ضمانات حماية المستهلك بين مخاطر التحول الرقمي وتعزيز الأمن السيبراني

الدكتورة منال منصور
أستاذة باحثة في القانون
بجامعة عبد المالك السعدي

أميمة بوعزة
باحثة في القانون بجامعة عبد المالك السعدي

الملخص

تتناول هذه الدراسة دور آليات الأمن السيبراني في تعزيز الثقة الرقمية للمستهلك الإلكتروني، وحمايته من المخاطر المتزايدة في ظل التحول الرقمي المتسارع الذي فرضته العولمة التكنولوجية وعمقته جائحة كوفيد-19، وتطرح الدراسة إشكالية رئيسية تتمثل في مدى فعالية ونجاعة آليات الأمن السيبراني (التشريعية، المؤسساتية، والدولية) في توفير حماية استباقية متكاملة للمستهلك الرقمي وتحقيق الثقة الرقمية.

ولمعالجة هذه الإشكالية، تم تقسيم البحث إلى مبحثين؛ خصص **المبحث الأول** لرصد وتحليل المخاطر السيبرانية المحيطة بالمستهلك، والتي تنقسم إلى اعتداءات تمس المعطيات الشخصية، وتهديدات تطال وسائل الأداء الإلكتروني، بينما تطرق **المبحث الثاني** إلى تقييم الآليات المعتمدة لتعزيز هذه الثقة، بدءا بالترسانة التشريعية المغربية، مرورا بالدور المؤسساتي الفاعل لهيئات وطنية كاللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي (CNDP) والمديرية العامة لأمن نظم المعلومات(DGSSI) ، وصولا إلى آليات التعاون الدولي والاتفاقيات المصادق عليها.

وقد خلصت الدراسة إلى أن مقاربة المشرع المغربي انتقلت من الطابع العلاجي التقليدي والمشتت إلى مقاربة أمنية ودفاعية استباقية نوعية عبر القانون رقم 05.20، مؤكدة على أن تحقيق الثقة الرقمية الكاملة يستلزم تكاملا وثيقاً بين القوانين الوطنية، وتطوير البنية المؤسساتية، وتفعيل آليات التعاون الدولي العابر للحدود.

الكلمات المفتاحية :الأمن السيبراني؛ المستهلك الإلكتروني؛ الثقة الرقمية؛ المعطيات الشخصية؛ الجريمة السيبرانية.

Abstract

This study examines how cybersecurity mechanisms (legislative, institutional, and international) protect e-consumers and foster digital trust amid rapid digital transformation. Divided into two sections, the research first analyzes cyber threats targeting personal data and e-payment systems, and then evaluates trust-building frameworks, focusing on Moroccan legislation (primarily Law 05.20), key national institutions (such as CNDP and DGSSI), and international cooperation. The study concludes that Morocco has transitioned from a reactive model to a proactive, defensive cybersecurity paradigm under Law 05.20, emphasizing that robust digital trust requires integrated domestic laws, stronger institutions, and active cross-border cooperation.

Keywords: Cybersecurity; E-Consumer; Digital Trust; Personal Data; Cybercrime.

ساهم التطور التكنولوجي المتسارع في بروز الرقمنة كبديل حداثي لعولمة المبادلات بمختلف أشكالها، ممتدة إلى كافة القطاعات الحيوية، وقد تعزز هذا التحول بشكل ملموس إبان جائحة كوفيد-19 التي ألقت بظلالها على النشاط الاقتصادي؛ حيث فرضت تبني أدوات مرنة ذات بعد رقمي (مثل التجارة الإلكترونية، التسويق الإلكتروني، والاستثمار الإلكتروني...)، هذا التحول لم يقتصر على إحداث تغيير جذري في بنية العمل التجاري فحسب، بل جعل الانخراط في الاقتصاد الرقمي ضرورة ملحة للبقاء، متجاوزا كونه مجرد رؤية استراتيجية للتنمية.

ومن أجل جعل هذه المرحلة الانتقالية فرصة حقيقية للابتكار والنمو ببلادنا، كان لابد من الالتفات لعنصر المخاطرة والتهديد الذي قد يطال الفضاء المعلوماتي، وبالتالي العمل على تعزيز استراتيجية حقيقية للدفاع والأمن، تجعل المستهلك أو المتعامل عبر شبكة الأنترنيت أقل عرضة للمخاطر والجرائم الإلكترونية التي قد تهدد عمليته الإستهلاكية، بل وتساهم في

بناء ثقته الرقمية تجاه هذا الفضاء الغير محسوس عن طريق تعزيز أنظمة الأمن السيبراني Cyber security، باعتباره المجال الذي يؤطر مقاييس ومعايير الحماية المفترض اتخاذها في النظام المعلوماتي المهدد بالمخاطر المحيطة به.

وتعد آلية التشريع حجر الزاوية الذي ترتكز عليه حماية أمن نظم المعلومات وحقوق الفاعلين في الفضاء الرقمي، وفي هذا الصدد حاول المشرع المغربي مواكبة هذا التحول عبر حزمة من النصوص الحمائية، أبرزها القانون رقم 31.08 المتعلق بحماية المستهلك خاصة الباب الثاني من القسم الرابع الذي خصصه للعقود المبرمة عن بعد، والقانون رقم 53.05 المتعلق بالتبادل الإلكتروني للمعطيات القانونية، وكذا القانون رقم 09.08 الخاص بحماية المعطيات ذات الطابع الشخصي، كما ينضاف إلى هذا المجهود التشريعي، المقتضيات الزجرية لمجموعة القانون الجنائي المغربي، لا سيما تلك التي أدخلها القانون رقم 07.03 المتعلق بالجرائم المتعلقة بنظم المعالجة الآلية للمعطيات، والتي أفردت عقوبات رادعة لجرائم القرصنة، والاختراق، وإتلاف البيانات المعرقلة لسلامة المعاملات الرقمية.

بيد أن هذه الترسانة التشريعية المشتتة، أثبتت عدم كفايتها في توفير درع وقائي استباقي متكامل للمستهلك الإلكتروني؛ إذ إن طابعها العلاجي والبعد التقليدي لبعض نصوصها ظلا عاجزين عن ملاحقة التطور المتسارع والديناميكي للجرائم السيبرانية المعقدة العابرة للحدود، والتي لا تستهدف فقط الاعتداء على الأفراد، بل تهدد سلامة الأنظمة المعلوماتية ككل، مما جعل الحاجة ملحة لقوانين تتبنى مقاربة أمنية ودفاعية محضة تتجاوز القواعد التقليدية للحماية.

وتجسيدا لهذه المقاربة الأمنية الاستباقية، وسدا لهذا الفراغ التشريعي والتنظيمي، جاء القانون رقم 05.20 المتعلق بالأمن السيبراني كطفرة تشريعية نوعية، حيث قامت إدارة الدفاع الوطني، بعد الموافقة الملكية السامية، بإعداد القانون رقم 05.20 المتعلق بالأمن السيبراني[448]، والذي

[448]- القانون 02-05 المتعلق بالأمن السيبراني، الصادر بتنفيذ الظهير الشريف رقم 1.20.69 الصادر في 4 ذي الحجة 1441 (25) يوليو 2020). الجريدة الرسمية عدد 6904، بتاريخ 9 ذو الحجة 1441 (30 يوليو 2020) ص4160.

تم تعريفه في إطار المادة 02 منه على أنه: "مجموعة من التدابير والإجراءات ومفاهيم الأمن وطرق إدارة المخاطر والأعمال والتكوينات وأفضل الممارسات والتكنولوجيات التي تسمح لنظام معلومات ان يقاوم أحداثا مرتبطة بالفضاء السيبراني، من شأنها أن تمس بتوافر وسلامة وسرية المعطيات المخزنة والمعالجة أو المرسلة، والخدمات ذات الصلة التي يقدمها هذا النظام او تسمح بالولوج إليه"، الأمر الذي يبين استناد المفهوم على ثلاثة مبادئ أساسية، والمتمثلة اساسا في "السرية"[449]، "السلامة"[450]، "الإتاحة"[451]، والتي تعد تجسيدا للفلسفة التشريعية التي يقوم عليها هذا النظام.

[449]- يستهدف جزءا من الهجمات السيبرانية الحصول على معلومات حساسة أو ذات أهمية حيوية ، عن طريق الاطلاع أو التصنت أو الاستنساخ غير المشروع عند تخزينها أو معالجتها أو تحويلها، وبالتالي فإن إستراتيجية الأمن السيبراني الوطنية في الجزء المتعلق بالسرية منها يستهدف منع كشف معلومات من هذا النوع إلى الغير(أشخاص / حواسيب / برمجيات) غير مصرح بها.
- انظر:
- محمد الناصري، كمال بروحو: "رقمنة الإدارة القضائية المغربية". مقال منشور بسلسلة منشورات المركز العلمي للأبحاث والدراسات القانون والقضائية تحت عنوان "التوجه التشريعي للرقمنة والذكاء الاصطناعي". الطبعة الأولى 2014. ص 76

[450]- يستهدف جزء آخر من الهجمات السيبرانية كالاعتداء على معلومات حساسة، أو ذات أهمية حيوية عن طريق التغيير، أو الحذف، وبالتالي فإن استراتيجية الأمن السيبراني في الجزء المتعلق بالسلامة منها يستهدف منها تغيير أو تدمير معلومات من هذا النوع من قبل اشخاص غير مسموح لهم بذلك بشكل متعمد أو بشكل غير مقصود من أجل ضمان دقتها وموثوقيتها.
- محمد الناصري، كمال بروحو: مرجع سابق. ص 76 و ما بعدها

[451]- الاتاحة يستهدف جزء آخر من الهجمات السيبرانية، اي جعل نظم المعلومات التي تحوي معلومات حساسة أو ذات أهمية حيوية غير قابلة للاستغلال أو الاستعمال ، وبالتالي فإن استراتيجية الأمن السيبراني في الجزء المتعلق بالإتاحة منها يستهدف ضمان أن تظل المعلومات قابلة للاستعمال وأن نظل المعلومات والخدمات قابلة للوصول إلها.
- محمد الناصري، كمال بروحو: مرجع سابق. ص 76 و ما بعدها

وقد توج هذا المسار التشريعي الوطني بتعزيز الانخراط في آليات التعاون الدولي، والتي كان آخرها توقيع المملكة على معاهدة الأمم المتحدة لمكافحة الجرائم السيبرانية بتاريخ 25 أكتوبر 2025، مما يجسد التزام بلادنا الراسخ بدعم الجهود الدولية في هذا الميدان.

وتأسيسا على ما سبق، تطرح إشكالية رئيسية تتجلى في **مدى فعالية ونجاعة آليات الأمن السيبراني في حماية المستهلك الإلكتروني وتحقيق الثقة الرقمية؟**

وللإجابة على هذا السؤال سوف نعتمد التقسيم التالي:

المبحث الأول: المخاطر السيبرانية المحيطة بالمستهلك الالكتروني

المبحث الثاني: آليات الأمن السيبراني المعززة لثقة المستهلك الالكتروني

- **المبحث الأول: المخاطر السيبرانية المحيطة بالمستهلك الرقمي**

في ظل الاقتصاد الرقمي أصبحت مسألة حماية المستهلك الالكتروني ضرورة حتمية، على اعتبار أن المستهلك يكون أكثر عرضة للتلاعب بمصالحه وعرضة لمختلف الأخطار السيبرانية، والتي تتمثل في إجراء عمليات تخريبية تمس بصفة خاصة المعطيات الشخصية للمستهلك **(المطلب الاول)**، أو طرق الأداء الالكترونية التي يستعملها **(المطلب الثاني)**.

- **المطلب الأول: المساس بالمعطيات الشخصية للمستهلك**

تعد خصوصية البيانات أمرا بالغ الأهمية للمستهلكين، خاصة وأنها تعتبر أكثر عرضة للهجمات السيبرانية، سواء على مستوى استغلالها في الدراسات التي تقوم بها الشركات أو أن تكون عرضة للعديد من الزيارات العدائية والاختراقات **(الفقرة الأولى)**، كما يمكن أن تكون عرضة لاختراقات سيبرانية تتسم بالطابع الجرمي **(الفقرة الثانية)**.

الفقرة الأولى: الزيارات العدائية الماسة بالمعطيات الشخصية للمستهلك

تتجلى صور عملية الاختراق المعلوماتي لحرمة الحياة الخاصة للمستهلك الالكتروني عبر صور متعددة يمكن ان نرصد البعض منها:

- **أولا: انتحال الشخصية:**

تتخذ هذه الجريمة على الأنترنت إحدى الوجهين التاليين: انتحال شخصية الفرد وانتحال شخصية المواقع ".452

بخصوص جريمة انتحال شخصية الفرد، فتتجلى عبر استغلال أحد المترصدين لبيانات شخص ما على شبكة الانترنيت، من أجل الحصول على بطاقات بنكية مثلا، في حين أن انتحال شخصية المواقع فيعد الاختراق الخداعي أبرز صورها، إذ يجسد أخطر أنواع الاختراقات، حيث يتنكر أحد القراصنة في شخصية طرف يمثل مؤسسة مالية أو صاحب بطاقات بنكية يمكنه من خلالها تحصيل أموال من التجار والمستهلكين على حد سواء،453 عبر تحويلهم نحو الموقع المحتال، ثم طلب الرموز السرية منهم.454

وقد اتخذت هذه الظاهرة منحى متسارعا، وسجلت الإحصائيات أنها من أكثر الجرائم الإلكترونية ارتكابا، ففي فرنسا تعرض حوالي 210000 شخص في عام 2009 العمليات انتحال لهويتهم الشخصية، كما وصلت التكلفة الإجمالية المترتبة على عمليات انتحال الهوية الشخصية المباشرة وغير المباشرة في الولايات المتحدة الأمريكية في عام 2012 إلى ما يقارب 24 بليون دولار 455.

452- عبد الرحمان بن جيلالي: "جريمة الانتهاك الالكتروني لحرمة الحياة الخاصة دراسة مقارنة مجلة الفقه والقانون"، أبريل 2014 العدد 18.ص96

453- سمية مزغيش: "الجرائم الماسة بالأنظمة المعلوماتية،" رسالة لنيل شهادة الماستر في الحقوق جامعة محمد خيضر، كلية الحقوق والعلوم السياسية. بسكرة 2013-2014. ص28

454- صليحة حاجي:" الآليات القانونية لتكريس الأمن المعلوماتي"، مقال منشور بمجلة العلوم الجنائية 2015، العدد الثاني، ص 11

455-الصالحين محمد: العيش التنظيم القانوني لاستخدام البيانات الشخصية في الإعلام الجديد مجلة الحقوق، المجلد 13، العدد 2. ص: 19
على الموقع الإلكتروني
http://journal.uob.edu.bh/bitstream/handle/123456789/3353/1.pdf?sequence=1&isAllow

استطلاع الرأي قام به مركز كريدوك (Crédoc). حول "الفرنسيين في مواجهة الاستخدام الاحتيالي لوثائقهم الورقية ".

ثانيا: اقتناص الرسائل الإلكترونية (البريد الإلكتروني):

تعد إمكانية اعتراض البريد الالكتروني أحد أهم التهديدات السيبرانية التي تواجه المستهلك، إذ يمكن اعتراض الرسائل التي يتم تحميلها عبر الشبكة، وكشف مضمونها من خلالها الموزع وعبر برامج معينة قادرة على قراءة هذه الرسائل، التي يجب أن تمر من خلال الموزع ليتم تحميلها إلى الطرف الآخر، مما يفتح المجال أمام إمكانية قراءتها، وهو أمر يمس بخصوصية المعلومات.

ثالثا: الغش المعلوماتي:

الغش المعلوماتي هو مفهوم واسع، حيث تنضوي تحته العديد من الجرائم من قبيل السرقة، النصب، اختلاس مال الغير، وهي أفعال غالبا ما تتم بواسطة الحاسوب وعن بعد.[456]

ولعل أبرز مظهر من مظاهر الغش المعلوماتي نجد جرائم السطو على بطاقات الائتمان والتحويل الالكتروني غير المشروع للأموال، خاصة وأن جريمة الغش المعلوماتي قد نشأت مع شيوع أنظمة تحويل الأموال بطريقة الكترونية، حيث تزايدت بشكل ملحوظ قيمة الأموال المتداولة بهذه الطريقة، مما جعلها تصبح موضوعا لجرائم التحويل الإلكتروني غير المشروع.

رابعا: السلب بالقوة الالكترونية:

Les Français face à l'usage frauduleux de leurs documents papiers Connaissances attitudes et comportements .»

نتائجه منشورة على الموقع الإلكتروني:

https://protegezvotreidentite.files.wordpress.com/2009/11/credoc-usurpation-didentite-en-france.pdf الإحصائية الصادرة عن مكتب إحصاءات العدالة التابع لوزارة العدل الأمريكية في شهر ديسمبر 2013.

منشورة على الموقع الإلكتروني :

https://www.bjs.gov/content/pub/pdf/vit12.pdf 2

[456]- عبد الوهاب العبل:" الحماية الجنائية للحساب البنكي من الاعتداء المعلوماتي" رسالة لنيل شهادة الماستر في العلوم الجنائية، جامعة القاضي عياض، كلية العلوم القانونية والاقتصادية والاجتماعية بمراكش، 2008-2009، ص 63

تظهر بجلاء صورة هذا الفعل اللامشروع في استخدام الحاسوب من أجل التلاعب بالمعلومات، وذلك بإدخال بيانات زائفة من جانب المتحايل واختلاق معاملات أو فواتير ينبغي تسديد ثمنها، أما المستهلك فلن يتمكن من إثبات كونه غير مدين بالأداء لوجود فواتير معلوماتية، وهكذا يستغل المتحايل طرق الدفع الآلية للحصول على أموال غير شرعية على حساب هذا المستهلك.[457]

خامسا: التجسس على البيانات الشخصية:

إن تقديم المعطيات الشخصية من قبل المستهلكين أمر يتم عن طواعية تامة، فالمبادلات التجارية وإبرام العقود يتطلب أساسا من أجل تأكيد العملية تقديم هذه المعلومات، إلا أن انتهاك هذه البيانات يستعمل أحيانا دون موافقة المعني بالأمر ويمكن ان يتعدى ذلك الى بيعها للغير، كما قد يمتد ليحول معرفة أرقام حسابات المستهلك أو أرقام بطاقات الائتمان، والتي تشكل من حق أكثر البيانات الشخصية عرضة للاعتداء بالحصول عليها عن طريق الاحتيال أو من خلال سرقة أرقام هذه البطاقات، وذلك بعد فك الشفرات التي تحمي سريتها وكسر الحواجز الأمنية واستكشاف مواطن الضعف في الجهاز أو الشبكة، كما يمكن اكتشاف كلمة السر للمعتمدة من قبل المستهلك، مما يخلق معه النفاذ إلى نظم بيانات مهمة أخرى، كتغيير اسم المدفوع لأمره في الشبكات الالكترونية، أو المبالغ المحولة إلى حساب بنكي.

وتتم عملية المتابعة والتعقب باستخدام برامج وأدوات وأجهزة ذكية يتم استخدامها، مثل عملية التنقيب عن البيانات "Data mining" والكوكيز والنماذج الكترونية (الاستمارة) التي يقوم الزبناء بتعبئتها عبر الموقع، وهناك وسائل أخرى غير أخلاقية مثل (Web Bugis وSpay وغيرها).

457- هداية بوعزة: " نظام الدفع الالكتروني بين المزايا والمخاطر"، مقال منشور بمجلة الفقه والقانون، يوليوز 2014، العدد 21، ص 137

كما يمكن أن يتم الاعتماد على هذه البيانات من أجل دراسة سلوك المستهلكين لترسم العادات والميولات، والأذواق ونوايا الأشخاص.

فالموقع الاجتماعي "فيس بوك"[458] مثلا يقترح أنواعا متعددة من الإعلانات التجارية، وذلك عبر توجيه الإعلانات بحسب اهتمامات المستخدم، حيث أعلن في يونيو من عام 2014 عن هذه الخاصية الجديدة التي تعتمد على تقفي أثر المستخدم خارج الموقع لمعرفة العمليات التي يقوم بها من شراء على الإنترنت وكذلك نوعية المواقع التي يزورها واهتماماته بشكل عام بقصد توجيه إعلانات مناسبة له مبررا أن الأمر يتعلق بآلية لتوجيه الإعلانات بشكل أفضل للمستخدمين بحسب احتياجاتهم ولا يتعلق بأي تجسس أو تطفل، لكون المعلومات تظل سرية ولا يطلع عليها أحد.

ولا تقتصر عملية تخزين البيانات ومعالجتها على مواقع التواصل الاجتماعي، وإنما تتعداه إلى شركات الانترنت هذه الأخيرة التي تسعى إلى تخزين البيانات في بنوك المعلومات وتكوين قاعدة بيانات تفيد موضوعا محددا وتهدف لغرض معين، ومعالجتها بواسطة أجهزة الحاسبات الإلكترونية لإخراجها في صورة معلومات تفيد مستخدمين مختلفين في أغراض متعددة.[459]

الفقرة الثانية: الجرائم الماسة بالمعطيات الشخصية للمستهلكين

يمكن الحديث في مجال الجرائم الماسة بالمعطيات الشخصية للمستهلكين عن العديد من الصور الإجرامية، يمكننا ذكر بعضها:

---

[458]- يراهن فيس بوك على جعل موقعه ليس فقط موقعا للتواصل الاجتماعي وإنما كذلك منصة إعلانية ضخمة عن طريق الإعلانات الموجهة، إذ تعتبر الإعلانات واحدة من أهم مداخيل المواقع عموما، ومواقع التواصل الاجتماعي خصوصا، ومن الواضح أن " فيس بوك" يريد الاستفادة إلى أقصى حد من هذه الخاصية.

[459]- إسماعيل بلفقي، ناجية شموط: "الحق في خصوصية البيانات الشخصية بين التحديات التقنية ومطالب الحماية القانونية". مقال منشور بسلسلة منشورات المركز المغربي للأبحاث والدراسات القانونية والقضائية – التوجه التشريعي للرقمنة والذكاء الإصطناعي-الطبعة الأولى 2024. ص 92-91

أولا: جريمة الاعتداء على بيانات نظام المعالجة الالية

تعتبر جريمة الاعتداء على بيانات نظام المعالجة الآلية من الجرائم العمدية التي ترد على محل وموضوع محدد هو "المعطيات" الموجودة داخل النظام، أي تلك التي يحتويها النظام وتشكل جزءا منه.

أما عن نشاطها الإجرامي فيتضح من خلال الفصل 6-607 460بأنه يتجسد في القيام بإدخال معطيات في نظم المعالجة الآلية للمعطيات أو إتلافها أو حذفها منه أو تغييرها، أو تغيير طريقة معالجة هذه المعطيات أو إرسالها عن طريق الاحتيال.

وعليه فالسلوك الإجرامي بالنسبة لهذه الجريمة يتجسد في القيام بعملية من العمليات أعلاه، إذ يكفي أن يصدر عن الجاني إحداها فقط سواء بإدخال معطيات في نظام المعالجة الآلية، الإتلاف، تغيير المعطيات أو تغيير طريقة معالجتها أو إرسالها.461

ثانيا: جريمة البقاء غير المشروع في نظام المعالجة الآلية للمعطيات

يتمثل السلوك الإجرامي لجريمة البقاء غير المشروع462 في نظم المعالجة الآلية للمعطيات في البقاء في النظام أو جزء منه، والذي يقصد به التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام، وقد يتحقق البقاء المعاقب عليه استقلالا حين يكون الدخول إلى النظام مشروعا، كمن يدخل إلى موقع الكتروني بالصدفة أو عن طريق الخطأ أو السهو، ولا ينسحب منه أو يبقى فيه بعد المدة المحددة له للبقاء داخله. وبالتالي،

460- الفصل 6-607: يعاقب بالحبس من سنة إلى ثلاث سنوات وبالغرامة من 10.000 إلى 200.000 درهم أو بإحدى هاتين العقوبتين فقط كل من أدخل معطيات في نظام للمعالجة الآلية للمعطيات أو أتلفها أو حذفها منه أو غير المعطيات المدرجة فيه، أو غير طريقة معالجتها أو طريقة إرسالها عن طريق الاحتيال.

461- عبد الحكيم زروق: "تنظيم التبادل الإلكتروني للمعطيات القانونية عبر الأنترنيت"، الطبعة الأولى، دار الأمان، 2016، ص 314

462- وقع التنصيص على هذه الجريمة ضمن الفقرة الثانية من الفصل 3-607 من مجموعة القانون الجنائي، والتي تنص على أنه :".... ويعاقب بنفس العقوبة من بقي في نظام للمعالجة الآلية للمعطيات أو في جزء منه، كان قد دخله عن طريق الخطأ وهو غير مخول له دخوله ....."

فإن امتناع الجاني عن قطع الاتصال بالنظام يشكل فعلا جرميا يعاقب عليه متى اتجهت إرادة الجاني إلى تحقيقه.463

ثالثا: جريمة العرقلة العمدية لسير عمل نظام المعالجة الآلية للمعطيات او إحداث خلل فيه

تهدد العرقلة العمدية لسير عمل أنظمة المعالجة الآلية للمعطيات ومنها النظام المعلوماتي لمواقع التجارة الالكترونية أو إحداث خلل فيها سلامة وسلاسة عمل النظام، علاوة على الإضرار بالتشغيل الصحيح لبرامج الموقع وأنظمته.

وباستقرائنا للفصل 5-607 من مجموعة القانون الجنائي يتضح أن السلوك الإجرامي في هذه الجريمة يتفرع لجريمتين مستقلتين، هما عرقلة سير النظام عمدا، وإحداث خلل في النظام.464 وقد نص المشرع المغربي على العقوبة المقررة لهذه الجريمة في الفصل 5-607 من مجموعة القانون الجنائي وذلك بمعاقبته مرتكبها بالحبس من سنة إلى ثلاث سنوات وبالغرامة من 10.000 إلى 200.000 درهم أو بإحدى هاتين العقوبتين.

- **المطلب الثاني: تهديدات الأداء الالكتروني**

إن الوفاء الإلكتروني الذي يتم بالوسائل الإلكترونية، كالحواسيب وعبر قنوات الاتصال المفتوحة على كافة المتعاملين والمستخدمين لها أدى إلى تعريض هذه التقنية للعديد من المخاطر الفنية التي يستطيع من خلالها المجرم الإلكتروني سرقة أموال الغير عن طريق الوسائل الفنية التي يصعب حصرها لسرعة وثيرة التطور في هذا المجال لكن يمكن الإشارة إلى أكثرها شيوعا على النحو التالي:

463-ضباء علي أحمد نعمان: "الغش المعلوماتي الظاهرة والتطبيقات". سلسة الدراسات القانونية في المجال المعلوماتي. المطبعة والوراقة الوطنية –مراكش-2010. ص 350

464-سعد مستور: "النظام القانوني للتاجر السيبراني –دراسة في ضوء القانون المغربي والمقارن". مطبعة الأمنية الرباط 2022. ص 453

الفقرة الأولى: استخدام برامج معدة خصيصا لتنفيذ الاختلاس

من بين هذه الوسائل[465] تصميم برامج معينة تهدف إلى إجراء عمليات التحويل الآلي من حساب إلى آخر، سواء كان ذلك من البنك نفسه أو من حساب آخر في بنك آخر، على أن يتم ذلك في وقت معين يحدده مصمم هذا البرنامج، كما توجد برامج أخرى تقوم بخصم مبالغ ضئيلة من حسابات الفوائد على الودائع البنكية بإغفال الكسور العشرية بحيث يتحول الفارق مباشرة إلى حساب الجاني لأنها برامج تعتمد على التكرار الآلي لمعالجة معينة، ومما يؤدي إلى صعوبة اكتشاف هذه الطريقة رغم ضخامة المبلغ هو أن تلك الاستقطاعات تتم على

[465]- البرمجيات الخبيثة:(Malware) برمجيات ضارة تُثبَّت على جهاز المستخدم دون علمه أو موافقته. تشمل الفيروسات، الديدان، وأحصنة طروادة(Trojans) ، التي يمكن أن تسرق البيانات أو تُعطل النظام.

- برمجيات تسجيل ضغطات المفاتيح:(Keyloggers) برمجيات خبيثة تقوم بتسجيل كل ما يكتبه المستخدم على لوحة المفاتيح، بما في ذلك أسماء المستخدمين، كلمات المرور، ومعلومات الدفع. هذه المعلومات تُرسل إلى المهاجمين الذين يمكنهم استخدامها لسرقة الحسابات.

- هجمات التصيد:(Phishing) هي رسائل احتيالية تستهدف خداع المستخدمين للكشف عن معلوماتهم الشخصية. يمكن أن تأتي عبر البريد الإلكتروني، الرسائل النصية، أو حتى عبر المواقع المزيفة التي تبدو مشابهة للمواقع الحقيقية.

- برمجيات الفدية:(Ransomware) نوع من البرمجيات الخبيثة التي تقوم بتشفير ملفات المستخدم، ثم يطلب المهاجم فدية لإعادة فك تشفير البيانات. هذا يمكن أن يُعيق الوصول إلى بيانات حساسة أو حتى إكمال عمليات الدفع.

- برامج الخداع المالي:(Adware & Spyware) برمجيات تجسس تقوم بجمع البيانات حول المستخدم بدون علمه، بما في ذلك عادات التسوق والمعلومات المالية. قد تُستخدم هذه البيانات لتنفيذ هجمات مالية أو بيعها لأطراف غير موثوقة.

- هجمات الوسيط:(Man-in-the-Middle Attacks) في هذا الهجوم، يقوم المهاجم بالتنصت على الاتصالات بين المستخدم والخادم (مثل الموقع البنكي أو موقع التسوق) لسرقة معلومات الدفع والبيانات الشخصية دون علم المستخدم.

مستوى آلاف الأرصدة في وقت واحد مع ضآلة المبلغ المخصوم من كل الحساب على حدة بحيث يصعب أن ينتبه إليه العميل466.467

وعليه يمكن ان يتخذ هذا الاعتداء كذلك صورة محاكات مواقع التجارة الالكترونية، حيث يتم نسخ البيانات المعروضة على الموقع وإعادة على موقع اخر بغرض تنفيذ جرائم متصلة بالغش المعلوماتي أو بإيقاع المستهلك الالكتروني في الغلط بخصوص هوية التاجر السيبراني، ليقبل آنذاك على التبضع من خلال هذا الموقع المقلد والذي غالبا ما يتعمد وضع أسعار مغرية تحث المستهلك على التعامل معه؛ وعندما يقوم الزبون بإرسال معلومات بطاقته الائتمانية لإتمام عملية الشراء، يقوم هذا الموقع غير القانوني باستغلالها لغايات إجرامية كالسرقة والتزوير وغيرها.

أما فيما يخص إتلاف مواقع التجارة الالكترونية، فإن ذلك يتم باستخدام المجرم الالكتروني للفيروسات المعلوماتية بهدف تدمير نظم حماية الموقع الالكتروني، والاستيلاء بعد ذلك بسهولة على بيانات بطاقات المستهلكين الائتمانية أو غيرها من وسائل الدفع الالكتروني التي يشارك المستهلك بياناتها عند السداد بها مع التاجر السيبراني. ويتم استخدام الفيروسات الالكترونية

466- ومن أشهر جرائم سرقة الأموال، تلك التي حدثت في إمارة دبي بدولة الإمارات العربية المتحدة في أواخر عام 2001 ما قام به مهندس حاسبات أسيوي يبلغ من العمر 31 سنة وتم نشر وقائع الجريمة في أبريل من عام 2003، حيث قام بعمل العديد من السرقات المالية لحسابات عملاء في 13 بنكا محليا وعالميا. حيث قام باختلاس الأموال من الحسابات الشخصية وتحويل تلك الأموال إلى حسابات وهمية قام هو بتخليقها كما قام أيضا بشراء العديد من السلع والخدمات عبر شبكة الأنترنيت مستخدما بيانات بطاقات الائتمان والحسابات الشخصية لعدد كبير من الضحايا. كل ذلك تم من خلال الدخول للشبكة من خلال إحدى مقاهي الأنترنيت العامة المنتشرة في دبي وقد بلغت قيمة الاختلاسات حوالي 300 ألف درهم من البنوك المحلية بالإمارات فقط.

467- فاطمة الزهرة خبازي:" جرائم الدفع الإلكتروني وسبل مكافحتها،" أعمال الملتقى الوطني آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري - الجزائر 29 مارس 2017، ص 35

قصد تدمير الموقع حالا أو في المستقبل المنظور والتي يمتد خطر استعمالها في قرصنة بطاقات الائتمان وسرقتها، أو تحويل رصيدها المالي إلى جهة مجهولة.468

الفقرة الثانية: التحويل المباشر للأرصدة والتلاعب بالبطاقات البنكية

يتم ذلك عن طريق اختراق أنظمة الحاسب وشفرات المرور، أشهرها قيام أحد خبراء الحاسب الآلي في الولايات المتحدة باختراق النظام المعلوماتي لأحد المصارف وقيامه بتحويل 12 مليون دولار إلى حسابه الخاص في ثلاث دقائق فقط وعادة ما يتم ذلك أيضا عن طريق إدخال معلومات مزيفة وخلق حسابات ومرتبات وهمية وتحويلها إلى حساب الجاني، ويمكن أن يتم التحويل المباشر أيضا عن طريق التقاط الإشعاعات الصادرة عن الجهاز إذا كان النظام المعلوماتي متصلا بشبكة تعمل عن طريق الأقمار الصناعية.

وهناك بعض الأنظمة التي تستخدم طابعات سريعة تصدر أثناء تشغيلها إشعاعات إليكترومغناطيسية تبث أنه من الممكن اعتراضها والتقاطها أثناء نقل الموجات وحل شفراتها بواسطة جهاز خاص لفك الرموز وإعادة بثها مرة أخرى بعد تدويرها.469

كما يعد التلاعب بالبطاقات البنكية نوع من الاحتيال الذي يعتمد على التقاط الأرقام السرية لبطاقات الائتمان وبطاقات الوفاء المختلفة من أجهزة الصرف الآلي للنقود وقد استمر هذا النوع من السرقة إلى أن ظهرت الصرافة الآلية، والنقود المالية.

وتتمثل جرائم الاعتداء على هذه البطاقات في استخدامها من قبل غير صاحب الحق بعد سرقتها أو بعد سرقة الأرقام السرية الخاصة بها، وهو ما يتم عن طريق اختراق بعض المواقع التجارية التي يمكن أن تسجل عليها أرقام هذه البطاقات. 470

468- سعد مستور: المرجع السابق. ص 414

469- فاطمة الزهرة خبازي. نفس المرجع السابق. 37

470- جلال محمد الزغبي وأسامة أحمد المناعسة :"جرائم تقنية نظم المعلومات الإلكترونية"، دراسة مقارنة، دار الثقافة، عمان، الأردن، الطبعة 1 2010 . ص120

بناء على هذا التشخيص الشامل لطبيعة المخاطر السيبرانية وأبعادها، تبرز الحاجة الملحة لإيجاد دروع واقية قادرة على كبح جماح هذه التهديدات؛ وهو ما سنعمل على بيانه في المبحث الثاني عبر تسليط الضوء على آليات الحماية القانونية والأجهزة المؤسساتية المعتمدة في هذا الصدد، وجانب التعاون الدولي.

- **المبحث الثاني: آليات الأمن السيبراني المعززة لثقة المستهلك الالكتروني**

لا يمكن فصل نجاح الاقتصاد الرقمي عن توفير بيئة افتراضية آمنة ومستقرة؛ فإذا كانت المخاطر السيبرانية المتعددة تقوض طمأنينة المستهلك وتدفعه نحو العزوف عن المعاملات الإلكترونية، فإن مجابهة هذه التهديدات تتطلب تجاوز المقاربات التقليدية نحو إرساء دعائم منظومة حمائية متكاملة قوامها الاستباقية والفعالية التقنية، ومن هذا المنطلق، أضحى تبني استراتيجيات دفاع وأمن سيبراني قوية مدخلا إلزامياً لبناء "الثقة الرقمية" وصيانة حقوق الفاعلين في هذا الفضاء الافتراضي.

وتجسيدا لهذا التوجه، تضافرت الجهود الوطنية والدولية لصياغة منظومة حماية شاملة، يتداخل فيها البعد القانوني **(المطلب الأول)** بالعمق المؤسساتي والتعاون العابر للحدود **(المطلب الثاني)**.

- **المطلب الأول: الآليات التشريعية المعززة للأمن السيبراني للمستهلك**

إن نجاح الاقتصاد الرقمي رهين ببناء ثقة المستهلكين بهذا النمط من الاقتصاد، كما أن المخاطر السيبرانية التي تهدد المستهلك والمتمثلة في الجرائم الالكترونية أو الافتراضية التي تتخطى الحدود والأماكن الجغرافية يعد أكبر تهديد لهذه الثقة، وبالتالي أصبح لا بد من إيجاد بيئة قانونية **(الفقرة الأولى)**، ومؤسساتية **(الفقرة الثانية)** مضبوطة كي تضمن حماية حقوق ومصالح كل أطرافها المتعاملين في ظل الاقتصاد الرقمي.

الفقرة الأولى: الإطار التشريعي المنظم للأمن السيبراني

إن توفير الحماية القانونية للمستهلك الالكتروني وتعزيز استراتيجيات الأمن السيبراني في الدول، تعتبر مرجعا تشريعيا مهما في شتى المجالات، وهذا يعكس التطور التكنولوجي

والاجتماعي الذي تحظى به، وتعتبر المملكة المغربية من بين الدول التي سعت ومازالت تسعى بتبني تشريعات كافية حاليا لتوفير الحماية القانونية المثلى للمستهلك الالكتروني سواء من خلال قانون إطار للمجال(أولا)، أو من خلال قوانين مرتبطة أشد الارتباط بهذا الأخير (ثانيا).

أولا: القانون 20-05 المتعلق بالأمن السيبراني

حدد المشرع الإطار الوطني لحكامة الأمن السيبراني من خلال اصدراه للقانون 05.20 والذي سطرت إدارة الدفاع الوطني في المذكرة التقديمية لهذا القانون أهدافه بشكل واضح، والمتجلية أساسا في وضع قواعد قانونية بشأن وسائل الحماية الرامية إلى تعزيز الثقة ودعم الاقتصاد الرقمي، وبشكل أعم ضمان استمرارية الأنشطة الاقتصادية والاجتماعية لبلادنا. 471

كما أن هذا النص التشريعي يتضمن تدابير أمنية تهدف إلى تقوية القدرات الوطنية في هذا المجال والمساهمة في تأمين عملية التحول الرقمي بالمغرب وكذا تنسيق إجراءات الوقاية والحماية في مواجهة هجمات وحوادث الأمن السيبراني.

نص القانون رقم 05.20 المتعلق بالأمن السيبراني على اتخاذ التدابير التقنية والتنظيمية اللازمة لحماية شبكات ونظم معلومات فئات فاعلة أخرى تشمل مستغلي الشبكات العامة للمواصلات، ومزودي خدمات الانترنيت، ومقدمي خدمات الأمن السيبراني، ومقدمي الخدمات الرقمية وناشري منصات الانترنيت.

كما يولي هذا القانون كذلك أهمية كبيرة للوقاية والتحسيس بشأن تحديات الأمن السيبراني، حيث يعهد للسلطة الوطنية بأن تنشر بانتظام على موقعها الالكتروني النصائح والتوصيات الوقائية المتعلقة بالأمن السيبراني لفائدة إدارات الدولة والجماعات الترابية والمؤسسات والمقاولات العمومية والبنيات التحتية ذات الأهمية الحيوية ومتعهدي القطاع الخاص والمواطنين.

471 -Hind Idrissi : "Cybersecurity in Morocco: between achievements and challenges" 22/11/2023. https://mipa.institute/en/10778

ومن أجل مضاعفة قدرات التصدي للهجمات السيبرانية، فإن هذا القانون يعطي أولوية هامة لتنمية التعاون وتطوير تبادل التجارب والخبرات مع المنظمات والمؤسسات الأجنبية المماثلة.

يولي هذا القانون أهمية بالغة لحكامة الأمن السيبراني من خلال تحديد المهام الموكلة إلى اللجنة الاستراتيجية للأمن السيبراني، والسلطة الوطنية للأمن السيبراني واللجنة الوطنية لإدارة الأزمات والأحداث السيبرانية الجسيمة. 472

وفي هذا الصدد، يضع القانون رقم 05.20 إطارا قانونيا يلزم مجموعة من الفئات باحترام التوجيهات والقواعد والأنظمة والمراجع والتوصيات الصادرة عن السلطة الوطنية في هذا المجال، والمتمثلة في إدارات الدولة والجماعات الترابية والمؤسسات والمقاولات العمومية وكل شخص اعتباري آخر خاضع للقانون العام، والتي يشار إليهم في القانون ب " الهيئة".

كما يشمل نطاق الحماية الأنظمة المعلوماتية الخاصة بالبنيات التحتية ذات الأهمية الحيوية وكذا مستغلي الشبكات العامة للمواصلات ومزودي خدمات الانترنت ومقدمي خدمات الأمن السيبراني ومقدمي الخدمات الرقمية وناشري منصات الانترنت، والتي يشار إليهم بالمتعهدين.

وتبعا لما سبق، فإن هذا القانون يهدف إلى توفير الحماية للبنية المعلوماتية الخاصة بالمؤسسات العامة للدولة، أي بالمصالح الإستراتيجية للدولة، كما تشمل أيضا القطاع الخاص المتمثلين في الشركات العاملة في مجال استغلال الشبكات العامة للاتصال ومقدمي خدمات الأمن السيبراني وبصفة عامة كل الجهات التي تدخل حسب قانون 05.20 ضمن ما يسمى بالمتعهدين.473

وقد أشار القانون لضرورة توفير مقدمي الخدمات الرقمية لاستراتيجيات الأمن السيبراني، الأمر الذي يعد إشارة واضحة من المشرع باهتمامه بفئة المستهلكين، خاصة وأنه عرف مقدمي

472 -Hind Idrissi : "Cybersecurity in Morocco: between achievements and challenges" 22/11/2023. https://mipa.institute/en/10778

473- التهامي الزروقي: قراءة من القانون 20-05 المتعلق بالأمن السيبراني". مقال منشور بمجلة الباحث للدراسات والأبحاث القانونية والقضاية.على الموقع الالكتروني:www.albahit.com

الخدمات الرقمية " كل شخص ذاتي أو اعتباري يقدم عن بعد وبطريقة إلكترونية وبناء على طلب مستفيد ما إحدى الخدمات التالية:

. خدمة رقمية تسمح المستهلكين أو المهنيين بإبرام عقود بيع أو خدمة عبر الإنترنت

. خدمة رقمية تسمح للمستعملين القيام بأبحاث على مواقع الإنترنت

. خدمة رقمية تسمح بالولوج إلى مجموعة مرنة ومتنوعة من الموارد المعلوماتية التي يمكن تقاسمها بما فيها مستضيفي المعطيات أو نظم المعلومات أو هما معا ومقدمي الخدمات الرقمية السحابية

كما انه قد نص في إطار المواد 33474 و 34475 على المسطرة الواجب اتباعها من قبل مقدمي الخدمات فور علمهم باي حادثة تؤثر على الشبكات ونظم المعلومات اللازمة.

ومن أجل تعزيز المقتضيات القانونية للقانون الإطار، قام المشرع بتخصيص الفصل الخامس منه لمعاينة المخالفات والعقوبات واعتبر ان كل مقدم خدمة رقمية امتنع عن اتخاذ التدابير المنصوص عليها في المادة 32 او قام بعرقلة عملية المراقبة المنصوص عليها في المادة 34 يعاقب بغرامة من 200.000 الى 40.000 درهم دون الاخلال بالعقوبات الجنائية الأشد المنصوص عليها في التشريع الجاري به العمل.

474-المادة 33: يجب على مقدمي الخدمات الرقمية، فور علمهم بأي حوادث تؤثر على الشبكات ونظم المعلومات اللازمة لتوفير خدماتهم، أن يقوموا بإبلاغ السلطة الوطنية بها، وذلك حينما يتبين من المعلومات المتوفرة لديهم أن لهذه الحوادث وقع بالغ يؤثر على تقديم هذه الخدمات.

475- المادة 34: إذا تم، بأي وسيلة كانت، إخبار السلطة الوطنية بأن أحد مقدمي الخدمات الرقمية لا يفي بأحد الالتزامات المنصوص عليها في هذا القانون، أمكن لهذه السلطة أن تخضعه للمراقبة من أجل التحقق من تقيده بهذه الالتزامات، وكذا من مستوى أمن الشبكات ونظم المعلومات اللازمة لتقديم خدماته. تتم المراقبة من قبل السلطة الوطنية أو من قبل متعهدي الافتحاص المؤهلين من قبل هذه السلطة.

وفي هذه الحالة الأخيرة يتحمل مقدم الخدمات الرقمية مصاريف عمليات المراقبة. إذا تبين أثناء إجراء المراقبة وجود أي إخلال بالالتزامات الملقاة على عاتق مقدم الخدمات بموجب هذا الفرع، أمكن للسلطة الوطنية إعذار مسيري مقدم الخدمات المعني بالتقيد بهذه الالتزامات، وذلك داخل أجل تحدده هذه السلطة.

في مقابل هذا القانون الوطني نجد التشريع الفرنسي الذي يؤطر مجال الأمن السيبراني بالقانون رقم 2018-498 relative à la sécurité des réseaux et (Loi n° 2018-498 des systèmes d'information) وهو قانون يهدف إلى تعزيز أمن الشبكات وأنظمة المعلومات، صدر في 20 يونيو 2018، وتعد الهيئة الوطنية للأمن السيبراني (ANSSI) الجهة المسؤولة عن تنفيذ استراتيجيته.

ومن خلال الاطلاع على مقتضياته، يبدو ان المشرع المغربي استقى منه العديد من المقتضيات، إلا أن هذا الأخير نص في المادة 5 منه على أن المؤسسات العامة والخاصة يجب أن تبلغ السلطات المختصة عن أي حادث أمني سيبراني أو خرق لبيانات المستهلكين خلال 72ساعة من وقوع الحادث، في حالة كانت البيانات الشخصية قد تأثرت.

هذه المادة تلعب دورا كبيرا في حماية المستهلك عبر السماح بالكشف السريع عن الحوادث، وبالتالي اتخاذ التدابير السريعة لمعالجة الموقف، وهو أمر غير موجود في مقتضيات القانون 20-05.

ثانيا: القوانين الأخرى المكرسة لآليات للأمن السيبراني

من أجل ضمان سلامة تبادل المعطيات القانونية بطريقة إلكترونية وضمان سريتها قام المشرع بإصدار القانون 47653.05 المتعلق بالتبادل الالكتروني للمعطيات حيث أتى ليتم ويعدل مقتضيات قانون الالتزامات والعقود، من خلال السماح بولوج الحقبة الرقمية من الباب الواسع للإثبات، إضافة الى تبنيه جملة من الأهداف أبرزها، فرض حماية خاصة لوسائل الاتصال من خلال المادة 32 التي تجرم استيراد أو استغلال استعمال إحدى الوسائل أو خدمات التشفير

476- القانون 53.05 المتعلق بالتبادل الالكتروني للمعطيات القانونية ، الصادر بتنفيذ الظهير الشريف رقم 1.07.129 الصادر في 19 ذي القعدة1428 (30 نوفمبر 2007). الجريدة الرسمية عدد 5584، بتاريخ 25 ذو القعدة 1428 (6ديسمبر 2007) ص3879.

دون الإدلاء بتصريح أو الحصول على الترخيص كما أنه يمكن للمحكمة الحكم بمصادرة وسائل التشفير المعينة.

كما جرم المشرع المغربي استعمال كل وسيلة تشفير لتمهيد، أو ارتكاب جناية أو جنحة أو لتسهيل تمهيدها أو ارتكابها.

ولتحقيق حماية جنائية للتوقيع الالكتروني عقبت المادة 35 كل استعمال غير قانوني للعناصر الشخصية لإنشاء التوقيع المتعلق بالغير.

كما حمى المشرع المغربي من خلال المادة 37 حجية الشهادة الالكترونية عبر تجريم الاستمرار في استعمالها بعد مدة صلاحيتها أو بعد إلغائها.

يتبين ان المشرع من خلال القانون 53.05، راهن على تحقيق مجموعة من المكتسبات القانونية على رأسها تنظيم التعاقد الالكتروني، والذي تعتبر التجارة الالكترونية بمكوناتها الأساسية "التاجر الالكتروني –المستهلك الالكتروني" أبرز صوره وتجلياته.

ومن أجل تعزيز المقتضيات القانونية المتعلقة بالتبادل الالكتروني للمعطيات لا بد من تعزيزها بجملة من الإجراءات تهم أساس مجابهة مخاطر تسريب البيانات وانتهاك الخصوصية، وعليه قام المشرع بإصدار القانون 09.08[477] المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي بتاريخ 18 فبراير 2009، وتبدو أهمية هذا القانون في أنه يساهم في تقوية ثقة المستهلك المغربي في المعاملات الالكترونية والاستفادة من مزايا التجارة الالكترونية.

477- القانون 09.08 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، الصادر بتنفيذه الظهير الشريف رقم 1.09.15 بتاريخ 22 من صفر 1430، الموافق ل18 فبراير 2009، المنشور بالجريدة الرسمية عدد 5711 بتاريخ 27 صفر 1430، الموافق ل23 فبراير 2009. ص552.

إلا ان هذا العالم الافتراضي ساهم في ظهور نمط جديد من الإجرام، أصبح يطلق عليه "الجرائم المعلوماتية او الالكترونية"، مما دفع بالمشرع المغربي إلى أصدر القانون رقم 07.03478 المتعلق بمكافحة الجرائم الماسة بنظم المعالجة الآلية للمعطيات والتي تعد من أهم النصوص التي أضيفت لمجموعة القانون الجنائي المغربي من أجل سد الفراغ في مجال مكافحة الجريمة الإلكترونية479.

ويحتوي هذا القانون على تسعة فصول من 607.3 إلى 607.11 من مجموعة القانون الجنائي المغربي، حيث وضعت هذه الفصول الإطار القانوني الخاص بتجريم الأفعال التي تعتبر جرائم ضد نظم المعالجة الآلية للمعطيات، غير المشروع للنظام المعلوماتي، أو البقاء فيه، أو تغيير المعطيات داخل هذا النظام، حيث ساوى المشرع في قيام المسؤولية الجنائية بين الولوج إلى جزء من النظام والولوج إلى كامل النظام، المهم أن يكون ذلك قد تم عن طريق الاحتيال480.

كما لا ننسى قانون رقم 31.08 القاضي بتحديد تدابير لحماية المستهلك الذي يعد النظام الحمائي الأصيل والشريعة العامة للمستهلكين، والذي سعى المشرع من خلال الباب الثاني لتخصيص مقتضيات قانونية للعقود المبرمة بوسيلة إلكترونية، بحيث جعل أحكام هذا الباب

478- قانون 07.03 المتمم لمجموعة القانون الجنائي في ما يتعلق بالجرائم المتعلقة بنظم المعالجة الالية للمعطيات. الصادر بتنفيذه ظهير شريف رقم 1.03.197 بتاريخ 16 رمضان1424، الموافق ل11 نونبر 2003، المنشور بالجريدة الرسمية عدد 5171 بتاريخ 27 شوال 1424، الموافق ل 22 ديسمبر 2003. ص4284.

479- يعاقب هذا القانون جميع عمليات الاقتحام غير المرخص لها في نظام معالجة البيانات الالي.

480- اخذ المشرع المغربي بالمفهوم الواسع لمحل الدخول، ويتضح ذلك من خلال الفصل 607-" من القانون الجنائي، اذ ينص على أنه: "كل من دخل الى مجموع او بعض نظام الالية للمعطيات".

تسري في مواجهة كل شخص طبيعي أو معنوي يمارس نشاطا عن بعد أو يقترح بواسطة الكترونية توريد منتج او سلعة او تقديم خدمة للمستهلك[481].482

وإيمانا من المشرع ان المنظومة الخاصة بالاستهلاك في جزئها الرقمي لا زالت بحاجة لإعادة النظر، تتم مناقشة مشروع قانون 13.23 المتعلق بتغيير وتتميم القانون 31.08، والذي يبدوا من خلال مسودة مشروع القانون الأثر المستمر والواضح لانتشار تكنولوجيا الاتصال والمعلوميات على النص، وبالتالي ضرورة توفير الحماية الرقمية للمستهلك.

الفقرة الثانية: المؤسسات المتدخلة وطنيا لتعزيز آليات الأمن السيبراني

لا يكفي لتعزيز آليات الأمن السيبراني للمستهلك وضع تشريعات تبين القواعد والجزاءات، بل يتطلب الأمر وضع مؤسسات ساهرة على تنفيذ هذه السياسة الرقمية، تعمل على ضبط التعاملات الرقمية تبعا لخصوصية هذا المجال اللامادي وتبعث الثقة في تعاملات المستهلك الإلكتروني، وهو ما نجده عبر مجموعة من المؤسسات الوطنية يمكننا أن نذكر أبرزها:

أولا: الهيئة الوطنية لحماية المعطيات الشخصية CNDP

[481]- نصت المادة 26 من القانون 31.07 على انه: "تطبق احكام هذا الباب على كل شخص طبيعي او معنوي يمارس نشاطا عن بعد او يقترح بواسطة الكترونية توريد منتج او سلعة او تقديم خدمة للمستهلك، كما تطبق هذه المقتضيات على كل عقد ينتج عن هذه العملية بين مستهلك ومورد بواسطة تقنية للاتصال عن بعد...".

[482]- سعد مستور: "النظام القانوني للتاجر السيبراني". مرجع سابق. ص 64

تم إحداث "اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي"[483] بمقتضى القانون رقم 09.08 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي[484].

يترأس اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي رئيس يعنيه جلالة الملك، وتتكون من أعضاء يعينهم أيضا جلالة الملك باقتراح عضوان من طرف رئيس الحكومة، وعضوان من طرف رئيس مجلس النواب وعضوان من طرف رئيس مجلس المستشارين.

وتحدد مدة العضوية في اللجنة الوطنية في خمس سنوات قابلة للتجديد مرة واحدة، ويشترط أن يكون بين الأعضاء شخصيات مؤهلة لكفاءتها في الميادين القانونية من جهة والقضائية من جهة أخرى، وشخصيات متوفرة كذلك على خبرة واسعة في ميدان الإعلاميات بالإضافة إلى شخصيات بارزة لمعرفتها بقضايا تهم الحريات الفردية.

إن القرارات التي تصدرها اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي أعطى المشرع صلاحية البث فيها للقضاء العادي، وذلك عبر النظر في الطعون الموجهة ضد القرارات الصادرة عن اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي عكس بعض الدول التي جعلت من اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي

483- يؤطر المرسوم رقم 2.09.165 الصادر في 25 جمادى الأولى 1430 (21 ماي 2009)، قواعد عمل اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي، كما يحدد شروط وطرق تعيين أعضائها وإدارتها، كذا سلطات اللجنة الخاصة بالتقصي والمراقبة وغيرها من تفاصيل قيام اللجنة بمهامها.

484- ينص الفصل 24 من دستور فاتح يوليوز 2011 على أنه "لكل شخص الحق حماية حياته الخاصة"، و"لا تنتهك حرمة المنزل ولا يمكن القيام بأي تفتيش إلا وفق الشروط والإجراءات التي ينص عليها القانون"، ثم نص على أنه "لا تنتهك سرية الاتصالات الشخصية، كيفما كان شكلها، ولا يمكن الترخيص بالاطلاع على مضمونها أو نشرها، كلا أو بعضا، أو باستعمالها ضد أي كان، إلا بأمر قضائي، ووفق الشروط والكيفيات التي ينص عليها القانون."

هيئة قضائية من الدرجة الأولى وأن قراراتها تستأنف لدى محكمة الاستئناف كما فعل المشرع التونسي في القانون المنظم لحماية المعطيات الشخصية.485

تتلخص مهام اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي في خمس مهام أساسية، وهي "الإخبار والتحسيس" و"الاستشارة والاقتراح" و"الحماية"، ثم "المراقبة والتحري" و"اليقظة القانونية والتكنولوجية".

ثانيا: اللجنة الإستراتيجية للأمن السيبراني

تم إحداث اللجنة الاستراتيجية للأمن السيبراني (المسماة سابقا باللجنة الإستراتيجية لأمن نظم المعلومات) بموجب القانون رقم 20 – 05 بتاريخ 25 يوليوز 2020، وهي السلطة المسؤولة عن:

- إعداد التوجهات الاستراتيجية للدولة في مجال الأمن السيبراني والسهر على ضمان صمود نظم معلومات الهيئات والبنى التحتية ذات الأهمية الحيوية والمتعهدين المشار إليهم في الفرع الثالث من الفصل الثاني من القانون رقم 20 – 05 المذكور أعلاه.
- إجراء تقييم سنوي لأنشطة المديرية العامة لأمن نظم المعلومات.
- تقييم عمل اللجنة الوطنية لإدارة الأزمات والأحداث السيبرانية الجسيمة المنصوص عليها في المادة 36 من القانون رقم 20 – 05 المذكور أعلاه.
- حصر نطاق افتحاصات أمن نظم المعلومات التي تنجزها المديرية العامة لأمن نظم المعلومات.
- تشجيع البحث والتطوير في مجال الأمن السيبراني.
- تشجيع برامج وأنشطة التحسيس وتعزيز القدرات في مجال الأمن السيبراني لفائدة الهيئات والبنيات التحتية ذات الأهمية الحيوية.

485- لبنى الوزاني:" الرقابة القضائية على أعمال اللجنة الوطنية لحماية المعطيات الشخصية". مجلة قضاء محكمة الاستئناف بالدار البيضاء. ع. 2. 2018. ص15

- ابداء الرأي في مشاريع القوانين والنصوص التنظيمية المتعلقة بمجال الأمن السيبراني.

- **المديرية العامة لأمن نظم المعلومات(DGSSI)**

المديرية العامة لأمن نظم المعلومات، التابعة لإدارة الدفاع الوطني للمملكة المغربية والمعروفة اختصارا بـ (DGSSI)هي جهاز أمني تم إحداثه بموجب المرسوم رقم 2.11.509 الصادر في 21 سبتمبر 2011.

وتضم المديرية أربع مديريات هي كالآتي:

1- مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية

2- مديرية الإستراتيجية والتقنين

3- مديرية المساعدة والتكوين والمراقبة والخبرة

4- مديرية نظم المعلومات المؤمنة

وتتكلف هذه المديرية بتطوير الأنظمة الضرورية لتشغيل نظم مؤمنة لفائدة الإدارات والمؤسسات العمومية، كما تقوم بالدراسات والأبحاث وتحليل النظم.

وتضم المديرية العامة لأمن نظم المعلومات قسما مسؤولا عن إجراء الدراسات والأبحاث في المجالات المتصلة بالأمن السيبراني، لاسيما الأطروحات المنجز ة بالتعاون مع الجامعات الوطنية والدولية. وتهدف هذه المبادرة إلى اقتراح حلول مبتكرة تستند إلى حصيلة إجراءات اليقظة في مجال البحث العلمي من جهة، والمساهمة في أبحاث مرتبطة بمجال أمن نظم المعلومات عن طريق نشر نتائجها في المؤتمرات والمجلات المختصة من جهة أخر ى. وتقود المديرية العامة لأمن نظم المعلومات أبحاثا أكاديمية في مجالات التشفير، رصدا لاختراقات وأمن المبادلات الإلكترونية، كما تقدم باستمرار نشرات حول الأمن المعلوماتي، ترصد من خلالها كل الهجومات والتهديدات السيبرانية.[486]

- **المطلب الثاني: التعاون الدولي لتنفيذ استراتيجية الأمن السيبراني**

[486] -Taieb Debbagh, « 15 ans de Cybersécurité au Maroc » 2020.

إن تحقيق نتائج إيجابية في مجال الأمن السيبراني يتطلب تكريس تعاون دولي يمكن من الاستفادة من التجارب، وتكثيف الجهود وكذا تقديم الدعم الممكن، الأمر الذي نلمحه من خلال هيئات التعاون الدولي **(الفقرة الأولى)**، أو من خلال الاتفاقيات الدولية الموقعة **(الفقرة الثانية)**.

الفقرة الأولى: هيئات التعاون الدولي

إيمانا من المغرب بأن نجاح أي استراتيجية رقمية رهين بتعزيز التعاون الدولي فالمغرب يعد من الدول الأعضاء المنتمية للاتحاد الدولي للاتصالات، حيث يقوم هذا الاتحاد ببناء جسور بين المجتمعات داخل صناعة تكنولوجيا المعلومات والاتصالات وكذلك بين تلك الصناعة والعديد من المجتمعات الأخرى التي تبتكر تكنولوجيا المعلومات والاتصالات، يوفر الاتحاد الدولي للاتصالات كذلك منصة محايدة لبناء الثقة المتبادلة اللازمة للتقدم التقني المشترك، وهو الأساس الذي يستند إليه الأمن السيبراني.[487]

كما أن المغرب يعد عضوا فعالا في المجموعة الإفريقية للأمن السيبراني(AfricaCERT) ، وهي منظمة إقليمية تهدف إلى تعزيز الأمن السيبراني في القارة الإفريقية، تأسست المجموعة لدعم جهود التعاون بين فرق الاستجابة لحوادث أمن الكمبيوتر (CSIRTs) في إفريقيا، والمساعدة في إنشاء هذه الفرق في البلدان التي لم تنشئها بعد، بالإضافة إلى تعزيز القدرة على الاستجابة للحوادث السيبرانية.

انضم المغرب إلى AfricaCERT كجزء من جهوده لتعزيز الأمن السيبراني على المستوى الوطني والإقليمي، إلا أنه لم يتم تحديد تاريخ محدد لانضمام المغرب إلى هذه المجموعة، ولكنه يشارك في الأنشطة والبرامج التي تنظمها AfricaCERT في إطار التزامه بتعزيز القدرات السيبرانية الوطنية والإقليمية.

[487] - Benjamin S. Buckland, Fred Schreier, Theodor H. Winkler:" democratic governance challenges of cyber security" DCAF HORIZON 2015 WORKING PAPER No. 1. P: 46

المغرب، من خلال الوكالة الوطنية لتقنين المواصلات (ANRT) ومؤسسات أخرى، يعمل على تطوير السياسات والاستراتيجيات التي تتماشى مع أهداف AfricaCERT لتعزيز الأمن السيبراني في البلاد والمنطقة488.

كما انه يعد عضوا نشيطا في المنتدى العالمي للأمن السيبراني Global Forum on) Cyber Expertise GFCE، وهو منصة دولية تعزز التعاون وتبادل المعرفة بين الدول والمنظمات بهدف تعزيز قدرات الأمن السيبراني على مستوى العالم.

يهدف المنتدى إلى تطوير القدرات في مجال الأمن السيبراني من خلال تبادل الخبرات وأفضل الممارسات بين الدول الأعضاء والمنظمات، ويعد المغرب عضوا نشيطا في هذا المنتدى ابتداءا من تاريخ 16 أبريل 2015.489

الفقرة الثانية: الاتفاقيات الدولية

وقع المغرب على مجموعة من الاتفاقيات الدولية من أجل دعم التعاون الدولي، كانت أبرزها: اتفاقية مكافحة الجرائم السيبرانية (CETS 185) المعروفة باتفاقية بودابيست490، التي وضعتها لجنة أوروبا بمشاركة كندا واليابان وجنوب إفريقيا والولايات المتحدة، وكذلك البروتوكول المتعلق بكراهية الأجانب والعنصرية المرتكبة من خلال أنظمة الكمبيوتر (CETS 189)491.492

488 -INTERPOL (2022).African Cyber-Threat Assessment Report. https://www.interpol.int/fr/content/download/19174/file/African%20Cyberthreat%20Assessment%20Report%202022-V2.pdf

489 -Cybersecurity and Cyberwar: What Everyone Needs to Know. P.W. Singer and Allan Friedman, Oxford University Press 2014. ISBN: 978-0-19-991811-9, 306 pages

490- فتحت هذه الاتفاقية للتوقيع في بودابست في نوفمبر 2001 ودخلت حيز التنفيذ منذ يوليو 2004. وهي مفتوحة للانضمام من قبل أي دولة، كما انها تعد الاتفاقية الدولية الملزمة الوحيدة التي تم تبنيها حتى الآن في هذا المجال.

491- فتح للتوقيع في يناير 2003 ودخل حيز التنفيذ منذ مارس 2006.

492 - Benjamin S. Buckland, Fred Schreier, Theodor H. Winkler:" democratic governance challenges of cyber security" DCAF HORIZON 2015 WORKING PAPER No. 1. P: 41-42

تتطلب الاتفاقية من الدول الموقعة493 إنشاء البنية القانونية الأساسية اللازمة لمكافحة الجرائم السيبرانية بفعالية والالتزام بمساعدة الدول الموقعة الأخرى في التحقيق ومقاضاة الجرائم السيبرانية.

تشمل نطاق الاتفاقية:

- تجريم التصرفات؛
- الوصول غير القانوني إلى نظام الكمبيوتر؛
- الاعتراض غير القانوني؛
- تدخل البيانات؛
- تدخل النظام؛
- سوء استخدام الأجهزة؛
- التزوير والاحتيال المتعلق بالكمبيوتر؛
- المواد الإباحية للأطفال؛
- انتهاك حقوق الطبع والنشر والحقوق ذات الصلة؛
- وأدوات التحقيق الفعالة ووسائل الحماية.

493- تمت المصادقة على الاتفاقية من قبل ثمان وعشرين دولة (دول الاتحاد الأوروبي بالإضافة إلى الولايات المتحدة الأمريكية)؛ وأربع وأربعين دولة موقعة (دول الاتحاد الأوروبي وكندا واليابان وجنوب إفريقيا وجميع دول حلف الناتو)؛ وخمس دول مدعوة للانضمام (شيلي وكوستاريكا وجمهورية الدومينيكان والمكسيك والفلبين)؛ بالإضافة إلى عدة دول بارزة لم توقع (الصين وروسيا). تُستخدم الاتفاقية كدليل أو معيار مرجعي أو قانون نموذجي في أكثر من 100 دولة. علاوة على ذلك، تدعم الاتفاقية وتُشير إليها منظمات أخرى، بما في ذلك: الاتحاد الأوروبي؛ منظمة الدول الأمريكية؛ منظمة التعاون والتنمية الاقتصادية(OECD) ؛ التعاون الاقتصادي لآسيا والمحيط الهادئ؛ الإنتربول؛ وأعضاء من القطاع الخاص.

وهي تنطبق على أي جريمة ترتكب باستخدام نظام كمبيوتر وأي دليل في شكل إلكتروني.

على الرغم من القبول الدولي الواسع للاتفاقية، فقد انتقدها البعض باعتبارها غير كافية للتعامل بشكل مناسب مع الأفعال التي تتضمن تداعيات على الأمن القومي، كما انها تعتبر اتفاقية تعالج الهجمات على أنظمة تكنولوجيا المعلومات كجرائم ضد الممتلكات الخاصة والعامة، متجاهلةً البُعد الأمني الوطني لهذه الهجمات، ومن جهة أخرى فهي لا تميز بين الهجمات على أنظمة الكمبيوتر العادية وتلك التي تستهدف أنظمة المعلومات الخاصة بالبنية التحتية الحيوية، أو بين الهجمات الصغيرة والكبيرة.

ومع ذلك، تمثل الاتفاقية قطعة أساسية ولكن ضرورية من التشريعات الدولية، فهي توفر مجموعة قوية من التعريفات القانونية والتقنية التي يمكن بناء الاتفاقيات الإضافية عليها لتعزيز التعاون.

و نظرا لوجود تداخل كبير بين الجرائم السيبرانية والإرهاب السيبراني والحرب السيبرانية، فإن تجريم الاتفاقية لجميع أفعال الهجوم السيبراني، بغض النظر عن الدوافع، يعني أنها تتطلب من الدول الموقعة، عند الطلب، القبض على وتسليم جميع المهاجمين السيبرانيين الدوليين للمحاكمة، بغض النظر عن تعريفهم من قبل الدول المضيفة كجرائم أو إرهابيين أو حتى أشخاص يستحقون الثناء[494].

انضمت المملكة المغربية إلى اتفاقية بودابست لمكافحة الجرائم السيبرانية، التي فتحت للتوقيع في 23 نوفمبر 2001، وصادق عليها في 9 يونيو 2016، كما دخلت الاتفاقية حيز التنفيذ بالنسبة للمغرب في نفس العام.

بالإضافة إلى ذلك، قامت المملكة المغربية بالانضمام إلى البروتوكولات الإضافية المرتبطة بالاتفاقية، ومن بين هذه البروتوكولات، بروتوكول كراهية الأجانب والعنصرية المرتكبة من خلال أنظمة الكمبيوتر (CETS 189) الذي تم توقيعه في ستراسبورغ في 28 يناير 2003

[494] -- Benjamin S. Buckland, Fred Schreier, Theodor H. Winkler.op .p: 42

ودخل حيز التنفيذ في مارس 2006، وكذلك بروتوكول حماية البيانات الشخصية CETS) (198الذي فتح للتوقيع في يونيو 2005 وبدأ تنفيذه في يوليو 2007.

من خلال هذه الخطوات، تعزز المغرب من التزامه بالمعايير الدولية لمكافحة الجرائم السيبرانية وتوفير حماية فعالة ضد الأنشطة الإجرامية الرقمية ذات الطابع العنصري وحماية البيانات الشخصية.

كما وقع المغرب على الاتفاقية الإفريقية للأمن السيبراني وحماية البيانات الشخصية (اتفاقية مالابو)، التي تشكل نصا قانونيا استراتيجي في مجال مكافحة الجرائم الإلكترونية في إفريقيا، بحيث تعالج مسألة الأمن السيبراني بتوسع، بحيث تضمنت مكافحة الجريمة السيبرانية وحماية البيانات الشخصية والإشراف على المعاملات الإلكترونية، وهي تهدف على غرار الاتفاقيات ذات الصلة إلى تعزيز ومواءمة التشريعات الحالية للدول الأعضاء والمجموعات الاقتصادية الإقليمية في مجال تكنولوجيا المعلومات والاتصالات مع احترام الحريات الأساسية وحقوق الإنسان والشعوب.

كما أنها تعمل على إنشاء وثيقة معيارية مناسبة تتوافق مع البيئة القانونية والثقافية والاقتصادية والاجتماعية الإفريقية التأكيد على حماية البيانات الشخصية والخصوصية وهي قضية رئيسية في مجتمع المعلومات، بحيث يجب أن تحترم أي معالجة للبيانات الشخصية التوازن بين الحريات الأساسية ومصالح الجهات الفاعلة العامة والخاصة تعزيز استخدام تكنولوجيا المعلومات والاتصالات، وزيادة التدفق وانقاص أسعار الأنترنيت.

كما انها تعمل على تعهد كل دولة طرف باعتماد تدابير تشريعية أو تنظيمية لتحديد القطاعات التي تعتبر حساسة لأمنها القومي ورفاهية اقتصادها العمل على تنظيم الاعتراف القانوني بالمعاملات التجارية والعقد والإمضاء الإلكترونيين، وإيجاد قواعد قانونية تحمي المستهلكين

وحقوق الملكية الفكرية والبيانات الشخصية وأنظمة المعلومات، بالإضافة للتشريعات المتعلقة بالخدمات الهاتفية والعمل عن بعد وغيرها.495

تعد هذه الاتفاقية التي تم اعتمادها في قمة الاتحاد الإفريقي في مالابو بغينيا الاستوائية في عام 2014 من أبرز الاتفاقيات المتعلقة بالأمن السيبراني في إفريقيا، التي تهدف إلى وضع إطار قانوني لحماية البيانات الشخصية، وتعزيز الأمن السيبراني، ومكافحة الجرائم الإلكترونية على مستوى القارة الإفريقية.

كما ان تصديق الدول الإفريقية على اتفاقية مالابو بشأن الأمن السيبراني وحماية البيانات الشخصية يمكنه أن يوفر فهما حقيقيا ومنسقا لسياسة الأمن السيبراني على المستوى القاري، الا انه لم تصادق عليها سوى 15 دولة فقط من دول الاتحاد القاري من أصل الدول الأعضاء؛ من ضمنهم المغرب ومصر ونيجيريا والجزائر وجنوب إفريقيا وإثيوبيا، وهذا ما حدّ من فاعليتها ومصداقيتها496.

خاتمة:

يبدو جليا مما تقدم أن الحديث عن بناء الثقة في معاملات المستهلك الالكتروني تستدعي أساسا الوقوف عند آليات تعزيز الأمن السيبراني، وما يبدو من خلال الدراسة أنه على الرغم من انتهاج أسلوب حكيم في ضبط المعاملات المنجزة داخل العالم الافتراضي على المستوى التشريعي، بالاعتماد على محصلات التجارب التشريعية للدول من جهة، وعلى تعزيز التعاون الدولي من جهة أخرى، إلا أنه لابد من الاعتراف أن تحقيق الحماية بالشكل المطلوب يحتاج

495-مريم لوكال: "قراءة في اتفاقية الاتحاد الافريقي حول الأمن السيبراني وحماية المعطيات ذات الطابع الشخصي".مقال منشور بمجلة الدراسات القانونية والاقتصادية . المجلد 04. العدد3 السنة 2021. ص657 وما بعدها

496- توفيق بوفرتيح: " تقرير يرصد واقع الأمن الرقمي في إفريقيا ويوصي بالدبلوماسية السيبرانية". مقال منشور بالموقع الالكتروني:https://www.hespress.com

تكريس المزيد من الجهد ومواجهة العديد من التحديات التي تواجه عمل المؤسسات الوطنية الساهرة على تكريس الثقة الرقمية في الفضاء السيبراني بشكل عام، وثقة المستهلك بشكل خاص، وعليه نتقدم بجملة من التوصيات والمقترحات تتمثل في:

تأطير التزام الإبلاغ بوعاء زمني صارم :تعديل المادة 33 من القانون رقم 05.20 المتعلق بالأمن السيبراني عبر إلزام مقدمي الخدمات الرقمية بإبلاغ السلطة الوطنية (DGSSI) وكذا المستهلكين المتأثرين بأي اختراق أو تسريب للبيانات الشخصية والمالية في أجل أقصاه 72 ساعة من تاريخ كشف الحادث، أسوة بالتشريعات المقارنة كالتشريع الفرنسي (القانون رقم 2018-498)، تفادياً لتراخي متعهدي الخدمات حمايةً لسمعتهم التجارية على حساب أمن المستهلك.

- **تعجيل إخراج وتنزيل مشروع القانون رقم 13.23** :الإسراع في المصادقة وتنزيل مشروع القانون رقم 13.23 المتعلق بتغيير وتتميم القانون 31.08 (بمثابة قانون حماية المستهلك)، لضمان مواءمة تامة وعصرية بين القواعد العامة لحماية المستهلك والأبعاد الأمنية والتقنية المستجدة في التجارة الإلكترونية.
- **تقوية التنسيق المؤسساتي بين (CNDP) و (DGSSI)**:إرساء قنوات تواصل مؤسساتية مباشرة وآليات تنسيق مرنة بين "اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي" و"المديرية العامة لأمن نظم المعلومات" لتوحيد جهود اليقظة والتحري وتجنب التنازع الإداري في تتبع الهجمات السيبرانية التي تمس البيانات الشخصية.
- **تحديث المنظومة الجنائية الرقمية** :مراجعة وتطوير المقتضيات الزجرية الواردة في القانون 07.03 المتعلق بالجرائم الماسة بنظم المعالجة الآلية للمعطيات، وتضمينها عقوبات مشددة تلائم خطورة الجرائم السيبرانية الحديثة المستعملة للذكاء الاصطناعي وتقنيات الهندسة الاجتماعية المعقدة.

- **تفعيل وتعميق آليات التعاون الدولي** :تنشيط الانخراط المغربي في الاتفاقيات الدولية المصادق عليها (كاتفاقية بودابست ومجهودات معاهدة الأمم المتحدة لمكافحة الجرائم السيبرانية لعام 2025) عبر تفعيل مذكرات تسليم المجرمين وتسهيل المساعدة القضائية الرقمية المتبادلة لتعقب الجناة في الجرائم العابرة للحدود

-