The North African Journal of Scientific Publishing (NAJSP)
مجلة شمال إفريقيا للنشر العلمي (NAJSP)
E-ISSN: 2959-4820
Volume 1, Issue 2, April-June 2023, Page No: 174-189
Website: https://najsp.com/index.php/home/index

الأمن السيبراني وحماية الأنظمة المعلوماتية

بدر الحيمودي*
باحث بسلك الدكتوراه، قسم القانون الخاص، كلية العلوم القانونية والاقتصادية والاجتماعية، جامعة محمد الأول، المغرب

Cybersecurity and the Protection of Information Systems

Bader El Himoudi *
PhD researcher, Department of Private Law, Faculty of Legal, Economic and Social Sciences, Mohammed I University, Morocco

*المؤلف المراسل	tallimbadar@gmail.com	*Corresponding author
تاريخ الاستلام: 2023-03-27	**تاريخ القبول:** 2023-04-24	**تاريخ النشر:** 2023-04-27

الملخص

ان التقدم الكبير في تكنولوجيا المعلومات والاتصالات جعل من الامن السيبراني أهمية كبيرة للمجتمع المغربي وللمملكة المغربية، حيث ان الامن السيبراني مهم على مستوى الفرد في حماية البيانات الشخصية والصور والملفات والفيديوهات والحسابات الشخصية وكلمات المرور والحسابات البنكية وغيرها من الامور التي ترتبط بحياة المواطن المغربي، وعلى مستوى المجتمع المغربي، من حيث حماية المجتمع من الهندسة الاجتماعية واستهداف السلوك الاجتماعي والبيانات المجمعة والخصوصيات للمجتمع، وعلى مستوى الشركات والمؤسسات، في حماية الأصول الإلكترونية والبيانات والمعلومات وبيانات الموظفين والعملاء والمواقع الإلكترونية، وعلى مستوى الدولة، في حماية أمنها الالكتروني وحماية الأنظمة المالية والاقتصادية وغيرها من الهجمات الالكترونية والابتزاز والقرصنة والتعطيل، وبما أن الأمن السيبراني عبارة عن مجموع الوسائل التقنية والتنظيمية والادارية التي يتم استخدامها لمنع الاستخدام الغير مصرح به و سوء الاستغلال واستعادة المعلومات الالكترونية ونظم الاتصالات والمعلومات التي تحتويها وذلك بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصية واتخاذ جميع التدابير فإننا سنتعرف في هذا البحث على مدى تكريس الأمن السيبراني على المستوى الوطني والدولي وذلك لمعرفة مدى ملاءمة المشرع المغربي للاتفاقيات والمعاهدة الدولية.

الكلمات المفتاحية: الأمن السيبراني، السيادة السيبرانية، معطيات ذات طابع شخصي، معطيات حساسة، الجريمة السيبرانية.

Abstract

The great progress in information and communication technology has made cybersecurity of great importance to Moroccan society and the Kingdom of Morocco, as cybersecurity is important at the individual level in protecting personal data, photos, files, videos, personal accounts, passwords, bank accounts and other matters related to the life of the Moroccan citizen, and at the level Moroccan society, in terms of protecting society from social engineering and targeting social behavior, collected data and privacy of society, and at the corporate and institutional level, in protecting electronic assets, data, information, employee and customer data, and websites, and at the state level, in protecting its electronic security and protecting financial and

economic systems and other attacks And since cybersecurity is a set of technical, organizational and administrative means that are used to prevent unauthorized use and misuse and restore electronic information and communication systems and the information they contain, with the aim of ensuring the availability and continuity of the work of information systems and enhancing the protection, confidentiality and privacy of personal data and taking In this research, we will learn about the extent to which cyber security is devoted at the national and international levels, in order to find out the suitability of the Moroccan legislator for international conventions and treaties.

Keywords: Cyber Security, Cyber Sovereignty, Personal Data, Sensitive Data, Cybercrime**.**

مقدمة:

أولاً: الإطار العام للموضوع.

مرت المجتمعات البشرية عبر العديد من المحطات بدأ من المجتمع البدائي والمجتمع التقليدي ووصولا إلى المجتمع المعلوماتي[1] فحاليا نعيش في خضم مجتمع يغمره العالم المعلوماتي والثورة التكنولوجية حيث لم يعد من الممكن تخيل مجتمع بدون معلومات وبدون تطورات تكنولوجية في مختلف المجالات.

فالعالم على اعتاب ثورة نوعية جديدة يقودها الذكاء الاصطناعي[2] فالبشرية أصبحت على وشك التحول نحو جيل جديد من المجتمعات يندر هذا التحول بظهور مجتمع فائق الذكاء تتحقق فيه نبوءات أفلام الخيال العلمي حيث سنذهب من مجتمع معلوماتي الى مجتمع ما بعد المعلومات[3].

فما حققته التكنولوجيا في خلق مجتمع معلوماتي وما تزال تحققه من تطورات تسهل على العالم تعامل في: مختلف المجالات وتسهيل نمط الحياة، الا انه سهلت ايضا التعامل في مجالات تنحو في منح سلبي، حيث سهلت ايضا ارتكاب افعال ضارة ومجرمة وقد تساهم في تخريب العالم بأكمله بشتى مجالاته؛ فظهرت في المجتمع المعلوماتي انواع جديدة من الجرائم مختلفة تماما عن الجرائم ذات الطابع التقليدي جرائم بوسائل تقنية حديثة والتكنولوجيا فهي الجريمة الحديثة التي تبنت مصطلح الجريمة السيبرانية المرتكبة عبر الفضاء السيبراني والظهور نمط جديد من التهديدات تنحو في نفس السياق.

فالتهديدات السيبرانية شر لابد منه لا تقتصر فقط على الفرد بل تزعزع سيادة الدول وكياناتهم فهو تهديد أمنى جديد ساهم في بروز مظهر جديد للأمن للحماية من تلك الهجمات السيبرانية وهو الامن السيبراني فهو يهدف الى الردع السيبراني اي حماية الفضاء السيبراني من كل الهجمات التي قد تطاله.

حيث يعتبر الأمن السيبراني هو عملية حماية الأنظمة البنكية والشبكات والبرامج ضد الهجمات الرقمية تهدف هذه الهجمات السيبرانية عادةً إلى الوصول إلى المعلومات الحساسة واستغلالها في أفعال قد تهدد أمن الدول والأشخاص كانوا الاعتباريين أو الذاتيين.

---

[1] ورد تعريف مجتمع المعلومات في الموسوعة العربية للمجتمع المعلوماتي على أنه:" هو مجتمع تتاح فيه الاتصالات العالمية، وتنتج فيه المعلومات بكميات ضخمة، كما توزع توزيعا واسعا، والتي تصبح فيه المعلومات لها تأثير على الاقتصاد."

[2] يشير مصطلح الذكاء الاصطناعي (AI) إلى الأنظمة أو الأجهزة التي تحاكي الذكاء البشري لأداء المهام والتي يمكنها أن تحسن من نفسها استنادا إلى المعلومات التي تجمعها. يتجلى الذكاء الاصطناعي في عدد من الأشكال. بعض هذه الأمثلة: تستخدم روبوتات المحادثة الذكاء الاصطناعي لفهم مشكلات العملاء بشكل أسرع وتقديم إجابات أكثر كفاءة القائمون على الذكاء الاصطناعي يستخدمونه لتحليل المعلومات الهامة من مجموعة كبيرة من البيانات النصية لتحسين الجدولة يمكن لمحركات التوصية تقديم توصيات مؤتمتة للبرامج التلفزيونية استنادا إلى عادات المشاهدة للمستخدمين.

[3] إيهاب خليفة مجتمع ما بعد المعلومات تأثير الثورة الصناعية الرابعة على الامن القومي - المستقبل الأبحاث والدراسات المتقدمة، ص 10.

حيث ان الأمن السيبراني لم يبدأ إلا في سبعينيات القرن الماضي، إذ لم يكن هناك الكثير من المعلومات عما بات يُعرف ببرامج التجسس والاختراق والفيروسات، وغيرها من المصطلحات التي أصبحت فيما بعد معروفة ومتداولة على نطاق واسع، وذلك بعد حدوث ارتفاع هائل في جرائم الإنترنت خاصة الجرائم المتعلقة بالأنظمة البنكية، حيث أصبح مفهوم الأمن السيبراني معروفًا وشائعًا ومهما، وذلك بسبب الاعتماد المتزايد على مختلف أنواع الأجهزة الإلكترونية المتصلة بالإنترنت وبشبكات الاتصال اللاسلكية؛ فبدأ مفهوم الأمن السيبراني يظهر شيء فشيء مع ظهور أنواع جديدة من تقنيات وتضاعف اخطارها وظهور أنماط جديدة من التهديدات المرتبطة بالأنترنت مرورا من الثمانينات والتسعينيات.

مع بداية فترة التسعينيات من القرن الماضي، بدأت خدمة الإنترنت تدخل في الكثير من المجالات، وازداد عدد المستخدمين لها بشكل ملحوظ، وأصبحوا يضعون معلوماتهم الشخصية والمهمة على المواقع الإلكترونية؛ الأمر الذي فتح المجال واسعًا أمام بعض الأشخاص لسرقة تلك المعلومات والبيانات، بهدف تحقيق بعض المكاسب المادية، ومع حلول منتصف التسعينات أصبحت التهديدات التي تواجه الشبكات الإلكترونية والأنظمة البنكية كثيرة ومتعددة. وهو الأمر الذي دفع بالكثير من الباحثين في هذا المجال وكذلك من الشركات والمؤسسات على اختلاف أنواعها إلى السعي إلى إنتاج جدران حماية فعالة بشكل عالي، وكذلك اختراع برامج عالية الكفاءة لمكافحة الفيروسات على نطاق أوسع.

ووصولا إلى فترة القرن الحادي والعشرين؛ بحلول العقد الأول من القرن الحادي والعشرين تنوعت وتضاعفت التهديدات والاختراقات وكذلك الهجمات الإلكترونية المتعلقة بالأنظمة البنكية التي بدأت كثير من الكيانات الإجرامية القيام بها وبشكل محترف باستخدام تقنيات عالية، الأمر الذي دفع الكثير من الدول والحكومات إلى اتخاذ العديد من القرارات من أجل تضييق الخناق على هذه الجهات. وكان ذلك من خلال العديد من الخطوات مثل؛ سن التشريعات الخاصة بهذا النوع من الجرائم، وإصدار الأحكام الجنائية، ومع مرور الوقت، تقدم أمن وحماية المعلومات والبيانات على شبكة الإنترنت ذلك ما تزال العديد من الجهات تنتج مختلف أنواع الفيروسات لخرق هذا الإنترنت، ومع الأمن[4].

بدأت الارهاصات الأولى لمصطلح الأمن السيبراني في الدول المتقدمة فهي السباقة لتبني أمن سيبراني يهدف الى حماية الفضاء السيبراني من الهجومات التي قد تطاله خاصة تلك المتعلقة بالأنظمة البنكية؛ وبعدها انتشر الأمن السيبراني وتداعياته في جل العالم المغرب أيضا بادر في إقرار الأمن السيبراني ضمن امن الدولة من اجل محاربة الجريمة الحديثة المرتبطة بالتكنولوجيا حيث قام الغرب بسن قوانين تسد الفجوة التشريعية التي تخلفها التكنولوجيا منها القانون المتعلق بحماية المعطيات ذات الطابع الشخصي 09.08[5] وكذا القوانين المتعلقة بتعزيز الثقة الرقمية ولا ننسى اهم الاستراتيجيات المتخذة لتصدي للجريمة المعلوماتية وحماية النظم البنكية وتعزيز الثقة في المعاملات الرقمية. ففي سنة 2020 سن المغرب قانون 05.20[6] المتعلق بحماية النظم المعلوماتية ذات بنية أهمية حساسة ذات طابع اعتباري، ويبدو كذلك أن جهود المملكة المغربية لتحصين الأمن السيبراني في محاولة وقف هجمات التدمير والتخريب ما زالت تتطور وتتسع، مختلف وضع والسبب في ذلك تطور قراصنة الإنترنت باستمرار،

[4] مها دحام تاريخ الأمن السيبراني انظر الموقع mawdoo3.comتاريخ الاطلاع 2022/24/05 الساعة 17:24.

[5] قانون 09.08 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي الصادر بالجريدة الرسمية عدد 5711 بتاريخ 27 صفر 1430 (23) فبراير (2009) بمقتضى ظهير شريف رقم 15.09.1 صادر في 22 صفر 1430 (18) فبراير (2009).

[6] قانون صادر عن الظهير الشريف رقم 1.20.69 في 4 ذي الحجة 1444 25 يوليو 2020 بتنفيذ القانون 05.20 المتعلق بالأمن السيبراني 4160.

وذلك من خلال الاستراتيجيات الجديدة والمبتكرة من أجل ردع هجمات إلكترونية غير متوقعة على العديد من المواقع والمنصات الإلكترونية المهمة والحساسة.

ثانياً: الإطار المفاهيمي للموضوع.

1- تعريف الأمن السيبراني:

يتكون الأمن السيبراني من مصطلحين مصطلح "الأمن"، ثم مصطلح "سيبراني" وأشار ابن منظور إلى أن الأمن من الناحية اللغوية «أمن الأمان، وقد أمنت فأنا أمن وأمنت غيري من الأمن والأمان والأمن ضد الخوف أمن فلان يأمن أمنا وأمانا. وقال صاحب الصحاح الأمن ضد الخوف والأمنة»[7].

أما من الناحية الاصطلاحية فهو «عملية جادة تهدف إلى ضبط كيانها وكرامتها وسيادتها على ترابها دفاعا عن شخصيتها وثقافتها باسم المشاعر الوطنية، كما يعد من المصطلحات قديمة النشأة إذ تعود جدوره التاريخية إلى معاهدة وستفاليا سنة 1648 من خلال بروز الدولة الوطنية أو الدولة الأمة في إطار تبني مقاربات ومضامين في مجالات تسيير الشأن العام»[8].

أما بالنسبة للأمن السيبراني فقد اختلفت التعاريف التي وضعت له فنجد من يعرفه بكونه حماية الشبكات والانظمة المعلوماتية والبيانات والمعلومات المرتبطة بالأنترنت من التهديدات التي من الممكن أن تلحق بها، ومحاولة الوقوف على التحديات التي تعترض توفير الحماية للمعلومة المتواجدة في الأوساط الالكترونية[9].

وقد عرفه المشرع الأردني من خلال قانون الأمن السيبراني الأردني بكونه «مجموعة من الإجراءات المتخذة لحماية الأنظمة والشبكات المعلوماتية والبنى التحتية الحرجة من حوادث الأمن السيبراني والقدرة على استعادة عملها واستمراريتها سواء أكان الوصول إليها بدون تصريح أو سوء استخدام أو نتيجة الاخفاق في اتباع الاجراءات الأمنية أو التعرض للخداع الذي يؤدي لذلك[10].

في حين عرفه القانون 05.20 المغربي المتعلق بالأمن السيبراني من خلال الفقرة الأولى من المادة الثانية منه بكونه مختلف التدابير والإجراءات التي تسمح للنظام المعلوماتي بمواجهة المخاطر في الفضاء السيبراني[11].

وتأسيسا على كل ما تقدم نستنتج بأن الأمن السيبراني هو بمثابة مجموعة من الإجراءات والتدابير الهادفة إلى توفير الحماية اللازمة للأنظمة والشبكات والبرامج من كل الهجمات التي تشكل مساسا بالمعلومات المتضمنة في هذه الأنظمة والبرامج الرقمية، والتي يسعى من ورائها منفذوها إلى الحصول على المعلومات الحساسة أو تغييرها أو تخريبها.

السيادة السيبرانية:

تعتبر السيادة السيبرانية خضوع الفضاء السيبراني لمصالح وقيم الدولة، أي قدرة الدول على التحكم في مجالها السيبراني بما يضمن تتبع نفس القواعد والمعايير والاعتبارات من بقية المجتمع. فهي عبارة تستخدم في مجال حوكمة الانترنت لوصف رغبة الحكومات في ممارسة السيطرة على الانترنت

---

[7] جمال الدين بن مكرم بن منظور الأفريقي المصري لسان العرب" حرف الألف، العدد الأول، دار صادر، بيروت – الطبعة الثالثة لسنة 2000، ص: 163.

[8] ميلود عامر حاج الأمن القومي العربي وتحدياته المستقبلية، دار جامعة نايف للنشر والتوزيع، الرياض، الطبعة الأولى لسنة 2016، ص:19-120.

[9] منى الأشقر: جبور السيبرانية هاجس العصر، جامعة الدول العربية، ص 25.

[10] المادة الثانية من قانون الأمن السيبراني الأردني.

[11] تنص الفقرة الأولى من المادة الثانية من القانون 05.20 على أن "الأمن السيبراني 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".

داخل الحدود الوطنية التابعة لهذه الحكومات، أي أنها تطبيق لحقوق والتزامات سيادة الدول على القضاء السيبراني[12].

ويعد مفهوم "السيادة السيبرانية من المفاهيم الجديدة التي انت بها الرقمنة هذا المفهوم الذي يعبر عن مدى قدرة الدول وتوفرها على الوسائل الكافية لحماية فضائها السيبراني وقدرتها على حماية بياناتها وأنظمتها المعلوماتية دون اللجوء إلى التكنولوجيا الأجنبية، هذا دون أن ننسى بأن مكافحة الجريمة السيبرانية وتحقيق الأمن السيبراني رهين دائما بوجود التعاون الدولي بين الدول.

السيبرانية:

مصطلح السيبرانية مشتقة من كلمة " سايبر Cyber " وتعني: «كل ما يتعلق أو يرتبط بالحواسيب وتكنولوجيا المعلومات والواقع الافتراضي، أصل الكلمة يوناني kybernetecs وتعني القيادة أو التوجيه ومصدرها Cybernetics الذي يعني: "علم الاتصالات وأنظمة التحكم الآلي في كل من الآلات والأشياء الحية»[13].

معطيات ذات طابع شخصي:

كل معلومة كيفما كان نوعها بغض النظر عن دعامتها، بما في ذلك الصوت والصورة والمتعلقة بشخص ذاتي معرف أو قابل للتعرف عليه والمسمى بالشخص المعني[14].

معطيات حساسة:

معطيات ذات طابع شخصي تبين الأصل العرقي أو الاثني أو الآراء السياسية أو القناعات الدينية أو الفلسفية أو الانتماء النقابي للشخص المعني أو تكون متعلقة بصحته بما في ذلك المعطيات الجينية[15].

2- المفاهيم الوارد التنصيص عليها في القانون 05.20.

الجريمة السيبرانية:

تبدأ معظم التقارير والأدلة والمنشورات المتعلقة بالجريمة السيبرانية بتعريف مصطلح الجريمة السيبرانية بكونها مجموعة من الأنشطة التي تستخدم فيها الحواسيب أو الشبكات كأداة أو هدف أو مكان لممارسة النشاط الإجرامي»[16].

وتعرف الجريمة السيبرانية أيضا بكونها أنشطة معتمدة على الحاسوب تعد إما غير قانونية أو تعتبر غير مشروعة من جانب أطراف معينة ويمكن الاضطلاع بها عن طريق الشبكات الإلكترونية العالمية»[17].

من خلال ما سبق يمكن القول بأن مصطلح الجريمة السيبرانية يشمل مجموعة من الأفعال غير المشروعة التي يكون فضاؤها الحاسوب وتستهدف البيانات والمعلومات الموجودة في البرامج والأنظمة المعلوماتية.

ويستخدم مصطلح الجريمة السيبرانية للدلالة على أعمال جرمية محددة قانونا وعندما يكون الاعتداء ماسا بأمن المعلومات وسلامة الأشخاص وسلامة الأموال وأمن الدولة[18]...

وبالرجوع إلى القانون 05.20 المتعلق بالأمن السيبراني المغربي، نجده تناول تعريف لمصطلح الجريمة السيبرانية بصيغة الجمع، وهو ما تم التنصيص عليه من خلال مقتضيات الفقرة الثانية من المادة الثانية من القانون 05.20 السالف الذكر والتي جاء فيها ... جرائم سيبرانية: مجموعة من الأفعال المخالفة

---

[12] الفاطمة بيرم مرجع سابق ص: 799.
[13] معجم اكسفورد على الرابط: https://en.oxforddictionaries.com/definition/cyber
[14] الفقرة الأولى من المادة الأولى من القانون المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي.
[15] الفقرة الأولى من المادة الثانية من نفس القانون.
[16] الاتحاد الدولي للاتصالات: مرجع سابق، ص 16.
[17] الاتحاد الدولي للاتصالات: مرجع سابق، ص 16.
[18] منى الأشقر جبور: مرجع سابق، ص 50.

للتشريع الوطني أو الاتفاقيات الدولية التي صادقت عليها المملكة المغربية، التي تستهدف شبكات ونظم المعلومات أو تستعملها كوسيلة لارتكاب جنحة أو جناية»[19].

ثالثاً: أهمية الموضوع.

مع تزايد استخدام اليومي للأنترنيت وتقنية المعلومات والاتصالات في انجاز مختلف الانشطة اليومية منها مهنية وشخصية وادارية وهناك أنشطة حيوية مما أدى إلى بروز العديد من التحديات في مقدمتها مجموعة من الحقوق التي لابد من تنظيمها وحمايتها وضمان ممارستها في إطار آمن يمنع الإعتداء عليها وهنا تتجلى أهمية الأمن السيبراني لتحقيق وتوفير هذا الإطار للأفراد والمؤسسات والحكومات في علاقة التفاعل التي فيما بينهم في جميع المجالات الاقتصادية الاجتماعية القانونية السياسية.

- على المستوى الاجتماعي:

ان الدخول للعالم السيبراني غير مقيد بأي شروط أو مخصص لفئة اجتماعية محددة أو سن محدد أو مستوى فكري؛ مفتوح في وجه كل المجتمع يظهر الاختلاف في كيفية ونوايا وهدف المستخدم في استغلاله للعالم السيبراني حيث كما نعلم العالم المعلوماتي كسيف ذو حدين يسهل الحياة الاجتماعية ويذهب بالمجتمع نحو مجتمع واعي ومتقدم وراقي مليء بالحداثة والسرعة والمرونة ومتفتح نحو استخدام السليم للمعلوميات ونجد في المقابل جانب يدفع بالمجتمع نحو جميع أنواع الجرائم من هذا النوع والرذيلة وخلق مجتمع فاشل في حالة الاستخدام السيء.

- على المستوى القانوني:

يتميز الجانب القانوني في أي مجال مواكبة التطورات التي تطرأ عليه وتوفير الإطار القانوني منظم والحماية القانونية من أي فعل إجرامي قد يمس به وبما أن العالم السيبراني يتطور يوم بعد يوم وتظهر ثغرات إجرامية لهذا لعب القانون دورا مهما في هذا المجال لتجريم أي فعل قد يظهر في المجال المعلوماتي.

- على المستوى السياسي:

إلى جانب هروب جميع المؤسسات في جميع المجالات للعمل بالرقمنة، استخدمت الدول أيضا الرقمنة في المجال السياسي لتسهيل عليها الوصول لأهدافها كتسهيل عملية الاقتراع و ضمان نزاهته وتسهيل على المواطن الاطلاع على خلفيات القرارات السياسية و تسهيل على السياسيين أيضا معرفة رأي المواطن و ضمان سرعة وسهولة وصول قراراتهم لمن تخصهم وفهمها بشكل صحيح و تنظيم التظاهرات الافتراضية وافتعال الاحتجاجات الإلكترونية وبما ان السياسة الدولة هي اساس استقرار علاقة مؤسساتها في ما بينها وعلاقتها مع مواطنيها وعلاقتها الدبلوماسية مع الدول وهنا تظهر اهمية الأمن السيبراني لهذا الفضاء السياسي المعلوماتي لحماية وضمان سياسة رقمية آمنة للدولة.

- على المستوى الاقتصادي:

بما أن العالم أصبح يعيش ثورة من الأسواق الإلكترونية وعقود تجارية إلكترونية ونقود إلكترونية وأبناك إلكترونية عالمية ووطنية وإقليمية بظهور مقاولات الكترونية وتجارة الكترونية فردية بتسهيل عملية البيع والشراء وتحقيق ارباح مهمه بإمكانها تحقيق التنمية المستدامة على المستوى الاقتصادي والتطوير من الاقتصاد الوطني بالتعامل مع الدول وجلب رؤوس الأموال عن طريق إبرام معاملات بطرق حديثة لذلك على الأمن السيبراني توفير لهذه المعاملات الأمان وضمان الحقوق والثقة الرقمية التجارية.

- على المستوى الأمني:

كم نعلم المهمة الأولى للأمن هو السهر على توفير الأمان للمواطنين وبما ان كل المواطنين يتعاملون بالمعلوميات في كل مشاغلهم اليومية ويضعون فيها معلوماتهم الشخصية لذلك يجب على الأمن

[19] الفقرة الثانية من المادة الثانية من القانون 05.20 المتعلق بالأمن السيبراني.

مواكبة كل ما يمس أمن المواطنين والعمل على توفير أشخاص الأمن لديهم خبرة في المجال السيبراني لرصد أي فعل اجرامي في هذا المجال.

- على المستوى الدولي:

كما سبق أن أشرنا اعلاه عدم وجود حدود دولية على المستوى الرقمي في كل المجالات وهنا تتجلى أهمية الأمن السيبراني في خلق مجال رقمي امن وموثوق به عن طريق إصدار مواثيق واتفاقيات الدولية وتوحيد الاحكام الدستورية في هذا المجال الرقمي.

خامساً: اشكالية الموضوع.

بعد قراءتنا للتقديم أعلاه وعنوان هذا البحث نفهم أننا أثناء التحليل سنناقش استراتيجية التي تبنتها المملكة المغربية وفق القانون 05.20 وكذا التعاون الدول لحماية الفضاء السيبراني من الجرائم البنكية التي قد تمسه عن طريق المواثيق والاتفاقيات الدولية ولتحليل هذا الموضوع نقترح إشكالية مفادها:
هل استطاع المشرع المغربي توفير مجال سيبراني أمن لحماية الأنظمة المعلوماتية لاسيما البنكية وتعزيز الثقة الرقمية داخل المملكة المغربية وخارجها؟

ومن خلال الإشكالية يمكن إعطاء تساؤلات فرعية تتجلى في:

- إلى أي حد يمكن تحديد الإطار العام الأمن السيبراني وحماية الأنظمة البنكية؟

-أين تكمن التهديدات السيبرانية وما دوافعها؟

-إلى أي مدى ستطاع المغرب التصدي للهجمات السيبرانية وتعزيز الثقة في المعاملات الرقمية؟

-ما الجهود المبذولة على المستوى العالمي والإقليمي والوطني؟

-إلى أي حد تمكن المغرب والدول من تحقيق الأمن السيبراني وحماية الأنظمة البنكية؟

سادسًا: المنهج المعتمد في الموضوع.

الدراسة الموضوع تم اعتماد المناهج المعروفة في الأبحاث القانونية والجامعية ومنها:
المنهج الوصفي، يظهر من خلال قيامنا بوصف ظاهرة الأمن والإجرام السيبراني وتحديد بعض المفاهيم التي يقومان عليها، وكذا وصف المفاهيم الخاصة بالإجراءات واستراتيجيات الإدارة الإلكترونية والصعوبات والعراقيل التي تواجهها سواء الآنية أو المستقبلية.

المنهج التحليلي، حاولت في هذا البحث تحليل بعض المفاهيم والغوص في جزئياتها وطرحها بشكل من التفصيل لما بدا لي من أهميتها.

كما تم توظيف المقترب القانوني لجرد أهم المقتضيات القانونية التي تنظم المعاملات الالكترونية، وتقدير مدى ملائمة وفعالية النصوص القانونية الجاري بها العمل.

سابعًا: خطة البحث

وفي ضوء ما سبق ذكره فإنه سيتم الحديث عن تكريس الأمن السيبراني على المستوى الإنابة القضائية وتسليم المجرمين (المطلب الأولى وتكريس الأمن الصبياني على المستوى الدولي على مستوى اتفاقية بوادبست والاتفاقية العربية(المطلب الثاني)

المطلب الأول: الإنابة القضائية وتسليم المجرمين

إن التعاون الدولي ينبني على عدة اتفاقيات سواء تعلق الأمر بالاتفاقيات الثنائية والاتفاقيات الإقليمية الدولية وفي كافة الأحوال على المعاملة بالمثل بتطبيق القانون الداخلي للدولة المطلوبة في التعاون، أي قانون المسطرة الجنائية الذي نظم الكتاب السابع منح الاختصاص المتعلق ببعض الجرائم المرتكبة خارج المملكة والعلاقات مع السلطات القضائية الأصلية وتتعدد آليات التعاون الدولي في مجال تكريس الأمن

السيبراني على المستوى الدولي، من أهمها الإنابة القضائية (الفقرة الأولى) وتسليم المجرمين(الفقرة الثانية).

الفقرة الأولى: الإنابة القضائية.

تعد الانابة القضائية من بين الأليات التي يعتمد عليها التعاون القضائي الدولي في مجال التصدي للإرهاب الإلكتروني، وتعتبر مظهرا من مظاهر المساعدة القضائية، ويقصد بالإنابة القضائية « طلب اتخاد إجراء قضائي من إجراءات الدعوى الجنائية تتقدم به الدولة الطالبة لهذا الإجراء من الدولة المطلوب إليها، وذلك لأهميته للفصل في موضوع معروض على السلطة القضائية في الدولة الطالبة، ويتعذر عليها القيام به لنفسها»[20].

وعليه فإن الإنابة القضائية تلعب دورا هاما في مجال مكافحة الارهاب الالكتروني ذو الطابع الانتشاري الذي يتجاوز الحدود الوطنية بسرعة هامة وفي لحظة زمنية وجيزة، ما يفرض على الدول ويحتم عليها ضرورة التعاون في مجال منح المساعدات القضائية بينها في مجال التحقيقات والمحاكمات[21].

وللإنابة القضائية الدولية مصادر متعددة، فمنها الاتفاقيات الدولية، ومنها ما هو مرتبط بالتشريع الوطني، بالإضافة إلى مصادر أخرى، فمن بين الاتفاقيات الفاعلة في هذا المجال، نجد الاتفاقية المغربية الأمريكية[22]، وكذلك الاتفاقية المغربية الايطالية[23] والاتفاقية المغربية الفرنسية[24].

أما على المستوى الوطني فإن قانون المسطرة الجنائية نظم هذه الآلية، وذلك في إطار الباب الثاني من القسم الثالث ضمن المادتين 714 و715 من ق.م.ج.

والواضح من خلال المادتين السابقتين أن المشرع أعطى الإمكانية للقضاة المغاربة من أجل إصدار إنابات قضائية قصد تنفيذها خارج أراضي المملكة وفق الشروط والإجراءات المنصوص عليها في هذه المواد[25]

وفي هذا الصدد جاء في قرار المجلس الأعلى ما يلي:

" ويمكن لقضاة المملكة أن يضعوا الإنابات قصد تنفيذها خارج المملكة، إذ لم يحدد القانون نوع الإنابات القضائية ولم يحصرها في أبحاث التحقيق. ولما كانت المحكمة قد قامت بوضع إنابة قضائية موجهة إلى السلطات القضائية في بلد آخر (فرنسا) قصد إجراء خبرة طبية على شخص كان ضحية حادثة سير في التراب المغربي، إنما قامت بإجراء مسطر في حدود القانون، ولم تتجاوز الصلاحيات المخولة لها، ولهذا فإن المحكمة باتخاذها لهذا الإجراء، لم تتنازل عن سلطاتها، ولا على اختصاصاتها للبلد الأجنبي الذي انتدب سلطاته القضائية لإنجاز هذه الخبرة[26]

---

[20] عبد الجليل إسماعيل حسن الشيخ زيني: "الإرهاب الالكتروني في القانون الدولي (الماهية والجزاء)" منشورات الحبلى الحقوقية بيروت لبنان، الطبعة الأولى 2020، ص: 221.

[21] وهذا ما نصت عليه اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية من خلال المادة 18 منها والتي نصت على: « تقدم الدول الأطراف بعضها البعض، أكبر قدر ممكن من المساعدة القانونية المتبادلة في التحقيقات والملاحقات والاجراءات القضائية فيما يتصل بالجرائم المشمولة بهذه الاتفاقية حسبما تنص عليه المادة الثالثة، وتمد كل منها الأخرى تبادلها بمساعدة مماثلة عندما تكون لدى الدولة الطرف الطالبة دواع معقولة للاشتباه في أن الجرم المشار إليه في الفقرة (1) أو (ب) من المادة الثالثة ذو طابع عبر وطني، بما في ذلك أن ضحايا تلك الجرائم أو الشهود عليها أو عائداتها أو الأدوات المستعملة في ارتكابها أو الأدلة عليها توجد في الدولة الطرف متلقية الطلب وأن جماعة إجرامية منظمة ضالعة في ارتكاب الجرم».

[22] اتفاقية التعاون القضائي في الميدان الجنائي الموقعة بالرباط في 17 اكتوبر 1983 بين المغرب والولايات المتحدة الأمريكية.

[23] اتفاقية التعاون القضائي المتبادل وتنفيذ الأحكام القضائية وتسليم المجرمين المبرمة بين المغرب والجمهورية الايطالية 12 فبراير 1971.

[24] الاتفاقية بين المغرب وفرنسا للتعاون وتسليم المجرمين في الميدان الجنائي 2 غشت 2011.

[25] ومن بينها استثناء بعض الانابات القضائية من التنفيذ، ومن ذلك استثناء الانابات القضائية من التنفيذ في حالة ما إذا لم تكن من اختصاص السلطات القضائية المغربية، أو إذا كان تنفيذها من شأنه المساس بسيادة المملكة أو أمنها أو نظامها العام أو مصالحها الأخرى.

[26] قرار صادر عن المجلس الأعلى سابقات محكمة النقض حاليا غير منشور.

ويذهب الفقيه الفرنسي برنار بولاك إلى أن الإنابة القضائية هي إجراء بمقتضى نظام داخلي يمكن أن يساءل عنه الأدنى المنفذ للإنابة أمام الأعلى المصدر للإنابة.

من هنا نتساءل ألا يحق لقاض التحقيق تفويض رئيس المحكمة الذي يعتبر أعلى درجة منه؟

يجيب الأستاذ عمر الزعلاني على تساؤلنا هذا بقوله إن قاضي التحقيق لا يمكنه أن يفوض رئيس المحكمة الذي يعتبر أعلى درجة منه إلا إذا اقتضت الضرورة ذلك ورغم التدرج السلمي.

كما نصت المادة 715 عن طرق تبليغ الانابات القضائية، والتي تكون إما بالطريقة المباشرة أو بالطريقة الدبلوماسية، لتكون بذلك المادة 715 قد سايرت أحكام الاتفاقيات الدولية ذات الصلة بالموضوع.

ومن بين هذه الاتفاقيات نجد الاتفاقية المغربية الفرنسية حيث جاء فيها «بخصوص التبليغ أن الانابات القضائية في الشؤون الجنائية التي ينبغي تنفيذها فوق تراب أحد الجانبين تبلغ بالطريق الدبلوماسي»[27].

وكذلك الاتفاقية المغربية البلجيكية التي تنص على أنه «توجد الانابات القضائية المنصوص عليها في المادتين الرابعة والسادسة من هذه الاتفاقية عبر الطريق الدبلوماسي»[28].

أما بخصوص التبليغ المباشر فنجد الاتفاقية المغربية الفرنسية نصت على هذا الإجراء بنصها **«أنه في حالة الاستعجال المبرر يمكن توجيه طلبات التعاون مباشرة من طرف السلطات القضائية للطرف الطالب إلى السلطة القضائية للطرف المطلوب، وتعمل السلطة المركزية للطرف المطلوب في أقرب الآجال ولتبقى بذلك هذه المسطرة استثنائية قائمة وممكن اللجوء إليها كلما كانت هناك ظروف مبررة لذلك ...»**[29].

والملاحظ أن الطريقة المثلى لتبليغ الإنابة القضائية في جريمة الارهاب الالكتروني هي الطريقة الثانية، نظرا لخصوصيات هذه الجريمة وسهولة اندثار أدلتها، على اعتبار أن طريقة التبليغ المباشر توفر السرعة في الوصول إلى الدليل الفعال في أقرب وقت، الشيء الذي يحول دون قرار المجرم من العقاب.

الفقرة الثانية: تسليم المجرمين.

يعتبر نظام تسليم المجرمين من بين أهم آليات التعاون القضائي الدولي في مجال مكافحة الجريمة، وبالخصوص الجريمة عبر الوطنية العابرة للحدود الإقليمية المرتكبة الفضاء عبر الافتراضي.

ويعرف هذا النظام بكونه «الإجراء الذي بموجبه يتم فيه تخلي دولة عن شخص موجود في إقليم لدولة أخرى بناء على طلب هاته الأخيرة من أجل محاكمته عن فعل بعد جريمة في قانون الدولة الطالبة أو لتنفيذ حكم صادر في حقه من إحدى محاكمها»[30].

كما يعرف أيضا بكونه «إجراء تعاون دولي تقوم بمقتضاه دولة تسمى الدولة الطالبة بتسليم شخص يوجد في إقليمها إلى دولة ثانية تسمى بالدولة المطلوب إليها أو جهة قضائية بهدف ملاحقته عن جريمة اتهم بارتكابها أو لأجل تنفيذ حكم جنائي ضده»[31].

يعتبر هذا الاجراء من بين آليات التعاون الدولي وأحد أهم مظاهره في مجال مكافحة الجريمة المنظمة بصفة عامة وجريمة الارهاب الالكتروني بصفة خاصة، وفيه تجسيد لمبدأ العالمية الذي يتميز به

---

[27] المادة 8 من هذه الاتفاقية.

[28] المادة 14 من هذه الاتفاقية.

[29] الفقرة الثانية من المادة الخامسة من الاتفاقية المغربية الفرنسية.

[30] هذا مع ضرورة الإشارة إلى أن تسمية هذا النظام بهذا الاسم يطرح العديد من الاشكالات، وبالخصوص عندما يتعلق الأمر بمرحلتي البحث والتحقيق، بحيث أن تسمية شخص منهم بمجرم فيه ضرب للعدالة، على اعتبار أن مبدأ البراءة في الأصل ، فوفقا لهذا المبدأ فإنه لا يمكن الحديث عن المجرم إلا بعد صدور قرار أو حكم قضائي في حقه حائز لقوة الشيء المقضي به.

[31] عبد المنعم سليمان: الجوانب الاشكالية في النظام القانوني لتسليم المجرمين، الجامعة الجديدة الاسكندرية 2010.

القانون الجنائي، بحيث أن المجرم ورغم تواجده في إقليم الدولة التي لم تتضرر من فعله الإجرامي، إلا أنه يجب أن تتم ملاحقته وعدم إفلاته من العقاب، ومن هذا المنطلق جاءت فكرة التعاون الدولي في مجال تسليم المجرمين، من أجل توقيع العقاب على كل مخالف للقانون أينما حل وارتحل.

ويبقى تسليم المجرمين من أصعب جوانب التعاون الدولي، بحيث أن طلبات التسليم تؤدي في الكثير من الحالات إلى التنازع بين ضرورة تقرير الحماية للمواطن والحاجة إلى المساعدة في التحقيق الذي يجري بالخارج[32].

والجدير بالذكر أن هذا الإجراء تم التنصيص عليه في العديد من الاتفاقيات الدولية والإقليمية، ونذكر منها على سبيل المثال اتفاقية بودابست[33]، ثم الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، حيث حددت الجرائم المعنية بالتسليم، والمدرجة في إطار الفصل الثاني من هذه الاتفاقية، وهي في مجملها جرائم تعتمد على تقنية المعلومات، كما حددت هذه الاتفاقية مجموعة من الشروط والإجراءات التي يجب احترامها لتطبيق هذا الإجراء[34].

أما على مستوى القانون الداخلي، نجد أن قانون المسطرة الجنائية بدوره خصص جزءا هاما منه لنظام تسليم المجرمين، وذلك من المادة 715 إلى المادة 745 والتي حددت مجموعة من الاجراءات والشروط الخاصة بالتسليم[35].

والملاحظ أن تسليم المجرمين بين الدول، يستدعي أن تكون الجرائم المراد بشأنها التسليم مجرمة ومعاقب عليها قانونا بسنة واحدة بين الدولتين المعنيتين طرفي الاتفاقية أو بعقوبة أشد منها.

المطلب الثاني: التعاون الدولي على مستوى اتفاقية بودابست والاتفاقية العربية.

إن التهديدات السيبرانية هاجس العصر خلقت الرعب في العالم بأسره فالتهديدات السيبرانية من المشاكل التي يجب على الدول السيطرة عليها من أجل ضمان الأمن والسلم العالمي فبعد بروز تلك التهديدات الإلكترونية بادرت الدول في وضع استراتيجيات عالمية للتصدي للهجمات السيبرانية ومختلف الجرائم المرتكبة عبر الأنترنت والتي تمس بالنظام العالمي وتهدد سيادة الدول وتزعزع الأمن العالمي. ولهذا صدد تم تبني استراتيجيات دولية تحمي القضاء السيبراني من كل الجرائم التي قد تمس به وتأثر على أمن وسلامة العالم وتهدد أيضا المعاملات الرقمية التي باتت شيء لا يمكن الاستغناء عنه. خصوصا في العلاقات الدولية سواء على المستوى التجاري او الاقتصادي او غيره من المجالات. فالاستراتيجيات التي تبنها العالم تتدرج في إطار اتفاقيات ومعاهدات دولية التي نظمتها أهم المؤسسات والمنظمات العالمية

---

[32] الاتحاد الدولي للاتصالات، فهم الجريمة السيبرانية دليل البلدان النامية، مرجع سابق، ص: 192.

[33] تم التنصيص عليه في إطار الفصل الثالث من هذه الاتفاقية، وبالضبط المادة 24 منها، والتي جاء فيها تسليم المجرمين يتم الاتفاق على تسليم المجرمين بين الأطراف لمرتكبي الجرائم المنصوص عليها في المواد من المادة الثانية إلى المادة 11 من هذه الاتفاقية.

[34] وهذا ما يتضح من خلال مقتضيات المادة 31 من الاتفاقية العربية، والتي اعتبرت أن تسليم المجرمين محصور في الجرائم الوارد التنصيص عليها في الفصل الثاني من الاتفاقية، وذلك شريطة أن تكون تلك الجرائم يعاقب عليها في قوانين الدول الأطراف المعينة بسلب الحرية لفترة سنة واحدة أو بعقوبة أشد ، وأضافت نفس المادة ضمن فقرتها الثالثة على أنه إذا قامت دولة طرف ما يجعل تسليم المجرمين مشروطا بوجود معاهدة وقامت باستلام طلب لتسليم المجرمين من دولة طرف أخرى ليس لديها معاهدة تسليم فيمكن اعتبار هذه الاتفاقية كأساس قانوني لتسليم المجرمين فيما يتعلق بالجرائم المذكورة في الفقرة الأولى من هذه المادة » ، وأضافت الفقرة الخامسة على أن تسليم خاضع للشروط المنصوص عليها في قانون الدولة الطرف التي يقدم إليها الطلب أو لمعاهدات التسليم المطبقة بما في ذلك الأسس التي يمكن لدولة الطرف الاستناد عليها لرفض تسليم المجرمين ».

[35] من بين هذه الشروط ما ورد التنصيص عليه في إطار الفقرة الثانية من المادة 718 والتي أقرت برفض التسليم في حالات معينة، من بينها ارتكاب الجريمة إما بأرض الدولة الطالبة من طرف أحد مواطنيها أو من شخص أجنبي، وإما خارج أراضيها من أحد مواطنيها، وإما خارج أراضيها من شخص اجنبي غير مغربي، إذا كانت الجريمة المنسوبة إليه تدخل من ضمن الجرائم التي يجيز التشريع المغربي إجراء متابعة بشأنها في المغرب، ولو ارتكبها أجنبي بالخارج »، وأضافت المادة 721 من نفس القانون لتحدد حالات رفض الموافقة على التسليم إذا كان الشخص المطلوب مواطنا مغربيا، وإذا كانت الجريمة المطلوب من أجلها التسليم جريمة سياسية أو مرتبطة بها، وإذا ارتكبت الجنايات أو الجنح بأراضي المملكة المغربية، وكذلك إذا كانت الجنايات قد وقع الحكم فيها نهائيا في المغرب...».

من أجل مكافحة جرائم الأنترنيت وكذلك تندرج في إطار انعقاد العديد من المؤتمرات فهي كلها تعتبر جهود دولية لتعزيز التعاون من أجل الحد ومكافحة الجريمة السيبرانية.

الفقرة الأولى: **معاهدة بودابست.**

في سنة 2000 تقدمت اللجنة الاوروبية بمشروع معاهدة حول مشكلات الجرائم المعلوماتية والحساب الآلي وفي سنة 2001 تمت المصادقة على معاهدة بودابست المتعلقة بمكافحة الجريمة عبر الأنترنت و التي بلورت أسس التعاون والتضامن الدولي في محاربتها ومحاولة الحد منها خاصة بعد أن وصلت تلك الجرائم إلى حد خطير أصبح يهدد الأشخاص والممتلكات ، وبعد التوقيع على تلك المعاهدة الدولية الخطوة الأولى في مجال تكوين تضامن دولي مناهض لتلك الجرائم التي تتم عبر شبكة الأنترنت و استخدامها استخدام سيء وبناء عليه قد وقعت تلك المعاهدة 26 دولة أوروبية بالإضافة إلى كندا وجنوب أفريقيا والولايات المتحدة الأمريكية. وللمعاهدة أهمية قصوى في توفير أسس الأمن العام، وتتضمن تلك المعاهدة 48 مادة وبعد التوقيع على تلك المعاهدة دوليا التي تهدف إلى توحيد الجهود الدولية في مجال مكافحة جرائم الأنترنت والتي انتقلت من مرحلة ابتدائية كانت تتمثل في محاولات التسلل البريئة التي كان يقوم بها الهواة في الأغلب الحالات ودون أي فرض إجرامي إلى مرحلة جديدة يقوم بها محترفون على أعلى درجة من التخصص وتتمثل في الاحتيال والاختلاس وجرائم تهديد الحياة وهي قضايا تعرض حياة وممتلكات الكثير من رواد شبكة الأنترنت للخطر.

سطر الهدف الأساسي لهذه الاتفاقية صادق عليها المغرب سنة 2014[36] ضمن ديباجيتها بكونه اتباع سياسة جنائية مشتركة تهدف إلى حماية المجتمع من الجرائم الإلكترونية، لاسيما من خلال اعتماد التشريعات المناسبة وتعزيز التعاون الدولي، وتهدف الاتفاقية بشكل أساسي إلى:

-مواءمة عناصر القانون الجنائي الموضوعي للجرائم والأحكام ذات الصلة في مجال الجريمة الإلكترونية.

-توفير سلطات قانون الإجراءات الجنائية المحلية اللازمة للتحقيق والملاحقة القضائية لمثل هذه الجرائم وكذلك الجرائم الأخرى المرتكبة عن طريق نظام الكمبيوتر أو الأدلة المتعلقة بها في شكل الكتروني.

-إقامة نظام سريع وفعال للتعاون الدولي للحد من الجرائم السيبرانية.

وقد عرفت هذه الاتفاقية مجموعة من الجرائم السيبرانية من قبيل الوصول غير المشروع اعتراض غير قانوني تدخل البيانات والتدخل نظام وإساءة استخدام الأجهزة، ذات الصلة بالحاسوب التزوير ذات الصلة بالحاسوب الاحتيال والجرائم المتعلقة المواد الإباحية عن الأطفال والجرائم المتعلقة بحق المؤلف والحقوق المجاورة.

كما حددت قضايا المرتبطة بالقانون الإجرائي مثل الحفظ العاجل للبيانات المخزنة، والحفظ العاجل والكشف الجزئي لبيانات المرور، وأمر الإنتاج، والبحث عن بيانات الكمبيوتر والاستيلاء عليها، وجمع بيانات حركة المرور في الوقت الفعلي، واعتراض بيانات المحتوى بالإضافة إلى ذلك، تحتوي الاتفاقية على حكم بشأن نوع معين من الوصول عبر الحدود إلى بيانات الكمبيوتر المخزنة التي لا تتطلب مساعدة متبادلة بموافقة أو حيثما تكون متاحة للجمهور) وتنص على إنشاء شبكة على مدار الساعة طوال أيام الأسبوع لضمان المساعدة السريعة بين الأطراف الموقعة. علاوة على ذلك، وكشروط وضمانات، تتطلب الاتفاقية توفير الحماية الكافية لحقوق الإنسان والحريات بما في ذلك الحقوق الناشئة عملا بالالتزامات

[36] ظهير شريف رقم 1.14.85 صادر في 12 من رجب 1435 (12 ماي 2014) بتنفيذ القانون رقم 136.12 الموافق بموجبه على اتفاقية الجرائم المعلوماتية الموقعة ببودابست في 23 نوفمبر 2001 وعلى البروتوكول الإضافي لهذه الاتفاقية، الموقع ستراسبورغ في 28 يناير 2003، منشور بالجريدة الرسمية عدد 6260 بتاريخ 29 ماي 2014.

بموجب الاتفاقية الأوروبية لحقوق الإنسان، والعهد الدولي الخاص بالحقوق المدنية والسياسية، وغير ذلك من صكوك حقوق الإنسان الدولية المعمول بها، ويجب أن تتضمن مبدأ التناسب[37].

ب) – الاتفاقيات الإقليمية الدولية لمكافحة الجريمة السيبرانية:

الفقرة الثانية: الاتفاقية العربية لمكافحة جرائم تقنية المعلومات[38]

إن الدول العربية الموقعة، رغبة منها في تعزيز التعاون فيما بينها لمكافحة جرائم تقنية المعلومات التي تهدد أمنها ومصالحها وسلامة مجتمعاتها، واقتناعا منها بضرورة الحاجة إلى تبني سياسة جنائية مشتركة تهدف إلى حماية المجتمع العربي ضد جرائم تقنية المعلومات وأخذا بالمبادئ الدينية والأخلاقية السامية ولا سيما أحكام الشريعة الإسلامية، وكذلك بالتراث الإنساني للأمة العربية التي تنبذ كل أشكال الجرائم، ومع مراعاة النظام العام لكل دولة، والتزاما بالمعاهدات والمواثيق العربية والدولية المتعلقة بحقوق الإنسان ذات الصلة من حيث ضمانها واحترامها وحمايتها. تضمنت الاتفاقية خمسة فصول وأربعة وثلاثون مادة.

فالهدف من الاتفاقية هو تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات، لدرء أخطار هذه الجرائم حفاظاً على أمن الدول العربية، ومصالحها، وسلامة مجتمعاتها وأفرادها حيث وقع المغرب على هذه الاتفاقية سنة 21\12\2014 ووافق عليها مجلسا وزراء الداخلية والعدل العرب في اجتماعهما المشترك المنعقد بمقر الأمانة العامة لجامعة الدول العربية بالقاهرة بتاريخ 1432/ 1/ 15 هـ الموافق 2010 / 12 / 21 م. تسري هذه الاتفاقية بعد مضي ثلاثين يوما من تاريخ إيداع وثائق التصديق عليها أو قبولها أو إقرارها من سبع دول عربية بموجب الفقرة (3) من الاحكام الختامية للاتفاقية.

ففي الفصل الأول من الاتفاقية المتعلق بالأحكام العامة الذي يتضمن تعريفا لبعض المصطلحات المتعلقة بمجال المعلوماتي وكل مجالات تطبيق هاته الاتفاقية وصيانة السيادة لكل دولة طرف في الاتفاقية. وفيما يخص الفصل الثاني الذي يكمن في طياته العديد من المواد المتعلقة بالتجريم اي على كل دولة طرف الالتزام بتجريم الأفعال المنصوص عليها ضمن هذا الفصل مثلا جريمة الاعتداء على سلامة البيانات وجريمة إساءة استخدام وسائل تقنية المعلومات وغيرها من الجرائم الماسة بنظام المعلوماتي. وفي الفصل الثالث هناك عديد من المواد التي تحدد الأحكام الإجرائية. كما أن التعاون القانوني القضائي يندرج في الفصل الرابع من الاتفاقية وكذلك يضم الفصل الخامس أحكام ختامية[39].

خاتمة:

إن الامن كان ولازال الركيزة الأساسية للمجتمع، بحيث لا يمكن تصور نمو أي نشاط بعيداً عن تحققه، سواء أكان ذلك، على المستوى التقني، أم على المستوى القانوني. وقد تحول الأمن، مع بروز مجتمع المعلومات، والفضاء السيبراني، إلى واحد من قطاع الخدمات، التي تشكل قيمة مضافة ودعامة أساسية لأنشطة الحكومات والأفراد، كما هو الحال التطبيقات الخاصة بالحكومة الإلكترونية، والصحة الإلكترونية، والتعليم عن بعد مع والعقود الالكترونية، التجارة الإلكترونية، والأنظمة البنكية. إلا ان الوجوه المتعددة للأمن السيبراني، ومضاعفاتها الخطيرة التي لا تقف عند حدود الاساءة إلى الأفراد والمؤسسات،

---

[37] للاطلاع على الاتفاقية كاملة باللغة العربية، المرجو زيارة الموقع:
https://Ram.coe.int/budapest-convention-in-arabic/1680739173

[38] حررت هذه الاتفاقية باللغة العربية بمدينة القاهرة في جمهورية مصر العربية في 1432/1/15هـ الموافق 2010/12/21م من أصل واحد مودع بالأمانة العامة لجامعة الدول العربية الأمانة الفنية لمجلس وزراء العدل العرب)، ونسخة مطابقة للأصل تسلم للأمانة العامة لمجلس وزراء الداخلية العرب، وتسلم كذلك نسخة مطابقة للأصل لكل دولة من الدول الأطراف، وإثباتا لما تقدم، قام أصحاب السمو والمعالي وزراء الداخلية والعدل العرب بتوقيع هذه الاتفاقية نيابة عن دولهم.

[39] انظر الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

بل تتعداها إلى تعريض سلامة الدول والحكومات والقطاعات المهمة والأجهزة الدول تزيد مهمة القيمين على الموضوع تعقيداً وصعوبة وتستدعي مقاربة شاملة ومتكاملة لجميع التحديات التي يطرحها الفضاء السيبراني، بحيث تأتي الردود والحلول المقترحة ناجعة وفاعلة فتحقيق الأمن وبناء الثقة في الفضاء السيبراني، من أساسيات تسخير تقنيات المعلومات والاتصالات، في مجالات التنمية خدمة للمجتمع المعلوماتي، وعلى هذا الأساس تبنت الدول العديد من الاستراتيجيات وخلق التعاون على المستوى العالمي من اجل احداث فضاء سيبراني آمن وتعزيز الثقة في المعاملات الرقمية ومحاربة الجرائم التي قد تهدد أمن المجتمع المعلوماتي بصفة عامة والأمن البنكي بصفة خاصة، حيث المغرب يشكل جزء من التعاون الدولي في هذا المجال من خلال توقيع عدة اتفاقيات دولية وإقليمية كما بادر في خلق استراتيجيات على المستوى الوطني لحماية النظم المعلوماتية وتعزيز الثقة في المعاملات الرقمية من اجل بناء مغرب رقمي آمن. اذ يمكن القول ان المغرب في تطور مستمر من أجل تحقيق المبتغى ومواكبة العصر ومنافسة الدول في المجال الرقمي ولاحظنا ذلك في الإستراتيجيات والقوانين التي سنها بخصوص هذا المجال. الا انه ورغم كل الجهود المبذولة على المستوى الدولي والوطني نجد أن لم يتم الحد من مخاطر الفضاء السيبراني بنسبة مهمة وذلك راجع لعدة أسباب منها:

ضعف التعاون الدولي سواء على المستوى التشريعي أو الإجرائي أو المؤسساتي في تحقيق الأمن السيبراني، عدم انخراط كل الدول في التعاون من أجل مكافحة الجريمة السيبرانية العابرة للحدود، وكذا ضعف التواصل بين الدول.

وعلى المستوى الوطني نجد أن المغرب رغم مواكبته للعصر وخلق عدة استراتيجيات وقوانين إلا أنه لا يزال هناك بعض الثغرات يجب سدها منها ثغرات تشريعية واجرائية ومؤسساتية.

مقترحات:

وفي الختام ارتأينا الى وضع بعض المقترحات من شأنها تسليط الضوء على بعض النقط الرئيسية التي يجب إعادة النظر فيها ومن أهمها:

- ضرورة إعادة النظر في بعض المقتضيات القانونية الإجرائية التي تعرقل وسائل كشف واثبات الجريمة السيبرانية خاصة المتعلقة بالأنظمة البنكية نظرا لما تخلقه الوسائل التقليدية من إشكالات أمام ضعف نجاعتها في الكشف عن الجريمة المتعلقة بالأنظمة البنكية، وبالتالي الارتقاء بقدرات المحققين، وكذا استغلال الأدلة الرقمية بالوسائل الإجرائية الحديثة في اثبات الجريمة.
- خلق مراكز جديدة وبآليات مستجدة لمواكبة الفضاء السيبراني والمعاملات الرقمية البنكية ومراقبة التدخل الغير المصرح به.
- منع اختراع التطبيقات والمواقع التي لها أضرار سلبية.
- احداث آليات جديدة لمحاربة الفيروسات الخبيثة، ومنعها من الدخول الأجهزة.
- خلق مراكز تكوينية في مجال الأمن السيبراني وتلقي تكوينات لساهرين على القطاع التكنولوجي في كل المؤسسات التابعة للدولة والبنوك.
- ينبغي دعم التنمية الفعالة والإسراع في تنفيذ التشريعات الوطنية والدولية لتحصين الأمن السيبراني.
- اعادة تأهيل المجرمين السيبرانيين وذلك بهدف استغلال قدراتهم وذكائهم بشكل إيجابي من أجل تدعيم المنظومة الأمنية على المستوى الوطني والعالمي.
- ضرورة تكوين القضاة في المجال المعلوماتي، من أجل مواكبتهم لمستجدات الجريمة السيبرانية، إذ لا يعقل عدم إلمام القاضي بخصائص الجريمة السيبرانية ومخاطرها وطرق ارتكابها وبالتالي كيف سنكون قضاء قادر على خلق اجتهادات قضائية فريدة مواكبة الفضاء السيبراني؟ مع ضرورة خلق خلية خاصة بالمحاكم تهتم بالجرائم المعلوماتية والتهديدات السيبرانية من أجل تخفيف العبء على المنظومة القضائية وتسريع وسائل التدخل الاستباقي.

- إنشاء مختبر عالمي للأدلة الجنائية الرقمية وذلك بغية الإسراع في الكشف عن الجرائم السيبرانية العابرة للحدود والماسة بأمن الدولة وبالمجتمع العالمي، وكذا تطوير الوسائل والخبرات ومواكبتها.
- إحداث مؤسسات عالمية متطورة من اجل دعم المؤسسات المتواجدة حاليا، بغرض الكشف السريع عن الجرائم السيبرانية بشكل استباقي.
- ضرورة تعزيز التعاون بين جهات الاتصال الكبرى بالبلد مع المصالح الأمنية المختصة بالأمن السيبراني، مع ضرورة الاعتماد على صد الإجرام بشكل استباقي.
- ضرورة تعزيز التعاون بين الأبناك الوطنية والجهات الأمنية بغية صد أي تزوير للأموال أو غسلها، أو في جرائم النصب.
- التأكيد على ضرورة التوعية القانونية والأمنية للمجتمع المغربي بشكل عام، وتوعية الشباب والأطفال بشكل خاص بمخاطر العالم الافتراضي والإنترنيت، وبالمقتضيات القانونية التي تهم الجريمة السيبرانية، من خلال حملات التوعية في المدارس وعبر محطات الإذاعة والشبكة العنكبوتية.

لائحة المراجع:

المراجع باللغة العربية:

- **الكتب:**

أولا: الكتب العامة:

1. أحمد فتحي سرور: حكم القانون في مواجهة الارهاب الدار الجامعية بيروت – لبنان 2005.
2. محمد عبد الشافي إسماعيل، مبدأ حرية القاضي الجنائي في الاقتناع، دراسة مقارنة، دار المنار القاهرة، 1992.
3. محمد علي شهيب: إدارة العمليات والإنتاج في المؤسسات الصناعية والخدمية"، مطبعة جامعة القاهرة، الطبعة الرابعة، مصر، 1989.

ثانيا: الكتب الخاصة:

1. أبا خليل التعاقد الالكتروني في ضوء القانون 53.05 المتعلق بالتبادل الالكتروني للمعطيات القانونية، مطبعة الأمنية بالرباط، الطبعة الأولى لسنة 2020.
2. إدريس النوازلي: الكترونية الجريمة الملكية الفكرية وقرصنتها نموذجا، مطبعة النجاح الجديدة الدار البيضاء- الطبعة الأولى: 2018.
3. أمير فرج يوسف، جريمة مكافحة الارهاب الالكتروني، دار الكتب والدراسات العربية، مصر طبعة 2016.
4. بشرى حسين الحمداني: القرصنة الالكترونية أسلحة الحرب الحديثة – عمان – الطبعة الأولى 2014.
5. حسن طاهر داوود أمن شبكات المعلومات مركز البحوث بمعهد الإدارة العامة، المملكة العربية السعودية، طبعة 2004.
6. خالد بن سليمان -الغثبر – محمد بن عبد الله القحطاني: "أمن المعلومات، معهد الإدارة العامة- المملكة العربية السعودية، الطبعة الأولى 2009.
7. خالد حسن أحمد لطفي: الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية، دار الفكر الجامعي للطباعة والنشر، الطبعة الأولى 2019.
8. ذيب بن عايض القحطاني أمن المعلومات، فهرسة مكتبة الملك فهد أثناء النشر الرياض 2010.
9. ذيب بن عايض القحطاني: أمن المعلومات مكتبة الملك فهد الوطنية الرياض طبعة 2010 سعد غالب ياسين نظم المعلومات الإدارية، دار الجنان للنشر والتوزيع عمان، الطبعة الأولى 2012.
10. سليم إبراهيم الحسنية نظم المعلومات الإدارية مؤسسة الوراق للنشر والتوزيع، الطبعة الثانية، الأردن 2002.
11. سليمان مصطفى الدلاهمة: أساسيات نظم المعلومات المحاسبية وتكنولوجيا المعلومات، مؤسسة الوراق، عمان، الطبعة الأولى، 2008.
12. ضابيان شمام حسن الزبيدي: نظم المعلومات وأثرها في التخطيط الاستراتيجي، دار الجنان للنشر والتوزيع، الطبعة الأولى.
13. طلعت أسعد عبد الحميد "التسويق الفعال"، مكتبة الشقري، مصر، بدون ذكر سنة الطبع.
14. -عائشة بن قارة مصطفى حجية الدليل الالكتروني في مجال الإثبات الجنائي، دار الجامعة الجديدة، مصر، 2010.
15. عبد الجليل إسماعيل حسن الشيخ زيني: "الإرهاب" الالكتروني في القانون الدولي (الماهية والجزاء)، منشورات الحبلى الحقوقية بيروت - لبنان، الطبعة الأولى 2020.

16. عبد الجليل مهرار السياسة الجنائية في المجال المعلوماتي في التشريع المغربي، مطبعة دار القلم بالرباط، الطبعة الأولى 2022.
17. عبد الرحمان الدباغ - عماد الصباغ: مبادئ نظم المعلومات الإدارية الحاسوبية - عمان دار زران للنشر والتوزيع، سنة 1996.
18. عبد الله الكرجي - صليحة حاجي التعاقد الرقمي ونظم الحماية الإلكترونية، الطبعة الأولى 2015 مكتبة الرشاد سطات.
19. عبد المنعم سليمان: الجوانب الاشكالية في النظام القانوني لتسليم المجرمين دار الجامعة الجديدة، الإسكندرية، 2010.
20. عزالدين أمين الأموي الجرائم المعلوماتية في ضوء التشريع والقضاء المغربي واليمني المكافحة الموضوعية والإجرائية، دراسة مقارنة دون ذكر دار النشر، الطبعة الأولى 2021.
21. عفيفي كامل عفيفي: جرائم الكمبيوتر وحقوق المؤلف والمصنفات الرقمية ودور الشرطة والقانون، منشورات الحلبي الحقوقية، بيروت لبنان، الطبعة الثانية، لسنة 2007.
22. عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، منشورات الحلبي الحقوقية منشورات الحلبي الحقوقية، الطبعة الأولى بيروت 2003.

- **الرسائل والأطروحات:**

1. الناجم كوبان "دور التعاون الدولي في مكافحة الجريمة المعلوماتية"، أطروحة لنيل شهادة الدكتوراه في الحقوق، كلية العلوم القانونية والاقتصادية والاجتماعية اكدال، جامعة محمد الخامس بالرباط 2020/2021.

- **المقالات:**

1. أحمد عبيس الفتلاوي" الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضود التنظيم الدولي المعاصر"، مجلة المحقق الحلي للعلوم القانونية والسياسية – العدد الرابع، سنة 2016.
2. إدريس بلمحجوب تأثير الجريمة الالكترونية على الائتمان المالي، سلسلة ندوات محكمة الاستئناف بالرباط العدد السابع، مطبعة الأمنية بالرباط.
3. سعد بن عجيبة الجريمة السيبرانية، مفهومها، خصائصها والمشاركة المباشرة فيها مقال منشور في المجلة الدولية للأبحاث الجنائية والحكامة الأمنية.
4. فاطمة بيرم: السيادة الوطنية فى ظل الفضاء السيبراني والتحولات الرقمية "الصين نموذجا، مقال منشور بالمجلة الجزائرية للأمن الإنساني، العدد 1.
5. محمد جوهى: قراءة في قانون المسطرة الجنائية المغربي من خلال بعض المهام المسندة إلى النيابة العامة ، المجلة المغربية للقانون والاقتصاد والتنمية العدد 23، 1990.
6. محمد يسري قسوة" التنظيم ومفهوم النظام، مجلة البنوك الإسلامية، العدد 52، 1987 منى عبد الله السمحان متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، مقال منشور في مجلة كلية التربية - جامعة المنصورة، العدد 111.
7. يوسف قجاج: خصوصية القواعد الإجرائية في مجال البحث عن الجريمة الالكترونية دراسة مقارنة -، منشورات مجلة المنارة للدراسات القانونية والإدارية العدد 14، مطبعة دار السلام دون ذكر الطبعة.

المراجع باللغة الأجنبية.

أولا: المراجع باللغة الفرنسية

Les ouvrages: ▪

1. Micheal S.Fuertes. <<cyber warfare.unjust Actins in a just war "Florida International University. Full 2013.p:1.
2. &Chakib ELOUFI – Amina DIK: La complémentaité du droit de la sécurité en matière informatique, Revue Marocaine du droit commercial et des affaires, N°3.2015.P:35.
3. &Jay Forder et Patick QUIRK, L'électronique commerce et la loi, willey,2001,p:8.

- **Articles :**

1. & Revue, INTERFACE. Article : « confiance numérique : le maroc se dote d'une dispositif approprie »>,édite par-la ministère de l'industrie du commerce et des nouvelles technologies,N°18 4eme trimestre 2010,p:21-22.

2. Revue, INTERFACE. Article: «< confiance numérique : le maroc se dote d'une dispositif approprie »>,édite par-la ministère de l'industrie , du commerce et des nouvelles technologies,N°18 4eme trimestre 2010.

ثانياً: المراجع باللغة الانجليزية.

- **Books :**

1. Jankoweki, Piotr, Nyerges Timorty << Geographic Information Systems Far Group Decision Making, New YORK, Francis, 2003.
2. Michael withman, Herbert J Mattord << Principles of Information security >>,Thomson; second Edition;2005.