يسعى إلى حماية النظم المعلوماتية من خطر التلاعب الالكتروني، كما يعد الإطار القانوني الخاص بتجريم الأفعال التي تعتبر جرائم ضد نظم المعالجة الآلية للمعطيات والدخول غير المشروع للنظام المعلوماتي، أو البقاء فيه، أو تغيير

العنصرية وكراهية الأجانب التي ترتكب عن طريق أنظمة الكمبيوتر في 28 يناير 2003، وذلك بتاريخ 29 ماي 2014، وفقا للظهير الشريف رقم 1.14.85 الصادر في 12 ماي 2014 بالجريدة الرسمية عدد 6260 (ص 4711).

[1]. صادق المغرب على هذه الاتفاقية، بموجب ظهير شريف رقم 1.13.44 الصادر في فاتح جمادى الأولى 1434 الموافق 13 مارس 2013 القانون 75.12 الموافق بموجبه على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الموقعة بالقاهرة في 21 دجنبر 2010، والمنشور بالجريدة الرسمية عدد 6140، ص 3023.

[2]. ويضم هذا القانون تسعة فصول تبتدئ من الفصل 607-3 إلى الفصل 607-11، من مجموعة القانون الجنائي.

المعطيات داخل هذا النظام، وقد ساوى المشرّع بين الدخول الجزئي والكلي غير المصرح به، ما دام ذلك تم عن طريق الاحتيال [1].

بقراءتنا لمضامين وأحكام هذه القانون، نجد أن المشرع جرم الأفعال التي تنصب على البيانات أو المعطيات بشكل أساسي، أو ما يسميه بعض الفقه بالأملاك غير المادية[2]، غير أنه استخدم مصطلح "البيانات "في النص دون إضافة وصف "المعلوماتية"، مما قد يفتح مجالًا للَّبس؛ إذ يمكن للبيانات أن تكون غير إلكترونية .وعليه، يُستحسن أن يتم التنصيص صراحة على الطبيعة المعلوماتية للبيانات محل الحماية، حتى يتضح أن المقصود هو البيانات الإلكترونية دون غيرها.

القانون رقم 53.05 المتعلق بالتبادل الالكتروني للمعطيات الالكترونية

أقر هذا القانون مبدأ المعادلة القانونية بين الوثائق الورقية ونظيرتها الإلكترونية، بما في ذلك الرسائل والعقود والتوقيع الإلكتروني. كما وضع الإطار القانوني لتنظيم عمليات تبادل المعطيات بطريقة إلكترونية، وحدّد نظامًا لاعتماد مقدمي خدمات التصديق الإلكتروني وبيّن التزاماتهم. إضافة لذلك، تضمّن القانون عقوبات على بعض الأفعال المرتبطة بالجريمة المعلوماتية، من قبيل إفشاء شخص للمعطيات التي وُضعت تحت يده بحكم وظيفته أو نشاطه والتحريض على ذلك أو المساهمة فيه، وغيرها من الجرائم المنصوص عليها ضمن أحكامه

- **القانون 05.20 المتعلق بالأمن السيبراني**

سعى هذا القانون إلى تحقيق عدة أهداف استراتيجية، من بينها: وضع إطار قانوني ومؤسسي لتدابير الحماية في الفضاء السيبراني للمغرب، وكذا ضمان صمود وأمن نظم المعلومات التابعة للدولة، الجماعات الترابية، المؤسسات والمقاولات، الأشخاص المعنويين الخاضعين للقانون العام، وكذلك حماية البنى التحتية ذات الأهمية الحيوية التي تعتمد على نظم معلومات حساسة بالإضافة إلى ذلك، فرض التزامات على المشغلين الرقميين، مزودي خدمات الإنترنت، مقدمي خدمات الأمن السيبراني، ناشري المنصات الإلكترونية وغيرها من المتعهدين، ثم تنظيم التوجيه، التعاون، التبليغ، والتنسيق بين السلطة الوطنية المختصة وباقي الجهات ذات العلاقة

[1]– بنسليمان، عبد السلام (2020): الإجرام المعلوماتي في التشريع المغربي، دراسة نقدية في ضوء آراء الفقه وأحكام القضاء، مكتبة دار الأمان بالرباط، الطبعة 2، ص 73.

[2]– Mohamed Ourgane. (2005). La criminalité informatique au regard du droit pénal marocain, centre marocain des études juridiques, Tome 1, p 236.

- **القانون رقم 09.08 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي**

جاء هذا القانون استجابة للحاجة إلى تأمين البيانات الشخصية للأفراد في سياق المعاملات الإلكترونية .فقد باتت المعطيات الشخصية المُعالجة إلكترونيًا ذات أهمية خاصة دوليا، مما حدا بالمشرّع المغربي إلى إصدار هذا القانون سنة 2009 تماشيًا مع التشريعات المقارنة.

وقد وضع القانون ضوابط صارمة لمعالجة البيانات ذات الطابع الشخصي، كما منح الأفراد حقوقا بشأن بياناتهم، كالحق في الاطلاع والتصحيح والاعتراض. وقد تضمّن أيضا عقوبات زجرية لحماية هذه الحقوق، من ذلك أن المادة 53 منه تعاقب بغرامة بين 20.000 و 200.000درهم كل مسؤول عن معالجة البيانات يرفض الاستجابة لطلبات الولوج أو التصحيح أو الاعتراض التي يخولها القانون للأفراد .كما تجرّم المادة 63[1] نقل المعطيات الشخصية خارج المملكة دون احترام الشروط المنصوص عليها في المادتين 43 و 44من القانون. ويرى البعض أن المشرّع كان حريا به تشديد العقوبات على خرق الضوابط الخاصة بالبيانات الشخصية، نظرا لحساسية هذه المعطيات ولما قد يترتب على انتهاكها من أضرار اقتصادية واجتماعية جسيمة على الأفراد، وذلك تحقيقا لمزيد من الردع العام والخاص.

2.2.1: القوانين المنظمة للعمليات المتعلقة بالفضاء الرقمي

من بين هذه القوانين نجد:

- **القانون 31.08 المتعلق بحماية المستهلك[2]**

إن الغاية من إصدار هذا القانون هو توفير الحماية القانونية للمستهلك سواء كانت العمليات التي يقوم بها المستهلك تقليدية أم إلكترونية، لذلك سنحاول الوقوف على بعض مظاهر الحماية الجنائية للمستهلك الالكتروني، بحيث نجد المشرع المغربي ينص من خلال المادة 175 نص على عقوبة الغرامة من 10.000 إلى 50.000 درهم بالنسبة للمورد الذي يرسل (خلافا لأحكام المادة 23 أعلاه) أي إشهار عن طريق البريد الإلكتروني دون الموافقة المسبقة والحرة والصريحة

[1]– تنص المادة 63 على أنه: "يعاقب كل مسؤول يرفض تطبيق قرارات اللجنة الوطنية بالحبس من 3 أشهر إلى سنة وبغرامة من 10,000 إلى 100,000 درهم أو بإحدى هاتين العقوبتين فقط.

[2]– ظهير شريف رقم 1.11.03 صادر في 14 من ربيع الأول 1432 (18 فبراير 2011) بتنفيذ القانون رقم 31.08 القاضي بتحديد تدابير حماية المستهلك، المنشور بالجريدة الرسمية عدد 5932 بتاريخ 3 جمادى 1432 (17 أبريل 2011) ص 1072.

للمستهلك بعد إخباره، كما يعاقب بنفس العقوبة كل من قام بإرسال إشهار عن طريق البريد الإلكتروني عندما يتم:

- استعمال البريد الإلكتروني أو هوية الغير؛
- تزييف أو إخفاء أي معلومة تكمن من تحديد مصدر الرسالة الموجهة عبر البريد الإلكتروني أو مسار إرسالها[1].

- **القانون 24.96 المتعلق بالبريد والمواصلات[2].**

تضمّن هذا القانون عددًا من المقتضيات الزجرية في حق كل من يستغل وسائل المعالجة المعلوماتية للاعتداء على خدمات البريد والاتصالات .فمثلًا يجرّم إنجاز إرسال لاسلكي راديوي باستخدام إشارة نداء دولية مخصصة لمحطة الدولة أو لشبكة الاتصالات العامة أو لمحطة خاصة مرخّص لها، إلى جانب تجريم بعض الأفعال الأخرى المنصوص عليها في المادة 83 منه [3]. وهذه الأحكام تهدف إلى حماية نظم الاتصالات من أي استعمال غير مشروع للتقنيات المعلوماتية.

- **القانون 02.99 المتعلق بمكافحة استغلال المعلوميات من أجل ارتكاب جريمة جمركية[4]**

---

[1]– بوعيدة، عبد الرحيم؛ نعمان، ضياء علي أحمد (2009): موسوعة التشريعات الالكترونية المدنية والجنائية، التشريع المغربي والعربي والفرنسي الاتفاقيات العربية والأوربية والدولية، المطبعة والوراقة الوطنية مراكش، الطبعة 1، ص 177 و178.

[2]– ظهير شريف رقم 1.97.162 صادر في 2 ربيع الآخر 1418 الموافق لـ 7 أغسطس 1997، بتنفيذ القانون رقم 24.96 المتعلق بالبريد والمواصلات، منشور بالجريدة الرسمية عدد 4518 بتاريخ 15 جمادى الأول 1418 الموافق لـ 18 سبتمبر 1997، ص 3721.

[3]– تنص المادة 83 على ما يلي: " يعاقب بالحبس من شهر إلى سنتين وبغرامة من 10000 إلى 200000 درهم:

"كل من أحدث أو أمر بإحداث شبكة مواصلات دون الحصول على الترخيص المنصوص عليه في المادة الثانية أعلاه أو استمر في استغلال شبكته خرقا المقرر التوقيف أو سحب الترخيص.

وكل من قدم أو أمر بتقديم خدمة مواصلات دون الحصول على الترخيص المنصوص عليه في المادة الثانية أعلاه أو استمر في تقديم الخدمة بعد صدور مقرر توقيف أو سحب الترخيص.

وكل من أحدث الشبكات أو التجهيزات الراديو كهربائية المشار إليها في المادة 19 أعلاه مخالفا بذلك ..."

[4]– القانون رقم 02.99 الصادر بتنفيذه الظهير الشريف رقم 1.00.222 الصادر في 2 ربيع الأول 1412 (5 يونيو 2000) المغير والمتمم بموجبه مدونة الجمارك والضرائب غير المباشرة المصادق عليها بالظهير الشريف بمثابة قانون رقم 1.77.339 بتاريخ 25 من شوال 1397 (9 أكتوبر 1977)، الجريدة الرسمية عدد 4804 بتاريخ 12 ربيع الأول 1421 (15 يونيو 2000)، ص 1652.

ينص البند 7 من الفصل 281 من مدونة الجمارك والضرائب غير المباشرة على أنه: "تشمل الجنح الجمركية من الطبقة الثانية كل عمل أو مناورة تنجز بطرق معلوماتية أو الكترونية، ترمي إلى حذف معلومات أو برامج النظام المعلوماتي للإدارة أو تغييرها أو إضافة معلومات أو برامج إلى هذا النظام، عندما ينجم عن هذه الأعمال أو المشاورات التملص من رسم أو مكس أو الحصول بصفة غير قانونية على امتياز معين".

- **القانون 03.03 المتعلق بمكافحة الإرهاب[1]**

تنبه المشرع المغربي إلى خطورة الاجرام المعلوماتي وخصوصا جرائم الارهاب الرقمي وتأثيره على استقرار وأمن المجتمع المغربي، الأمر الذي دفعه إلى صدور قانون رقم 03.03 المتعلق بالإرهاب الذي يعد أول نص تشريعي مغربي يشير بشكل صريح إلى الإجرام المعلوماتي كوسيلة للقيام بأفعال إرهابية لها علاقة عمدية بمشروع فردي أو جماعي يهدف إلى زعزعة الاستقرار والمس بأمن النظام العام المغربي، عن طريق استعمال وسائل التخويف والترهيب والعنف، وهذا ما أكده الفصل 1.218 من نفس القانون إذ حدد بعض الأفعال تعد ارهابية ومجرمة على سبيل الحصر، ومن بينها الارهاب المعلوماتي أي الجرائم المتعلقة بنظم المعالجة الآلية للمعطيات.

- **القانون 103.13 المتعلق بالعنف ضد النساء[2]**

تطرق هذا القانون لجميع أنواع العنف الموجه ضد النساء بما في ذلك العنف الرقمي أو الالكترونية، وذلك صرح الفصل 448.1 منه إلى حماية الحياة الخاص للنساء في المجال المعلوماتي، وتجريم كل الأفعال التي تؤدي الاضرار بها وبصمتها كامرأة، وخصوصا تجريم أفعال التقاط أو تسجيل أو توزيع أقوال أو معلومات بطريقة غير مشروعة، بالإضافة إلى التصدي إلى كل الجرائم ذات الطابع الجنسي الموجه ضد المرأة وعلى رأسهم جريمة التحرش الجنسي عبر الوسائل الالكترونية.

2. الإطار المؤسساتي للأمن المعلوماتي

[1]– ظهير شريف رقم 1.03.140 صادر في 26 من ربيع الأول 1424 (28 ماي 2003) بتنفيذ القانون 03.03 المتعلق بمكافحة الإرهاب، الجريدة الرسمية عدد 5112 بتاريخ 27 ربيع الأول 1424 (29 ماي 2003)، ص 1755.

[2]– ظهير شريف رقم 1.18.19 صادر في 5 جمادى الآخرة 1439 الموافق لـ 22 فبراير 2018، بتنفيذ القانون رقم 103.13 المتعلق بمحاربة العنف ضد النساء، المنشور في الجريدة الرسمية عدد 6655 بتاريخ 23 جمادى الآخرة 1439 الموافق لـ 12 مارس 2018، ص 1449.

يتكون الإطار المؤسساتي للأمن المعلوماتي في المغرب من منظومة تضم إدارة الدفاع الوطني كجهة وصية، إلى جانب المديرية العامة لأمن نظم المعلومات، واللجنة الاستراتيجية للأمن السيبراني، وهيئات أخرى متخصصة في الحوكمة والتنسيق التقني.

1.2: المديرية العامة لأمن نظم المعلومات

تعد السلطة الوطنية المسؤولة عن تنفيذ استراتيجية الدولة في مجال الأمن السيبراني، وتتكلف بـ:

- تنسيق إعداد وتنفيذ الاستراتيجية الوطنية للأمن السيبراني؛
- تحديد وتطبيق تدابير حماية نظم المعلومات؛
- تقديم اقتراحات لمواجهة الأزمات والتهديدات السيبرانية؛
- مراقبة تطبيق القوانين في المجال؛
- تقديم الدعم والمواكبة للهيئات الحيوية لتعزيز أمنها المعلوماتي؛
- تشجيع البحث العلمي والتقني في مجال الأمن السيبراني.

2.2: اللجنة الاستراتيجية للأمن السيبراني

تم إنشاء هذه اللجنة بموجب القانون رقم 05.20، وتعتبر الهيئة العليا المشرفة على التوجهات الوطنية للأمن السيبراني، وتضطلع بـ:

- وضع التوجهات الاستراتيجية للدولة في المجال وضمان صمود البنى التحتية الحيوية؛
- تقييم سنوي لأنشطة المديرية العامة لأمن نظم المعلومات؛
- تتبع عمل لجنة إدارة الأزمات السيبرانية الجسيمة؛
- تشجيع البحث العلمي وبرامج التوعية وبناء القدرات في الأمن السيبراني؛
- إبداء الرأي في مشاريع القوانين ذات الصلة.

البحث الثاني: الجريمة الالكترونية وتصدع الأمن المعلوماتي

أنتج التعامل مع الإنترنت وما يوفره من زخم معلوماتي وقدرات اتصال وخدمات، حالة من الارتباط، يصعب على الفرد والمؤسسات الاستغناء عنها، حيث أضحت الانترنت جزءا من الحياة اليومية للأشخاص والهيئات، كما أفرز هذا التعامل وهذا الارتباط كما هائلا من البيانات والمعلومات، تباينت في طبيعتها بين العام والشخصي، العلني والسري، برزت ظواهر سلبية في التعامل مع هذه الشبكات، أبانت اضرارا بمصالح الأشخاص والهيئات والدول عن طريق اختراق النظم المعلوماتية **(أولا)** باستخدام الأدوات التخريبية للنظم المعلوماتية **(ثانيا)**.

أولا: اختراق النظم المعلوماتية

سنحاول تحديد مفهوم الاختراق **(1)**، ثم الوقوف على أهم الخصائص المميزة له **(2)**.

1. مفهوم اختراق النظم المعلوماتية

إن البحث عن مفهوم اختراق النظم المعلوماتية يمكن أن يقودنا إلى مسارين أولهما أن الاختراق المعلوماتي هو عملية تقنية حيث يحمل مفهوم توظيف المعرفة العلمية السائدة في ميادين تقنية الحاسوب والمعلوماتية للوصول إلى معلومات لا تقع في حدود المتاح والمسموح به[1].

والمسار الثاني باعتباره جريمة حيث يبين التنقيب في النصوص القانونية التي تعالج جرائم الحاسوب، ويمكن أن يعزى هذا الأمر إلى التغيرات المتسارعة التي تسري في ميادين تقنيات المعلوماتية[2].

وبشكل عام، تتجسد الجريمة الإلكترونية في الفضاء المعلوماتي عبر آليات الاختراق التي تمنح الفاعل القدرة على تجاوز حدود الأنظمة الإلكترونية المألوفة والوصول إلى ما هو غير مسموح به .وتضم أنشطة الاختراق طيفًا واسعًا من الأفعال غير المشروعة من أبرزها: ـ

- استغلال أو سرقة البرمجيات دون الحصول على إذن مسبق؛
- الولوج غير المشروع إلى بيئة الحاسوب أو شبكات الاتصالات بأنواعها بهدف استغلال مواردها المتوفرة فيها دون وجه حق؛
- تغيير أو حذف أو تعديل أو نقل أو نشر ملفات ومعطيات تخص الغير من غير إذن صاحبها، مما يلحق ضررًا بحقوقه أو مصالحه؛
- اختراق وكسر الشيفرات البرمجية للبرمجيات التطبيقية المحمية، أو الملفات المشفرة بغرض الحاق الضرر بالغير؛
- إدخال الفايروسات أو برمجيات الخبيثة بهدف الإخلال بأدائها، أو إفساد الموارد المعلوماتية وشل خدماتها؛
- تنفيذ أنشطة تخريبية ذات طابع إرهابي عبر الفضاء الإلكتروني، كاستهداف البنى التحتية للدول أو المؤسسات أو الأفراد باستخدام الوسائل المعلوماتية لإشاعة الخوف والفوضى؛

[1]– جعيجع، عبد الوهاب (2017): الأمن المعلوماتي وإدارة العلاقات الدولية، منشورات دار الخلدونية، الطبعة الأولى، سنة 2017، ص 116.

[2]. المصدر السابق، ص 116.

2. خصائص بيئة الاختراق المعلوماتي

تعد ظاهرة الاختراق الرقمي من المواضع ذات الأهمية بسبب الأدوات الخطيرة المستخدمة وحجم الأضرار الممكنة وتأثيرها على الفضاء المعلوماتي ككل، وتبرز في البيئة القابلة للاختراق خصائص أساسية تسهل الهجمات نذكر منها:

- **الهشاشة:** تحتوي نظم المعلومات على ثغرات بنيوية تسمح للمخترقين بالتسلل وإحداث أضرار متنوعة، وممارسات عمليات تخريب على مستويات مختلفة.
- **غياب الحدود:** إن طبيعة الحدود اللامكانية للجرائم الالكترونية وغياب الهوية الرقمية تساهم بشكل كبير في إخفاء هوية المهاجمين مما يؤدي الزيادة في بنية الاختراق المعلوماتي؛
- **السهولة وتدني التكلفة:** توافر أدوات وهياكل برمجية على الإنترنت يتيح للمخترقين تنفيذ هجمات دقيقة وبموارد محدودة، الأمر الذي يساعدهم على فك الشيفرات باستعمال وسائل أقل كلفة دون حاجة إلى مصادر تمويلية ضخمة؛
- **تراكم الخبرة المعلوماتية:** تعد عناصر الخبرة التي يتوفر عليها شريحة واسعة من مستخدمي الحواسيب، سببا رئيسيا وعاملا حاسما في زيادة بالاهتمام بالاختراق المعلوماتي، نظرا لتوفر على كم هائل من المعلومات التي تساعد في تطوير مهارات الاختراق؛
- **انعدام المخاطرة المباشرة:** يتميز الاختراق المعلوماتي بكونه نشاطًا يمكن تنفيذه عن بعد من وراء شاشة الحاسوب، دون أي احتكاك مادي بالضحية .هذا يعني أن المخترق لا يعرّض نفسه لخطر مباشر كالذي يواجهه المجرم التقليدي في مسرح الجريمة، الأمر الذي يشجع الكثيرين على الانخراط في هذه الأفعال الإجرامية لاعتقادهم بصعوبة تعقّبهم أو مساءلتهم.

هذه العوامل وأخرى باتت تشكل بيئة خصبة لنمو الاختراقات الرقمية في الفضاء المعلوماتي، لتكون بديلا سهلا ومفضلا عن عمليات التجسس التقليدية[1].

[1]. مقبل، ريهام (2015): Cyber Intelligence كيف يمكن أن تمارس الدول نفوذها في العلاقات الدولية، دورية مفاهيم المستقبل، تصدر عن مركز المستقبل للأبحاث والدراسات المتقدمة، العدد 6، يناير، ص 16.

ثانيا: الأدوات التخريبية للنظم المعلوماتية

تتعدد طرق وأدوات اختراق نظم المعلومات وتتشعب، حيث يمكن أن يستخدم مجرم اختراق نظم المعلومات مجموعة من الأدوات للوصول إلى هدفه، إذ يمكن التمييز بين ثلاثة أنواع من هذه الأدوات، حيث تتمثل الأولى بالوسائل المادية وإمكانية استخدامها في الاختراق وجمع المعلومات **(1)**، والثانية تتعلق بأنظمة الحاسوب وتطبيقاتها **(2)**، والثالثة تعتمد على الاستخدام الكثيف والمتكرر لوسائل التواصل الاجتماعي **(3)**.

1. الأدوات المتعلقة بالوسائل المادية

تتمثل الأدوات المتعلقة بالوسائل المادية في تحديد الموقع الجغرافي أو المكاني، والثانية في عدسات وميكروفونات الأجهزة الإلكترونية.

1.1: تحديد الموقع الجغرافي

يوجد جهاز تحديد المواقع (GPS) في عدة أشكال[1]، أولها في صورته الحرة جهاز (Garmi)، أو المدمج على المركبات من سيارات وشاحنات أو المدمج على الهواتف النقالة والألواح الإلكترونية تربط أداة تحديد المواقع بالهوية الإلكترونية للمستخدم التي في الغالب تكون عبر البريد الإلكتروني أو رقم الهاتف، حيث يتم تجميع كم هائل من المعلومات حول المستخدم ومساراته وأماكن وجوده وترددات...

كما تستخدم الهواتف النقالة بكل أجيالها المعروفة لتعقب موقع المتصل حتى عندما لا يكون الهاتف في وضع التشغيل ومن دون تشغيل أداة تحديد المواقع (GPS) حيث يتم تحديد الموقع عبر قوة الإشارة الهوائيات (Antennas) المتصلة بالهاتف النقال، وبذلك يتم جمع بيانات حول المستخدم وحركاته ومساراته وأرقام هواتف الاتصالات والأشخاص الذين له صلة بهم أو يلتقيهم وحتى مدة اللقاءات وعددها، إلى آخره من البيانات المتعلقة بالحركة والموقع[2].

2.1: عدسات وميكروفونات الأجهزة الإلكترونية: إذ تستخدم عدسات وميكروفونات الأجهزة الإلكترونية المنتشرة من كاميرات مراقبة في الأماكن العامة، وهواتف نقالة شخصية وأجهزة حواسيب محمولة وأجهزة تلفزيون وأجهزة ألعاب الفيديو إلى غيرها من الأجهزة الإلكترونية المدججة بالعدسات والميكروفونات، تستخدم في تجميع الصور والفيديوهات وتسجيل الأحاديث والمكالمات

[1]– جعيجع، عبد الوهاب، الأمن المعلوماتي وإدارة العلاقات الدولية، م س، ص 120.

[2]– عبد الصبور، عبد الحي صباح، استخدام القوة الالكترونية في التفاعلات الدولية، مقال منشور على الموقع الالكتروني الخاص بالمعهد المصري للدراسات السياسية والاستراتيجية http://www.eipss-eg.org تم الاطلاع عليه بتاريخ 2025/10/04 على الساعة 23:00.

وبلورة صورة شاملة عن بيئة المستخدم، وكذا تجميع كم هائل من البيانات الصورية والصوتية التي تخضع للتحليل والتفكيك فيما بعد.

3. الأدوات المتعلقة باستخدام البرامج والتطبيقات

ستحاول أن نسرد أهم الأدوات ذات الصلة المباشرة بمحرك البحث وعمل المستخدم، وهي:

الأداة الأولى: الكعك المعلوماتي (Cookies)

بصورة عامة تتألف الكعك من مجموعة من الملفات النصية الصغيرة التي يخزنها خادم الويب تلقائيًا على القرص الصلب لحاسوب المستخدم عند زيارته لموقع معين .تحتوي هذه الملفات على مجموعة من البيانات التفصيلية حول تفضيلات المستخدم، مثل اللغة المفضلة وأنماط العرض ومعلومات دخوله وآثار تصفحه . وتمكن هذه المعلومات المواقعَ لاحقا من تتبع نشاط المستخدم وفهم سلوكه الرقمي، كما قد يتم تعديلها أو استثمارها لاحقا لأغراض إعلانية أو تجسسية دون علم المستخدم[1].

الأداة الثانية: برمجيات المراقبة والتلصص (Spyware)

تعتبر هذه البرمجيات من البرامج الخبيثة التي تُزرع خلسة في جهاز الكمبيوتر أو الهاتف المستهدف بهدف مراقبة كل ما يحدث فيه وجمع المعلومات دون إثارة انتباه الضحية .تقوم هذه البرمجيات عادة بتسجيل جميع ضغطات لوحة المفاتيح وما يكتبه المستخدم في الزمن الحقيقي، ولا سيما الكلمات المفتاحية التي يستعملها في محركات البحث أو إدخال بياناته السرية. ثم ترسل هذه البيانات المجمّعة إلى جهة خارجية مهاجمة .وغالبا ما تترسخ برمجيات التجسس عبر تثبيت ملفات خبيثة ضمن نظام التشغيل يصعب اكتشافها، لتبدأ برصد كافة الأنشطة على الجهاز المستهدف وإرسال التقارير للمخترق بشكل مستمر[2].

وللإشارة تعمل هذه البرمجيات بإيداع ملفات في الحاسوب الشخصي، ونقل جميع الأنشطة المعلوماتية التي تمارس في الحاسوب الشخصي، وطبيعة الأنساق المعرفية المتفاعل معها أثناء النشاط اليومي.

[1]– جعيجع، عبد الوهاب، الأمن المعلوماتي وإدارة العلاقات الدولية، مرجع سابق، ص 123 بتصرف.

[2]– Joseph S, Nye, "THE Future of Power ", meetings with Jack Landman Goldsmith at Bulletin of the American Academy, Vol, 64, No 3, Spring 201, 21 Marsh 2017.

الأداة الثالثة: محلل المرور المعلوماتي (Traffic Analyzer)

محللات المرور هي أدوات برمجية متقدمة تقوم بمراقبة وتحليل حركة البيانات والاتصالات عبر الشبكات الإلكترونية .تعمل هذه المحللات على تتبع استعلامات محركات البحث المستخدمة من قِبل الجمهور ورصد حجم الزيارات إلى مواقع الويب المختلفة. ومن خلال هذه المعطيات يمكن تحديد أكثر المواقع شعبيةً وجذبًا للمستخدمين وأهم المفاتيح البحثية التي تقود إليهم، بما يساعد الشركات مثلًا على تقييم نجاح صفحاتها أو حملاتها التسويقية الرقمية.

3: الأدوات المتعلقة باستخدام وسائل التواصل الاجتماعي

تتباين وتتعد طرق الاختراق المعلوماتي والحصول على المعلومات لارتباطها بالتطور التقني المتسارع، لذلك يتم تصنيفها إلى ثلاث طرق حسب التقنيات المستخدمة وهي:

1.3. رصد أنظمة الالتقاط الهوائية

تتم هذه العملية بواسطة إنشاء محطات تعتمد على هوائيات التقاط واعتراض لكل ما يحمله الهواء من ذبذبات وما يمر عبره من اتصالات، وما تقوم به الأقمار الاصطناعية من ربط ونقل للبيانات وهي من بين الطرق الأولى التي اعتمدت في عمليات التجسس الإلكترونية، ولعل أهم مشروع قام على استخدام هذه الطريقة هو برنامج إشلون.

2.3. استغلال نقاط ضعف تقنية في الأنظمة والشبكات

تتم بواسطة مخترقين ذوي كفاءة تقنية عالية، تمكنهم من تتبع نقاط الضعف في الأنظمة المعلوماتية وتحقيق الاختراق المطلوب وتتعد أهداف الاختراق في هذا النوع لتكون سرقة المعلومات هي أحد أهدافه.

3.3. استغلال أحد المستخدمين

تتم هذه العملية باستغلال أحد أفراد المؤسسات الأمنية أو مستخدمي شركات المعلوماتية الذين تمكنهم وظائفهم من الاطلاع على المعلومات وإمكانية حيازتها حيث تعد من أسهل طرق الاختراق الرقمي وأكثرها نجاعة وتتم بتواطؤ شركات المعلوماتية، وهي الحالات التي تعقد فيها مخابرات الدول صفقات مع مستضيفي قواعد البيانات وتمكينهم من حيازة نسخ عن البيانات والمعلومات التي تقع تحت طائلة معاملاتهم المعلوماتية تسمح هذه الطريقة بحيازة كم هائل من المعلومات المتكاملة والدقيقة وفي وقت قياسي.

كما توجد طرق أخرى أكثر خطورة يتم استخدامها لاختراق الشبكات والأنظمة بصورة عامة، حيث تعد أهم هذه الطرق:

- **مدفع:** يصد بهذه الأداة الترددات الراديوية أو بنادق الترددات الإشعاعية العالية حيث تقوم بتوجيه عاصفة من الإشارات الراديوية، على أهداف رقمية منتقاة الغرض هو إضعافها، أو إيقافها عن العمل، كما يمتلك هذا المدفع المعلوماتي القدرة على إطلاق قذائفه الراديوية التي تمثل حمولة كهرومغناطيسية على حاسوب، أو شبكة من الحواسيب يؤدي إلى توقفها كليا عن العمل، ما ينجم عنه حصول حالة رفض الخدمة، فتتوقف الشبكة المعلوماتية عن ممارسة دورها ووظيفتها في الربط والمعالجة[1].
- **القذيفة الكهرومغناطيسية:** وتسمى بقذيفة تحويل الذبذبات الكهرومغناطيسية (Electro Mégantic Pulse Transformer Bomba)، إذ تعمل بطريقة مقاربة لمدفع الترددات الراديوية، إلا أن طاقتها التدميرية تفوق بأضعاف التأثيرات المحتملة لاستخدام مدفع.

وبشكل عام فإن أهم الآلات التي تتعرض لهذه الهجمات هي الحواسيب، والأجهزة المرتبطة بها، وكذلك عناصر أشباه الموصلات المستخدمة في شبكات المعلومات، نظم التنبيه والاتصالات الداخلية، معدات أجهزة الهاتف، المراسلات والمستقبلات، ونظم التحكم الآلي بمختلف أشكالها[2].

- **الفيروسات:** وهي عبارة عن برنامج يقوم بلصق محتوياته على قائمة الأوامر التنفيذية للبرامج، أو محتويات الملفات الموجودة على وسائط خزن البيانات في الحاسوب، ويمتلك هذا البرنامج قدرة ذاتية على التكاثر والانتشار السريع في نظام التشغيل، فيورثه، بطئا في الأداء، أو تدمير بعض معدات الحاسوب، أو القيام بمهام اختراق مبرمج لها. وهناك عدة أنواع للفيروسات منها فيروسات قطاع التشغيل (Boot Sector)، فيروسات الماكر، والفيروسات الطفيلية، وفيروسات البرامج.
- **الديدان:** عبارة عن برنامج حاسوبي يقارب في عمله الفايروس غير أنه مستقل ولا يعتمد على البرامج الأخرى، له قدرة على الاستنساخ والتكاثر والانتقال والانتشار عبر شبكات المعلومات بصورة ذاتية، ثم يؤدي وظيفة الاختراق الموكلة إليه سواء تدمير المعلومات، أم التجسس ونقل المعلومات، أم تعطيل الخدمة[3].

---

[1]– حشود، نور الدين (2011): الاستراتيجية الأمنية الأمريكية تجاه الجزائر بعد 11 سبتمبر، م س، ص 76.

[2]. القحطاني، منصور بن سعيد (2008): مهددات الأمن المعلوماتي وسبل مواجهتها، رسالة مقدمة استكمالا لمتطلبات الحصول على درجة الماجستير في العلوم الإدارية، كلية الدراسات العليا، قسم العلوم الإدارية، جامعة نايف العربية للعلوم الأمنية، السعودية، ص 67 و69.

[3]– القحطاني، منصور بن سعيد، مرجع سابق، ص 69.

- **حصان طروادة:** هذا البرنامج يظهر بأنه مفيد، غير أنه في الحقيقة لا يعدو كونه مؤذيا يمارس عمليات تخريب معلوماتية موجهة وفق توقيت زمني أو منطقي، كما له القدرة على تخريب النظام عن بعد بواسطة شبكة الإنترنت ثم السيطرة على الحاسوب واحتكار وظائفه[1].

كما تعد أحصنة طروادة من الأدوات الفاعلة في ميدان الاختراق المعلوماتي شبيهة جدا بالديدان أو بالفيروسات، لكنها تختلف عنها في الهدف، فالديدان أو الفيروسات تقوم بمسح أو تدمير المعلومات من البرامج التطبيقية، كبرامج المحاسبة، وقواعد المعلومات، وبمقدورها التكاثر حتى تملأ الذاكرة، أما أحصنة طروادة لا تدمر، ولا تقوم بمسح المعلومات، ولكنها تتجسس وتقوم بجمع المعلومات والبيانات، وتحولها إلى مرسلها أي للشخص الذي أرسل حصان طروادة وتركز على المجال المالي بالدرجة الأولى، و توجد أكثر من خاصية برمجية تتصف بها النسخ المتوفرة في ميدان المعلوماتية من قبيل هذه الأداة[2].

الخاتمة:

في الختام يتضح أن العالم الرقمي، رغم ما يقدمه من مزايا هائلة في مجالات التواصل والمعرفة والاقتصاد، أصبح بيئة خصبة لظهور أنماط جديدة من الجرائم تمس مباشرة أمن الأفراد والمؤسسات والدول فالجريمة الإلكترونية لم تعد مجرد أفعال معزولة، بل باتت تشكل تحديا استراتيجيا يتطلب وعيا قانونيا وتقنيا متكاملا، قوامه التعاون الدولي، والتأطير التشريعي الفعال، وتطوير منظومات الحماية السيبرانية.

لقد أثبتت التجربة أن الأمن المعلوماتي هو حجر الزاوية في حماية البنى التحتية الحيوية وضمان استقرار المعاملات الرقمية، وهو ما يفرض على الحكومات والهيئات المختصة تبني سياسات استباقية تقوم على الرصد، والتحليل، والتكوين، وتحديث التشريعات بما يتلاءم مع سرعة تطور التقنيات الحديثة، كما أن مسؤولية الأفراد لا تقل أهمية، إذ إن تعزيز ثقافة الأمن الرقمي والسلوك المسؤول على الشبكة يعد خط الدفاع الأول ضد مختلف التهديدات الإلكترونية.

[1]– قريب، بلال (2011): السياسة الأمنية للاتحاد الأوربي من منظور أقطابه، التحديات والرهانات، رسالة لنيل شهادة الماجستير في العلوم السياسية، كلية الحقوق والعلوم السياسية، قسم العلوم السياسية، جامعة باتنة، الجزائر، ص 98.

[2]– الرزو، حسن مظفر (2004): الأمن المعلوماتي: معالجة قانونية أولية، مجلة الأمن والقانون، أكاديمية شرطة دبي، القيادة العامة لشرطة دبي، السنة 12، العدد 1، يناير، ص 88 وما بعدها.

في ضوء ما سبق من تحليل لتأثير الجريمة الإلكترونية على الأمن المعلوماتي، يمكن اقتراح مجموعة من التوصيات الضرورية لتعزيز المنظومة التشريعية المغربية في هذا المجال، بهدف تحقيق حماية فعالة وشاملة للفضاء الرقمي، ومن أبرزها ما يلي:

- تعزيز التنسيق بين النصوص القانونية ذات الصلة بالأمن السيبراني، كالقانون رقم 05.20 المتعلق بالأمن السيبراني، والقانون رقم 07.03المتعلق بالمس بنظم المعالجة الآلية للمعطيات، من أجل تحقيق الانسجام التشريعي وتفادي التكرار أو التناقض في المقتضيات.
- تعزيز صلاحيات الهيئة الوطنية للأمن السيبراني، وتمكينها من آليات التدخل الفوري، والمراقبة، والتنسيق مع القطاعين العام والخاص في مجال الوقاية من الهجمات الإلكترونية.
- تطوير آليات التعاون القضائي الدولي، من خلال إبرام اتفاقيات ثنائية ومتعددة الأطراف لتبادل المعلومات والأدلة الرقمية، وتسهيل تسليم المجرمين الإلكترونيين.
- إدماج الثقافة السيبرانية في المنظومة التربوية والتكوينية، عبر مقررات تعليمية وتدريبية ترفع من وعي الأفراد والمؤسسات بمخاطر الفضاء الرقمي وأساليب الوقاية منه.
- تحديث الإطار القانوني الوطني بشكل دوري لمواكبة التطورات التقنية السريعة، خصوصًا ما يتعلق بجرائم الذكاء الاصطناعي، والتزييف العميق، والجرائم العابرة للحدود.

قائمة المراجع والمصادر:

- بابكر، إسماعيل، خصائص الأمن السيبراني، مقال منشور على الموقع الالكتروني https://alwatannewssd.com/56117/
- بنسليمان، عبد السلام (2020): الإجرام المعلوماتي في التشريع المغربي، دراسة نقدية في ضوء آراء الفقه وأحكام القضاء، ط2، الرباط: مكتبة دار الأمان.
- بوعيدة، عبد الرحيم؛ نعمان، ضياء علي أحمد (2009): موسوعة التشريعات الالكترونية المدنية والجنائية، التشريع المغربي والعربي والفرنسي الاتفاقيات العربية والأوربية والدولية، ط1، مراكش: المطبعة والوراقة الوطنية.
- جعيجع، عبد الوهاب (2017): الأمن المعلوماتي وإدارة العلاقات الدولية، ط1، منشورات دار الخلدونية.
- حاجي، صليحة، الآليات القانونية لتكريس الأمن المعلوماتي، مقال منشور في مجلة مغرب القانون في الموقع الالكتروني التالي https://www.maroclaw.com

- حجازي، عبد الفتاح بيومي (2003): مقدمة في التجارة الالكترونية العربية الكتاب الثاني النظام القانوني للتجارة الالكترونية في دولة الامارات العربية المتحدة، دار الفكر الجامعي.
- حشود، نور الدين (2015): الاستراتيجية الأمنية الأمريكية تجاه الجزائر بعد 11 سبتمبر 2011، أطروحة لنيل الدكتوراه في العلوم السياسية والعلاقات الدولية، كلية الحقوق والعلوم السياسية، قسم العلوم السياسية، جامعة باتنة الجزائر.
- الرزو، حسن مظفر (2004): الأمن المعلوماتي: معالجة قانونية أولية، مجلة الأمن والقانون، أكاديمية شرطة دبي، القيادة العامة لشرطة دبي، السنة الثانية عشرة، العدد 1، يناير.
- ريهام، مقبل (2015): Cyber Intelligence كيف يمكن أن تمارس الدول نفوذها في العلاقات الدولية، دورية مفاهيم المستقبل، تصدر عن مركز المستقبل للأبحاث والدراسات المتقدمة، العدد 6، يناير.
- السحيمي، أمين؛ وبوفرعة، عبد المجيد (2024): الإطار القانوني المغربي للجرائم الالكترونية بين التشريع الوطني والاتفاقيات الدولية، مجلة البحث في العلوم الإنسانية والمعرفية، المجلد 1، العدد 6، السنة الأولى شتنبر.
- صدق، دلال؛ وفتال، حميد ناصر (2008): أمن المعلوماتي، هيئة التعليم التقني، الردن: دار اليازوردي العلمية للنشر والتوزيع.
- عبد الصبور، عبد الحي صباح استخدام القوة الالكترونية في التفاعلات الدولية، مقال منشور على الموقع الالكتروني الخاص بالمعهد المصري للدراسات السياسية والاستراتيجية http://www.eipss-eg.org
- القحطاني، منصور بن سعيد (2008): مهددات الأمن المعلوماتي وسبل مواجهتها، رسالة مقدمة استكمالا لمتطلبات الحصول على درجة الماجستير في العلوم الإدارية، كلية الدراسات العليا، قسم العلوم الإدارية، جامعة نايف العربية للعلوم الأمنية، السعودية.
- قريب، بلال (2011): السياسة الأمنية للاتحاد الأوربي من منظور أقطابه، التحديات والرهانات، رسالة لنيل شهادة الماجستير في العلوم السياسية، كلية الحقوق والعلوم السياسية، قسم العلوم السياسية، جامعة باتنة، الجزائر.
- مقناني، صبرينة (2020): تأثير الجريمة الالكترونية على المعلومات الرقمية، المجلة الجزائرية للأبحاث والدراسات، المجلد الثالث، العدد 9.

- Joseph S, Nye. (2017). "THE Future of Power," meetings with Jack Landman Goldsmith at Bulletin of the American Academy, Vol, 64, No 3, Spring 201, accessible at 21 Marsh.
- Mohamed Ourgane. (2005). La criminalité informatique au regard du droit pénal marocain, centre marocain des études juridiques, Hommage professeur JallalEssaid. Tome 1.