تكريس الأمن السيبراني لنظام الحماية الاجتماعية

Dedicating cybersecurity to the social protection system

الدكتور المصطفى طايل

Elmostapha Taile

أستاذ باحث بكلية العلوم القانونية والاقتصادية والاجتماعية جامعة مُحَمَّد الأول وجدة

بدر الحيمودي

Bader el himoudi

باحث دكتوراه في القانون الخاص بكلية العلوم القانونية والاقتصادية والاجتماعية جامعة مُحَمَّد الأول وجدة

ملخص:

أمام التحديات والاكراهات التي تعرفها منظومة الحماية الاجتماعية من جرائم الكترونية وهجمات سيبرانية والتي تعرف تزايدا ملحوظا في السنوات الأخيرة، عملت المملكة المغربية تحت القيادة الرشيدة لصاحب الجلالة الملك مُحَمَّد السادس نصره الله إلى اعتماد رؤية استباقية تعزز الجهود الرامية لتحصين الأمن المعلوماتي وحماية الفضاء السيبراني وتعزيز الثقة في المعاملات الرقمية عبر وضع استراتيجيات وطنية تعتمد بالأساس على آليات قانونية ومؤسساتية

وتتجلى مخاطر إختراق الأنظمة المتعلقة بالحماية الاجتماعية بوصفها ظاهرة مستحدثة، من خلال السهولة في تنفيذ المخططات الإجرامية، وتسهيل التواصل بين الشبكات الإجرامية في أسرع وقت ممكن عبر العالم بأسره قصد تحقيق الأهداف المتمثلة في إختراق معلومات نظام الحماية الاجتماعية على عكس الجرائم التقليدية التي تطلب جهدا ووقتا كبيرا.

Summary:

In the face of the challenges and constraints facing the social protection system in terms of electronic crimes and cyber attacks, which have witnessed a noticeable increase in recent years, the Kingdom of Morocco worked under the wise leadership of His Majesty King Mohammed VI, may God assist him, to adopt a proactive vision that enhances efforts aimed at fortifying information security, protecting cyberspace, and enhancing confidence in Digital transactions by developing national strategies that rely primarily on legal and institutional mechanisms

The risks of hacking into systems related to social protection are evident as a new phenomenon, through the ease in implementing criminal schemes, and facilitating

communication between criminal networks as quickly as possible throughout the entire world in order to achieve the goals of hacking into the information of the social protection system, in contrast to traditional crimes that require a great deal of effort and time.

مقدمة:

جعل التقدم الكبير في تكنلوجيا المعلومات والاتصالات من الأمن 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 وإستهداف 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 فإنه بات من الضروري تحسين وتجويد الحماية الاجتماعية يتطلب حلول تقنية مدعومة بالذكاء الصناعي في جمع وتخزين البيانات الضخمة الخاصة بسجلات الحماية الاجتماعية، هذه المعلومات التي غالبا ماتكون شديدة الخصوصية فهي تتضمن جمع المعلومات الشخصية والاكلينيكة حيث تهدف إلى مقدمي خدمات الحماية الاجتماعية إلى الوصول إلى السجلات بسهولة وتتيح لهم للمستفيدين من التحكم في سجلاتهم الشخصية، هذا الكم المعلوماتي الضخم جعل نظام الحماية الاجتماعية هدفا لعمليات القرصنة والهجمات السبيرانية،و تحدث هذه الهجمات الالكترونية عبر ثلاث محدادت رئيسية كمنافذ للهجمات الالكترونية وهي:المحدد التقني للأجهزة الذكية والكمبيوتر، الحوسبة السحابية، والشبكات من هنا برزت الضرورة الملحة للأمن السيبراني التي أولتها المملكة المغربية تحت القيادة الرشيدة لصاحب الجلالة الملك مُحَمَّد السادس نصره الله أهمية قصوى للعمل على حماية الأنظمة والشبكات والبرامج والبيانات من المخاطر الداخلية والخارجية من أي إستخدام أو إفصاح أو تعطيل أو تدمير غير مصرح به وضمان سرية وسلامة الفئات المشمولة بنظام الحماية الإجتماعية سواء من القرصنة أو أي عطل في أداء النظام، ولايغيب عن البال أن الأمن السيبراني يقوم على عدة عناصر أساسية أهمها السرية والخصوصية هذه الأخيرة التي تعني عدن إتاحة أي معلومات أو الكشف عنها للأشخاص غير المعنين بذلك أو العمليات غير المصرح بها ومنها أيضا سلامة البيانات وعدم تغييرها وتدبيرها بشكل غير مصرح به بالإضافة إلى إستمرارية وتوفر المعلومات لنظام الحماية الاجتماعية للأشخاص المعنيين بها لتكون جاهزة للاستخدام الشخصي المصرح له بذلك وحتى تكلل هذه الجهود بالنجاح لابد من تظافر الجميع وذلك على إعتبار أن الأمن السيبراني يتكون من مراتب وطبقات متعددة حزء منها يعتمد على المستخدم تفسه وفهمه لمبادئ أمان البيانات الأساسية مثل إختيار كلمات السر القوية والحذر من الروابط والمرفقات المجهولة المصدر وتحديث النسخ الاحتياطية للبيانات بشكل دوري سيتم الحديث عن تكريس الأمن السيبراني.

وتحذر الإشارة إلى أن الارهاصات الأولى لمصطلح الأمن السيبراني بدأت في الدول المتقدمة فهي السباقة لتبني امن سبيراني 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 وكذا القوانين المتعلقة بتعزيز الثقة الرقمية ولا ننسى اهم الاستراتيجيات المتخدة لتصدي للجريمة المعلوماتية وحماية النظم البنكية وتعزيز الثقة في المعاملات الرقمية. ففي سنة 2020 سن المغرب قانون 05.20 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، وذلك من خلال الاستراتيجيات الجديدة والمبتكرة من أجل ردع هجمات إلكترونية غير متوقعة على العديد من المواقع والمنصات الإلكترونية المهمة والحساسة.

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 لنظام الحماية الاجتماعية يمنع الإعتداء عليها وهنا تتجلى أهمية الأمن السيبراني لتحقيق وتوفير هذا الإطار للأفراد والمؤسسات والحكومات في علاقة التفاعل التي فيما بينهم

- **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 الإجتماعية ويذهب بالمجتمع نحو مجتمع واعي ومتقدم وراقي مليئ 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 الإستخدام السيء.

- **على المستوى القانوني:**

يتميز الجانب القانوني في أي مجال مواكبة التطورات التي تطرأ عليه وتوفير الإطار القانوني منظم لنظام الحماية الاجتماعية وتفعيل الحماية القانونية له 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 لنظام الحماية الاجتماعية.

- **على المستوى الأمني:**

كما نعلم المهمة الأولى للأمن هو السهر على توفير الأمان للمواطنين وبما ان كل المواطنين يتعاملون بالمعلوميات في كل مشاغلهم اليومية ويضعون فيها معلوماتهم الشخصية لاسيما في إطار نظام الحماية الاجتماعية لذلك يجب على الأمن مواكبة كل ما يمس

أمن المواطنين والعمل على توفير أشخاص الأمن لديهم خبرة في المجال السيبراني لرصد أي فعل اجرامي في هذا المجال ولاسيما مجال الحماية الاجتماعية.

- **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.

إشكالية الموضوع.

تبنت المملكة المغربية إستراتيجية محكمة وفق القانون 05.20 وكذا التعاون الدولي لحماية الفضاء السيبراني من الجرائم المرتبطة بالحماية الاجتماعية التي قد تمسها عن طريق ا قواعد قانونية جد محكمة في إطار تفعيل الطابع التدولي للمواثيق والإتفاقيات الدولية ولتحليل هذا الموضوع نقترح إشكالية مفادها:

هل استطاع المشرع المغربي توفير مجال سيبراني آمن لحماية نظام الحماية الاجتماعية وتعزيز الثقة الرقمية داخل المملكة المغربية ؟

ومن خلال الإشكالية أعلاه يمكن طرح تساؤلات فرعية تتجلى في:

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

-أين تكمن التهديدات السيبرانية وما دوافعها ؟

-إلى أي مدى إستطاع المغرب التصدي للهجمات السيبرانية وتعزيز الثقة في المعاملات الرقمية المرتبطة بالحماية الاجتماعية ؟

-ما الجهود المبذولة على المستوى العالمي والإقليمي والوطني؟

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

خطة البحث

المبحث الأول: تكريس الامن السيبراني لنظام الحماية الاجتماعية على المستوى الأمني

المبحث الثاني: تجليات نظام الحماية الاجتماعية في ضوء الأجهزة المنصوص عليها في القانون 05.20

المبحث الأول: تكريس الامن السيبراني لنظام الحماية الاجتماعية على المستوى الأمني

أمام التحديات والاكراهات التي تعرفها منظومة الحماية الاجتماعية من جرائم الكترونية وهجمات سيبرانية والتي تعرف تزايدا ملحوظا في السنوات الأخيرة، عملت المملكة المغربية تحت القيادة الرشيدة لصاحب الجلالة الملك مُحَمَّد السادس نصره الله إلى اعتماد رؤية استباقية تعزز الجهود الرامية لتحصين الأمن المعلوماتي وحماية الفضاء السيبراني وتعزيز الثقة في المعاملات الرقمية عبر وضع استراتيجيات وطنية تعتمد بالأساس على آليات قانونية ومؤسساتية

وتتجلى مخاطر إختراق الأنظمة المتعلقة بالحماية الاجتماعية بوصفها ظاهرة مستحدثة، من خلال السهولة في تنفيذ المخططات الإجرامية، وتسهيل التواصل بين الشبكات الإجرامية في أسرع وقت ممكن عبر العالم بأسره قصد تحقيق الأهداف المتمثلة في إختراق معلومات نظام الحماية الاجتماعية على عكس الجرائم التقليدية التي تطلب جهدا ووقتا كبيرا.

وأمام كل هذه الأوضاع وتنامي الاعتداءات والأفعال الاجرامية للأنظمة المتعلقة بالحماية الاجتماعية، لجأت جل الدول والتشريعات إلى اعتماد سياسة جنائية، من خلال محاولة التفكير في وضع ترسانة قانونية، تستجيب للتطورات الحاصلة على مستوى الجريمة في جميع مستوياتها ووضع نصوص جنائية تجرم وتعاقب على هذه الأفعال الشنيعة التي تهدد أمن واستقرار الدول، وأمام الصعوبة والتقيد التي تتميز به الجريمة الالكترونية بصفة عامة وجريمة إخراق الأنظمة المتعلقة بالحماية الاجتماعية في المغرب بصفة خاصة، فإن الأمر يتطلب بالإضافة إلى ما سبقت الإشارة إليه، تكثيف الجهود الوطنية من خلال الاعتماد على آليات وأجهزة قادرة على توفير الحماية الازمة للأنظمة المتعلقة بالحماية الاجتماعية في بلادنا والعمل على تكريس الأمن السيبراني وتعزيزه ولعل من بين الأجهزة التي تناط إليها مهمة تكريس الأمن السيبراني ببلادنا نجد النيابة العامة والشرطة القضائية أولا وبعض الأجهزة المنصوص عليها في القانون 05.20 ثانيا.

المطلب الأولى: دور النيابة العامة والشرطة القضائية في تعزيز الأمن السيبراني لنظام الحماية الاجتماعية.

إن رئاسة النيابة العامة تسهر على تتبع كل القضايا المتعلقة بالجرائم المعلوماتية، وذلك بتنسيق تام بين النيابات العامة بمختلف محاكم المملكة كما تعمل على تنفيذ الالتزامات الدولية وفق الإتفاقيات والمعاهدات التي صادق عليها المغرب من قبيل تنفيذ طلبات حفظ بيانات الكومبيوتر الواردة من الدول الأعضاء التي صادقت على اتفاقية بوادبست.

ومما تجدر الإشارة إليه أنه في إطار تنزيل مضامين السياسة الجنائية الوطنية في مجال مكافحة الجريمة المعلوماتية المتعلقة بالحماية الاجتماعية تم وضع استراتيجيات تسعى إلى تطوير وتعزيز قدرات قضاتها في إطار مستجدات الأمن السيبراني.

وجدير بالذكر أنه في إطار جرائم المس بنظم المعالجة الآلية للمعطيات تم رصد احصائيات مهمة من قبل رئاسة النيابة العامة حيث تابعت النيابات العامة 239 شخصا بسبب ارتكابهم لهذه الجرائم وفتحت في مواجهتهم 117 قضية ومن خلال تعزيز التعاون الأمني للتصدي للجرائم المعلوماتية، وبادرت رئاسة النيابة العامة إلى تعزيز التعاون بين مختلف المتدخلين الوطنيين والدوليين وذلك من خلال ما يلي:

-تثبيت طلبات التعاون الواردة في إطار شبكة 24/7 لاتفاقية بوادبست.

-إعداد مشروع التقرير السنوي بشأن وضعية الجريمة الإلكترونية والدليل الرقمي بالمغرب[1].

-إعداد دليل تكوين في الجريمة المعلوماتية.

إن رئاسة النيابة العامة أبدت اهتمامها بظاهرة العملات المشفرة، مثل البتكوين، منذ ظهورها، وقد تبين ذلك بشكل جلي من خلال رصد هذه الظاهرة في إطار الاحصائيات المسجلة بشأن استعمال هذه العملات المشفرة قد تم رصد في الثلاث سنوات الأخيرة 20 قضية، من بينها 13 قضية خلال سنة 2020 إلا أنه ما يثير الانتباه هو تسجيل قضايا تتعلق باقتناء كولولجيا التعديل هذه العمولات المشفرة وخاصة (البتكوين)[2].

ونظرا لغياب إطار قانوني واضح يؤطر التعامل بالعملات المشفرة، ولتباين وجهات النظر ومختلف المحاكم التي عرضت عليها مثل هذه القضايا، فقد بادرت رئاسة النيابة العامة إلى عد اجتماع لتدارس هذه المشكلة حضرته مجموعة من القطاعات المعنية.

وقد خلص الاجتماع المذكور إلى ما يلي:

-ضم رئاسة النيابة العامة وباقي المتدخلين إلى اللجنة المشكلة على مستوى بنك المغرب لتدارس هذه المشكلة.

-إنجاز دراسة شاملة لهذه الظاهرة قصد الوقوف على تفاصيلها، وإيجاد الحلول الكفيلة بتأطيرها على مستوى السياسة المالية والسياسة الجنائية.

-تنظيم يوم دراسي حول هذه الظاهرة من أجل الخروج بتوصيات يتم اعتمادها من قبل المسؤولين عن وضع السياسات العمومية في المستقبل.

وجذير بالذكر أنه تتميز الجرائم المعلوماتية بكونها جرائم تقنية تنشأ في الخفاء يرتكبها مجرمون أذكياء يمتلكون أدوات المعرفة التقنية التي توجه للنيل من الحق في المعلومات وتطال اعتداءاتها معطيات الحاسوب المخزنة والمعلومات المنقولة عبر نظم وشبكات المعلومات، لذا فالتصدي لها يقتضي وجود عناصر خاصة من الضابطة القضائية لها من التكوين العلمي والمعرفي في ميدان المعلوميات ما يكفي لمكافحة هذا النشاط الإجرامي الحديث، وهذا لا يتحقق إلا بعد تلقيها التعليم والتدريب الكافيين على استخدام شبكات الاتصال واستخدام الأجهزة الفنية الحديثة والمعرفة الكافية باللغات الأجنبية، مما يسمح لها بالقيام بإجراءات التفتيش والضبط والتحفظ على الأدلة التي تساعد على إثبات الجريمة.

وهكذا يستشف مما سبق الإشارة إليه أعلاه أن جهاز النيابة العامة يلعب دورا مركزيا في ضل السياسة الجنائية المغربية في جل الجرائم التي تعترض الأشخاص سواء المعنويين أو الطبيعيين، وفي هذا الإطار اعتبر الوكيل العام للملك، رئيس النيابة على أن المغرب استفاد من التجربة الدولية في المجال الإلكتروني، حيث أنه استفاد من مجموعة من برامج المساعدة التقنية خاصة في إطار برامج سيبير سود وكلاكسي بلوس[3] التي تنفذ بدعم ورعاية مجلس أوروبا حيث كان من نتائجها تكوين متخصصين في الجريمة

[1] تقرير رئاسة النيابة العامة الرابع لسنة 2020 الباب الثاني: تنفيذ السياسة الجنائية -الجرائم المعلوماتية- ص 332.

[2] هي العملة الرقمية أو النقد الرقمي، إلى المال الذي ينتقل الكترونيا باستخدام أجهزة الكمبيوتر والاتصالات لاسيما الأنترنيت والمثال الذي يساق في هذا المجال هو انتقال الأموال والإيداع وإبقاء قيمة الخدمات.

[3] Glacy+CyberSudGlacy.

المعلوماتية في صفوف القضاة وضباط الشرطة القضائية و إدراج الجرائم المعلوماتية ضمن برامج التكوين الأساسي للملحقين القضائيين وكذلك بالمعهد الملكي للشرطة.

ولضمان تنزيل الاستراتيجية الوطنية للأمن السيبراني، سارعت المملكة المغربية منذ بداية الألفية الثالثة إلى وضع إطار مؤسساتي يشمل مجموعة من الهيئات والمؤسسات الحكومية التي تتمتع بقدر عال من الاستقلالية الوظيفية، وتتنوع مهامها ومجالات عملها بتنوع وتشعب مجالات استعمال نظم المعلومات وتداخلها مع باقي الأنظمة الإدارية والاقتصادية والاجتماعية، وحتى الأمنية والدفاعية.

وقد يعتقد البعض أن الإنترنت وشبكات المعلومات يصعب في إطارها تطبيق القانون لغياب نقاط المراقبة على الشبكات وتقنيات إرسال الرسائل والتحقق من هوية المعتدين وتشفير التوقيعات، وهي خصائص يتميز بها الإنترنت تجعل من الصعب تحديد وملاحقة مرتكب الأفعال المجرمة، مما يعقد عمل الشرطة التي قد تبقى مكتوفة الأيدي[1].

إلا أن ذلك من وجهة نظر متواضعة غير منطقي فهذه الأفعال المجرمة ترتكب في بادئ الأمر داخل حدود الدولة يستطيع المحققون أن يتصرفوا حيالها دون مصاعب أو تعقيدات، كما أن معرفة شخصية الفاعل التي يتستر وراءها المجرم المعلوماتي هو أمر نسبي، إذ يترك آثارا أثناء تنقله في شبكة المعلومات تسمح للمحققين بالوصول إليه، علما أن الطابع الدولي للجريمة لا يمثل عقبة تمنع إجراء التحقيق والملاحقة' وإن كان الطابع اللامادي لشبكة الإنترنت باعتبارها ملتقى لمختلف الأصناف والمتعاملين القادمين من مختلف الأوساط، يقتضي لتفعيل دور مصالح الأمن خلق خلية للرصد والمتابعة 7 أيام /7 و 24 ساعة/24، تكون مهمتها الإبحار عبر الشبكة وبطريقة موجهة وهادفة لمعرفة التطورات التي تشهدها ومتابعة نوع المضامين المتداولة في مختلف مجالات استخدام هذه الشبكة[2]، ويبقى دور الأجهزة الأمنية مهما في ضبط معالم الجريمة المعلوماتية خاصة وأنها تتوفر على عناصر متخصصة في الميدان المعلوماتي فقد ساعدت مصلحة المعلوميات التابعة لقيادة الدرك الملكي بالرباط بتنسيق مع المصالح والمؤسسات المختصة في التعرف على أسماء وعناوين مجموعة من الضحايا تمت قرصنة بطائقهم البنكية، وجميع المعلومات المتعلقة بهذه البطائق المقرصنة وكذا الأشخاص المتورطين في ذلك مع التوصل لكيفية قيامهم بعمليات القرصنة ومعالجتهم للمعلومات المضمنة بالبطائق وتزويرها، كما أن تحليلها للمعطيات المستخرجة من الحاسوب المستعمل من قبل المتورطين مكنها من معرفة بعض أسماء الأبناك التي تم سحب النقود منها ورموز البطائق المقرصنة واكتشاف خزائن مختلفة مسجلة بالحاسوب تحتوي أرقام عدة بطائق بنكية لزبناء تمت قرصنتها تحمل أسماء المتورطين الذين ألقي القبض عليهم[3].

[1] صالح أحمد البربري: "دور الشرطة في مكافحة جرائم الإنترنت في إطار الاتفاقية الأوروبية الموقعة في بودابست في 23/11/2001"، مقال منشور بالدليل الإلكتروني www.arablawinfo.com، تاريخ ولوج الموقع يوم السبت 21 فبراير 2023- على الساعة الثالثة زوالا، صفحات متفرقة: 2-4.

[2] أحمد آيت الطالب: تقنيات البحث وإجراءات المسطرة المتبعة في جرائم الأنترنيت المعلوميات،مجلة الملف، العدد 9 نونبر2006 ص: 25.

[3] قرار عدد 299 صدر بتاريخ 23-03-2006، ملف 336-05-22 صادر عن محكمة الاستئناف بالرباط غير منشور.

وفي هذا الإطار كذلك تمكنت مصلحة الإعلاميات إثر استخدامها للمعلومات الموجودة في القرص الصلب لأحد الحواسيب ودراسة محتوياته من التوصل إلى عدد البطائق المقرصنة من طرف عناصر شبكة متخصصة في القرصنة ومعرفة الأماكن التي تمت بها عمليات هذه القرصنة[1].

من هنا تبدو أهمية الدور المنوط بوحدات الأمن في مواجهة هذه الظاهرة المستحدثة والمعقدة من الإجرام، فوجود شرطة تقنية وعلمية على درجة كبيرة من المعرفة بأنظمة الحاسب الآلي وكيفية تشغيلها وأساليب ارتكاب الجرائم عليها أو بواسطتها، مع القدرة على كشف غموض هذه الجرائم وسرعة التصرف بشأنها من حيث كشفها وضبط الأدوات التي استخدمت في ارتكابها والتحفظ على البيانات والأجهزة المستخدمة في ذلك أو تلك التي تكون محلا للجريمة، يبقى أمرا ضروريا في ضبط الجرائم ذات الصلة بالأنظمة المعلوماتية، والتي تتسم بحداثة أساليب ارتكابها وسرعة تنفيذها وسهولة إخفائها ودقة سرعة محو أثارها، الأمر الذي يقتضي الوقوف على آليات البحث والتحقيق المعتمدة في مواجهة هذه النوعية من الجرائم.

أما بالنسبة للقانون الإماراتي فقد كان أكثر تطورا ووضوحا من نظيره المغربي لاسيما فيما يتعلق بقانون مكافحة الشائعات والجرائم الإلكترونية[2] والذي يهدف بالأساس إلى توفير إطار قانوني شامل لتعزيز حماية المجتمع من الجرائم الالكترونية المرتكبة من خلال شبكات وتقنيات الإنترنيت، كما يسعى إلى حماية المواقع الإلكترونية وقواعد البيانات الحكومية في دولة الإمارات، ومكافحة إنتشار الشائعات والأخبار المزيفة، الاحتيال الالكتروني، والحفاظ على الخصوصية الشخصية

ويتناول القانون السالف الذكر بالإضافة إلى ماذكر أعلاه:

الإعلان أو الترويج المضلل للمستهلك، الترويج لمنتجات طبية دون ترخيص، الابتزاز أو التهديد الالكتروني، وقد تم إطلاق تطبيق رزام للأمن السيبراني وهو ملحق لمتصفح يوفر تقييما مستمرا للمختوى الضار في جنيع صفحات الويب، حيث تروم فكرة التطبيق على إضافة شبكة تعمل على تحديد المواقع الضارة، وعناوين التصفح الغير الآمنة

ومما تجذر الإشارة إليه أنه تتميز إجراءات البحث والتحقيق في جرائم المعلوميات بنوع من الخصوصية وتشمل هذه التقنيات ما يلي:

- **الفقرة الأولى: معاينة مسرح الجريمة المعلوماتية:**

ويقصد بالمعاينة فحص مكان أو أي شيء أو شخص له علاقة بالجريمة وإثبات حالته، ولا تتمتع المعاينة في مجال كشف غموض الجريمة المعلوماتية بنفس الدرجة من الخصوصية التي تكتسيها في مجال الجريمة التقليدية ومرد ذلك لاعتبارين، الأول أن الجرائم التي تقع على نظم المعلومات والشبكات قلما يترتب على ارتكابها آثار مادية، والثاني أن عددا كبيرا من الأشخاص قد يترددون على مكان أو مسرح الجريمة خلال الفترة الزمنية الفاصلة بين ارتكاب الجريمة واكتشافها، مما يهيء الفرصة لحدوث تغيير أو إتلاف أو عبث بالآثار المادية أو زوال بعضها، وهو ما يثير الشك في الدليل المستمد من المعاينة[3].

[1] قرار عدد 37 صدر بتاريخ 16-01-2006،ملف 909-05-22 صادر عن محكمة الاستئناف بالرباط غير منشور.

[2] المرسوم الاتحادي رقم 34 لسنة 2021 في شأن مكافحة الشائعات والجرائم الالكترونية في 2 يناير 2022.

[3] أحمد أيت الطالب، مرجع سابق ص26.

وحتى تصبح معاينة مسرح الجريمة المعلوماتية لها فائدة في كشف الحقيقة عنها وعن مرتكبيها ينبغي مراعاة عدة قواعد وإرشادات أبرزها، تصوير الحاسوب والأجهزة الطرفية المتصلة به والمحتويات والأوضاع العامة بمكانه، مع التركيز خاص على تصوير الأجزاء الخلفية للحاسوب وملحقاته ويراعى تسجيل وقت وتاريخ ومكان التقاط الصورة، كذلك يجب الاهتمام بملاحظة الطريقة التي تم بها إعداد النظام والآثار الإلكترونية وبوجه خاص السجلات الإلكترونية التي تتزود بها شبكات المعلومات لمعرفة موقع الاتصال ونوع الجهاز الذي تم عن طريقه الولوج إلى النظام أو الموقع، مع ملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يمكن إجراء عملية المقارنة والتحليل حين عرض الأمر فيما بعد على القضاء، ويتعين عدم نقل أي مادة معلوماتية من مسرح الجريمة قبل إجراء اختبارات للتأكد من خلو المحيط الخارجي لموقع الحاسوب من أي مجالات لقوى مغناطيسية يمكن أن تتسبب في محو البيانات المسجلة، وأخيرا التحفظ على محتويات سلة المهملات من الأوراق الملقاة أو الممزقة والمستعملة والشرائط والأقراص الممغنطة.

الفقرة الثانية: التفتيش

هو البحث عن شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبيها، وقد يقتضي التفتيش إجراء البحث في محل له حرمة خاصة، وقد أحاط القانون التفتيش بضمانات عديدة ومحل التفتيش قد يكون مسكنا أو شخصا، مع مراعاة الضوابط التي يرسمها قانون المسطرة الجنائية للدخول إلى المنازل لتفتيشها بحثا عن أشياء تؤدي إلى إظهار الحقيقة، يمكن لضابط الشرطة القضائية اعتماد هذا الإجراء لضبط أدلة لها علاقة بجريمة من الجرائم المرتبطة بالمعلومات، وبصرف النظر عن المعيقات التي قد تحول دون بلوغ الأهداف المتوخاة من هذه العملية، فإن القيام بالتفتيش في منزل شخص وفقا للشروط والإجراءات المنصوص عليها في القانون قد يساعد في ضبط الآلة المشبوهة وحجزها تمهيدا لفحصها وإجراء التحليلات التقنية عليها بحثا عما تتضمنه من معطيات أو أدلة رقمية، وأيضا الأدلة التقليدية ذات العلاقة بأنظمة وبرامج وتجهيزات الحاسبات الآلية ومعدات التشغيل والأوراق والمستندات وآلات الطباعة إلى غير ذلك[1].

غير أن عملية البحث في أطراف الحاسبات أو وحدات التشغيل أو ملحقاتها، قد تدفع الباحث الجنائي إلى توسيع دائرة التحريات إلى حاسب آلي أو مركزي موجود في محل آخر يشغله المشتبه فيه أو شخص آخر، كما قد يجد نفسه مضطرا للدخول إلى معطيات آلية أو قواعد بيانات أو مواقع محمية ومؤمنة، وهو ما يثير إشكالا بخصوص إمكانية الولوج إليها بناء على الإذن المحصل عليه أصلا عند الدخول إلى المنزل الذي قام فيه بتحرياته الأولى، أم أن هذا الإذن لا يجزا للقيام بعمليات تحري في وسط معلوماتي، باعتبار أن الأنظمة المعلوماتية المحمية لا تعتبر منازل في مفهوم القانون، وإذا كان الأمر كذلك فما هي المبررات القانونية الوجيهة التي يمكن اعتمادها لاقتحام أنظمة المعلومات المحمية وإجراء الأبحاث أو التحريات فيها بدون علم المكلفين بها أو أصحابها الشرعيين؟

[1] أحمد آيت الطالب: مرجع سابق، ص: 29-30.

وفي غياب إطار قانوني خاص يسمح بالولوج إلى هذه الأنظمة، يمكن القول أن قانون المسطرة الجنائية المغربي رغم حداثته، لا يتضمن استجابة صريحة لمتطلبات البحث وتفتيش قواعد المعطيات الآلية باستعمال الشبكة[1].

- **الفقرة الثالثة: الشهادة في الجريمة المعلوماتية:**

الشهادة هي الأقوال التي يدلي بها غير الخصوم أمام سلطة التحقيق بشأن جريمة وقعت، سواء كانت تتعلق بثبوت الجريمة وظروف ارتكابها وإسنادها إلى متهم أو براءته منها، والشاهد في الجريمة المعلوماتية هو الفني صاحب الخبرة والتخصص في تقنية وعلوم الحاسب الآلي، والذي لديه معلومات جوهرية أو هامة لازمة للولوج في نظام المعالجة الآلية للبيانات إذا كانت مصلحة التحقيق تقتضي التنقيب عن أدلة الجريمة داخله، ويطلق على هذا النوع من الشهود مصطلح الشاهد المعلوماتي تمييزا له عن الشاهد التقليدي، ويشمل الشاهد المعلوماتي عدة طوائف من أهمها القائم على تشغيل الحاسب الآلي، وهو المسؤول عن تشغيله والمعدات المتصلة به ويجب أن تكون لديه خبرة كبيرة في هذا المجال، ثم المبرمجون وهم الأشخاص المتخصصون في كتابة البرامج، ويمكن تقسيمهم إلى فئتين: الأولى تشمل مخططي برامج التطبيقات والثانية مخططي برامج النظم[2].

المنزل الذي قام فيه بتحرياته الأولى، أم أن هذا الإذن لا يجزا للقيام بعمليات تحري هناك أيضا المحللون، يتجلى دورهم في تجميع بيانات نظام معين ودراسته ثم تحليله أي تقسيمه إلى وحدات منفصلة، ثم مهندسوا الصيانة والاتصالات، هم المسؤولين عن أعمال الصيانة الخاصة بتقنيات الحاسوب بمكوناته وشبكات الاتصال المتعلقة به، بالإضافة إلى مديري النظم الذين يوكل لهم أعمال الرقمنة في النظم المعلوماتية.

ويتعين على الشاهد المعلوماتي أن يقدم لسلطات التحقيق ما يحوزه من معلومات جوهرية لازمة للولوج في نظام المعالجة الآلية للبيانات للكشف عن أدلة الجريمة.

عموما هناك صعوبات مختلفة تعترض سلطات البحث والتحقيق في ضبط الجريمة المعلوماتية وهو ما يقتضي من المشرع مراجعة قانون المسطرة الجنائية ليتلاءم مع خصوصية هذه الجريمة، الأمر الذي تنبهت له الكثير من التشريعات الأجنبية التي قررت بعد سنها للقوانين المتعلقة بنظم المعالجة الآلية للمعطيات تنظيم مسطرة خاصة للبحث، على غرار مسطرة التقاط المكالمات الهاتفية أو وسائل الاتصال الإلكترونية عن بعد، وخولت للسلطة القضائية – قاضي التحقيق- صلاحية مراقبة هذه العمليات، الذي يؤهل وحده من حيث المبدأ بالترخيص بإجرائها في 185 الحالات وضمن الشروط المنصوص عليها في القانون.

المبحث الثاني:تجليات نظام الحماية الاجتماعية في ضوء الأجهزة المنصوص عليها في القانون 05.20

إن المشرع المغربي تطرق في المادة الأولى من القانون 05.20 المتعلق بالأمن السيبراني إلى مجالات تطبيق هذا القانون من خلال تحديده لكل هذه المجالات على سبيل الحصر والتي يروم المشرع من خلالها توفير الثقة والحماية داخل الفضاء السيبراني عملا منه تنزيل استراتيجية المغرب الرقمي التي ستجعل المغرب في طليعة البلدان الصاعدة والتي تستدعي رقمنة الخدمات وتحقيق النجاعة

[1] أحمد أيت الطالب مرجع السابق، ص 30.

[2] صالح أحمد البربري مرجع سابق ص6.

والفعالية، وقد اعتمد هذا القانون على سياسة أمنية تروم مكافحة الهجمات والتعديلات التي من الممكن أن يتعرض لها الفضاء السيبراني من خلال التصدي لها موضوعيا وتقنيا من أجل تحقيق الحكامة والأمن للفضاء السيبراني لنظام الحماية الاجتماعية.

المطلب الأول: المقتضيات العامة الموضوعية الواردة في القانون 05.20

إن من بين الأهداف التي سعى المشرع المغربي تحقيقها في إطار هذا القانون هي توفير – الحماية داخل الفضاء السيبراني لنظام الحماية الاجتماعية من خلال سن مجموعة من الاحكام التي تصون حرمة من الفضاء وتعاقب كل من سولت له نفسه الدخول إلى النظم المعلوماتية قصد إحداث خلل فيها[1]، وضرورة إجراء افتحاص للنظم المعلوماتية الحساسة الذي تقوم به السلطة الوطنية أو متعهدي الافتحاص[2]، ولكن ورغم نجاعة هذا الأسلوب في مراقبة المعلومات والبيانات إلا يه يطرح العديد من الإشكالات والتي من ضمنها مثلا في حالة عدم التزام متعهد الافتحاص بقواعد السر المهني المنصوص عليها في المواد 21 و 22 من هذا القانون وترتب عن ذلك المساس على هذه البنيات التحتية ذات الأهمية الحيوية، خصوصا وأن المشرع لم يحدد في هذا الإطار جزاء الاخلال بقواعد السر المهني.

ونرى أنه كان على المشرع أن يدرج جزاء الاخلال بقواعد السر المهني في هذا القانون ان الأمر يتعلق ببنيات ذات أهمية حيوية وتحتوي على معلومات هامة، قد تكون للمساس سريتها آثار وخيمة على مستوى الأمن الداخلي والخارجي للبلد، إلا أنه وأمام غياب مقتضيات زجرية متعلقة بإفشاء السر المهني أثناء القيام بعملية الافتحاص، ليس هناك ما يمنع من تطبيق المقتضيات المنصوص عليها في مجموعة القانون الجنائي بخصوص هذا الإجراء، والتي أشارت إلى جزاء الاخلال بالسر المهني، فباعتبار القائم بالافتحاص من الأمناء على الأسرار فليس هناك ما يمنع من تطبيق هذا النص العام مادام أن النص الخاص لم يتطرق لهذه المسألة[3].

---

[1] وهذا ما أشار إليه المشرع من خلال المادة التاسعة من القانون 05.20 والتي نصت على " تعد كل هيئة مخطط لضمان استمرارية أو استئناف الأنشطة يتضمن مجموع الحلول البديلة لإبطال مفعول انقطاعات الأنشطة وحماية الوظائف المهمة والحساسة من الآثار الناجمة عن الاختلالات الأساسية لنظم المعلومات أو عن الكوارث، وضمان استئناف عمل هذه الوظائف في أقرب الآجال".

وأكدت الفقرة الأخيرة من هذه المادة على أنه يتعين اختبار مخطط ضمان استمرارية أو استئناف الأنشطة بصفة منتظمة من أجل تحيينه حسب التطورات الخاصة بالهيئة وتطور التهديدات.

[2] أكدت على هذا الاجراء المادة 20 من القانون 05.20 والتي تنص على « يجب على المسؤولين عن البنيات التحتية ذات الأهمية الحيوية من السلطة الوطنية أو متعهد الافتحاص المؤهل بالمعلومات والعناصر اللازمة لإجراء الافتحاص بما في ذلك الوثائق المتعلقة بسياستها الأمنية، وعند الاقتضاء نتائج الافتحاص الأمني السابقة والسماح لهم بالولوج إلى الشبكات ونظم المعلومات موضوع المراقبة قصد إجراء التحليلات واستخراج بيانات المعلومات التقنية »، وأكنت الفقرة الأخيرة من هذه المادة على ضرورة التزام متعهدو الافتحاص المؤهلون ومستخدموهم تحت طائلة العقوبات المقررة باحترام السر المهني بخصوص القيام بعملية الافتحاص.

[3] ينص الفصل 446 من مجموعة القانون الجنائي على ما يلي: « الأطباء والجراحون وملاحظو الصحة، وكذلك الصيادلة والمولدات وكل شخص يعتبر من الأمناء على الأسرار، بحكم مهنته أو وظيفته الدائمة أو المؤقتة إذا أفشى سرا أودع لديه، وذلك في غير الأحوال التي يجيز له القانون فيها ذلك أو يوجب عليه التبليغ عنه، يعاقب بالحبس من شهر إلى ستة أشهر وغرامة من ألف مائتين إلى عشرين ألف درهم ».

ولغاية تحقيق الأمن للفضاء السيبراني حث المشرع في إطار القانون 05.20 على ضرورة التعاون من أجل تجنب المخاطر السيبرانية وذلك في فصل خاص عنونه ب"التكوين والتحسيس والتعاون" وأفرد له المواد من 43 إلى المادة 47، هذا التعاون الذي يجب أن يكون على المستوى الوطني ثم على المستوى الدولي[1].

وهذا إن دل عن شيء فإنما يدل عن حرص المشرع المغربي على تنزيل أحكام الاتفاقيات الدولية التي صادق عليها، ويظهر ذلك جليا من خلال أحكام هذه الاتفاقيات، فنجد مثلا اتفاقية بودابست لمكافحة جرائم الحاسوب والانترنت تناولت هذا الأمر من خلال تنصيصها على هذا التعاون، وأفردت له حيزا هاما وخصصت له فصلا مستقلا بما يعادل تسعة مواد من المادة 23 إلى المادة 31 من هذه الاتفاقية، ونفس الشيء نجده في إطار الاتفاقية العربية لمكافحة جرائم تقنية المعلومات التي تضمنت جل أحكامها ما يفيد هذا التعاون، وبالخصوص المواد من 34 إلى المادة 43 من هذه الاتفاقية.

وهذا ما ذهب إليه أيضا بعض الفقه من خلال الدعوة إلى ضرورة التعاون وبدل الجهود من أجل إقرار وتنزيل سياسات واستراتيجيات تروم توفير الحماية داخل الفضاء السيبراني بشكل يضمن أمن المجتمع والدولة ثم وضع الأطر التنظيمية والتشريعية التي تضمن عدم الاعتداء على الحريات والحقوق[2].

ولتوفير الحماية أكثر اعتمد المشرع في إطار القانون 05.20 مقاربة زجرية من خلال تخصيص جانب مهم من هذا القانون للمخالفات والعقوبات، حيث خصص فصلا مستقلا لهذا الأمر بما يعادل 5 مواد من المادة 48 إلى المادة 52، ما يؤكد الطبيعة الردعية لهذا القانون، وتتجلى هذه الطبيعة من خلال مجموعة من العقوبات المقررة في هذا القانون والتي تتراوح ما بين 200.000 درهم إلى 400.000 درهم حسب الحالات الواردة في المادة 49 من القانون 05.20. ثم من 100.000 إلى 200.000 درهم في الحالات المنصوص عليها في المادة 50 من نفس القانون، ثم عقوبة المصادرة المنصوص عليها في المادة 51، وعاد المشرع في إطار المادة 52 ليتشدد ويقرر رفع العقوبة إلى الضعف وذلك في حالة العود.

إلا أن ما يعاب على المشرع في إطار قانون الأمن السيبراني هو انعدام العقوبات السجنية فيه، بحيث اقتصر على تضمينه الغرامات فقط، وهذا ما يطرح إشكالات عديدة في إطار هذا القانون و من فلسفة صدوره، إذ كيف يمكن تصور تطبيق غرامات مالية فقط على أفعال خطيرة تمس البنيات التحتية للدولة وتهدد أمنها الداخلي والخارجي.

---

[1] أكد المشرع على ضرورة التعاون من أجل توفير الحماية للفضاء السيبراني من خلال مقتضيات المواد من 43 إلى 47 من القانون 05.20، فيما يخص التعاون على الصعيد الوطني أشارت المادة 43 إلى أن السلطة الوطنية تقوم بتعاون مع المهنيين والفاعلين في مجال الأمن السيبراني بتنظيم دورات تكوينية وتمارين لفائدة مستخدمي الهيئات والبنيات التحتية ذات الأهمية الحيوية من أجل تطوير وتعزيز القدرات الوطنية في هذا المجال، أما فيما يخص التعاون الدولي فقد نصت عليه المواد من 46 إلى 47، حيث أن المادة 46 نصت على أنه تقوم السلطة الوطنية بالتشاور مع الإدارات المعنية بتطوير علاقات التعاون مع المنظمات الوطنية والأجنبية في مجال الأمن السيبراني وتنسيقها ونفس الأمر أكدت عليه المادة 47 من خلال إبرازها لوظائف السلطة الوطنية والتي تتجلى في ربط علاقات التعاون على الصعيدين الوطني والدولي لمعالجة حوادث الأمن السيبراني وتطوير تبادل التجارب والخبرات في هذا المجال.

[2] منى الأشقر "جبور السيبرانية هاجس العصر"، جامعة الدول العربية قطاع الأعمال والاتصال، المركز العربي للبحوث القانونية والقضائية، العدد 1، بدون ذكر مكان وسنة الطبعة، الصفحة: 76.

أشار المشرع المغربي من خلال المادة الأولى من القانون 05.20 إلى نطاق تطبيق هذا القانون على المستوى المؤسساتي، خصوصا في الفقرة الرابعة وما يليها من المادة السالفة الذكر[1] هذا الإطار الوطني الذي يسعى إلى تحقيق الحكامة داخل الفضاء السيبراني من خلال تنفيذ السياسة التي اعتمدها المشرع والهادفة إلى تحقيق الأمن والحماية للنظم المعلوماتية بما يعزز الثقة الرقمية في البلاد، ولقد عدد المشرع هذه المؤسسات وحدد اختصاصاتها في إطار الفصلين الثالث والرابع من هذا القانون، والتي تتمثل في السلطة الوطنية للأمن السيبراني (أولا)، ثم اللجنة الاستراتيجية للأمن السيبراني وكذا لجنة إدارة الأزمات والأحداث السيبرانية (ثانيا).

الفقرة الأولى: السلطة الوطنية للأمن السيبراني

لقد نظم المشرع المغربي هذه السلطة وخصص لها حيزا هاما من خلال القانون 05.20 وأوكل إليها مجموعة من المهام باعتبارها الساهرة على تطبيق أحكام هذا القانون، إلا أن الإشكال المطروح هنا هو أن المشرع لم يبين المقصود بهذه السلطة وإنما اكتفى بتحديد اختصاصاتها الشيء الذي أثار نقاشا كبيرا خصوصا وأن المشرع استعمل نفس المصطلح في ظل القانون 53.05 المتعلق بالتبادل الالكتروني للمعطيات القانونية، وبالتالي فهل السلطة الوطنية في إطار القانون 53.05 هي نفسها التي نظمها القانون 05.20.

بالرجوع إلى المرسوم المتعلق بتطبيق القانون 05.20 والسالف ذكره نجده حدد المقصود بالسلطة الوطنية[2]، فهذا المرسوم أزال بعض اللبس الذي يكتنف مواد القانون 05.20 بخصوص تحديد المقصود بالسلطة الوطنية في ظل هذه المواد وتحديدها في المديرية العامة لأمن نظم المعلومات.

والحديث عن السلطة الوطنية في إطار القانون 05.20 يستدعي دراستها على مستوى مجموعة من الصلاحيات المنوطة بها (أ)، وكذلك مجموعة من المساطر والإجراءات التي رسمها لها هذا القانون(ب).

الفقرة الثانية: صلاحيات السلطة الوطنية.

تقوم السلطة الوطنية للأمن السيبراني بمجموعة من المهام والتي رسمها لها القانون المتعلق بالأمن السيبراني وذلك من خلال المادة 38 والتي تتجلى في:

توليها خدمات التنسيق للأعمال المتعلقة بإعداد وتنفيذ استراتيجية الدولة في مجال الأمن السيبراني وكذا السهر على ضمان تطبيق توجيهات اللجنة الاستراتيجية للأمن السيبراني[3]، إضافة إلى توليها عملية تحديد تدابير حماية النظم المعلوماتية والسهر على ضمان تطبيقها، بالإضافة إلى تقديم الاقتراحات إلى اللجنة الاستراتيجية للأمن السيبراني بخصوص التصدي للأزمات التي من الممكن أن

[1] نص المشرع المغربي من خلال مقتضيات المادة الأولى على يحدد هذا القانون:
–الإطار الوطني لحكامة الأمن السيبراني »، والمقصود بهذا الاطار هو المؤسسات الساهرة على تطبيق أحكام هذا القانون، وقد حددها هذا القانون في الفصل الثالث من هذا القانون المعنون بـ"حكامة الأمن السيبراني"، والمتمثلة في اللجنة الاستراتيجية للأمن السيبراني ثم السلطة الوطنية للأمن السيبراني، ثم لجنة إدارة الأزمات والأحداث السيبرانية.

[2] نصت المادة الأولى من المرسوم 2.21.406 على « يقصد بالسلطة الوطنية للأمن السيبراني المشار إليها في القانون 05.20 اعلاه المديرية العامة لأمن نظم المعلومات التابعة لإدارة الدفاع الوطني ويشار إليها بعده بالسلطة الوطنية ».

[3] الفقرة الأولى من المادة 38.

تلحق بأمن النظم المعلوماتية[1]، والحرص على تأهيل مقدمي خدمات افتحاص نظم المعلومات الحساسة للبنيات التحتية ذات الأهمية الحيوية[2]، والقيام بأعمال المراقبة والسهر على ضمان افتحاص أمن نظم المعلومات والبنيات التحتية[3] والقيام بأنشطة البحث العلمي والتقني في مجال الأمن السيبراني وتشجيعها...[4]، وعلى العموم فأعمال السلطة الوطنية تشمل كل ما يتعلق بتحقيق الأمن داخل القضاء السيبراني مع حرصها الدائم للحفاظ على سرية المعلومات الحساسة التي تتوصل إليها تنفيذا لمهامها.

الفقرة الثالثة: المساطر والإجراءات

لقد أفرد المشرع في إطار القانون 05.20 للسلطة الوطنية مجموعة من القواعد الإجرائية التي يستلزم اتباعها خلال القيام بالتصدي للأفعال المخلة بالفضاء السيبراني، حيث ألزمها في مستهل هذه الإجراءات على الإلتزام بالسرية أثناء القيام بأدوارها التي أقرها لها القانون[5].

كما ألزم المشرع أعوان السلطة الوطنية وكلما تعلق الأمر بالتصدي لأي هجوم إلكتروني يستهدف المساس بالنظم المعلوماتية والوظائف الحيوية للمجتمع أو الصحة أو السلامة أو الأمن...بالقيام بالتحريات التقنية اللازمة لتحديد خصائص الهجوم والسهر على ضمان تنفيذ التدابير والتوصيات المتعلقة بها[6].

ومن جانب آخر فقد أناط المشرع بهذه المؤسسة أعمال التعاون مع المصالح المختصة عن طريق تبادل المعطيات والمعلومات المساعدة على كشف الجرائم التي تستهدف نظم المعالجة الآلية للمعطيات[7].

كما تقوم السلطة الوطنية كلما تبين لها إبان القيام بمهامها وجود أفعال يشتبه في مخالفتها للقانون إحالة الأمر على السلطات المختصة، هذه الأخيرة التي يتعين عليها إخبار السلطة الوطنية بالمآل المخصص للإحالة[8].

إن المهام التي أناطها المشرع بالسلطة الوطنية (المديرية العامة لأمن نظم المعلومات) تبين المجهودات التي تقوم بها هذه السلطة في مجال تحقيق الأمن السيبراني، ومن أجل تحقيق الغاية التي من أجلها السلطة الوطنية يستلزم الأمر منح هذه السلطة مجموعة من الإمتيازات التي قد تساعدها في القيام بأعمالها من قبيل توفير الوسائل التقنية والمادية و موارد بشرية مؤهلة في فك معالم الجريمة السيبرانية التي تعد من الجرائم الخطيرة مع منح هذا الجهاز التقنيات الخاصة التي ستساعده في عمليات الضبط والتحري والتحقيق...

---

[1] الفقرة الثانية والثالثة من المادة 38.

[2] الفقرة الرابعة من المادة 38.

[3] الفقرتين السادسة والسابعة من المادة 38.

[4] الفترة الأخيرة من المادة 38 من القانون 05.20.

[5] نصت المادة 39 من القانون 05.20 على "يتعين على السلطة الوطنية ضمان سرية المعلومات الحساسة التي تجمعها في إطار هذا القانون ".

[6] المادة 41 من القانون 05.20.

[7] الفقرة الأولى من المادة 42 من القانون 05.20.

[8] الفقرتين الأخيرتين من المادة 42 من نفس القانون.

المطلب الثاني: اللجنة الاستراتيجية للأمن السيبراني ولجنة إدارة الأزمات.

إن الوصول إلى مستوى الدول المتقدمة والرائدة في مجال الأمن السيبراني يتطلب وجود أجهزة وفاعلين أساسيين في هذا المجال وكذا توفير الإمكانات اللازمة التي ستساعدهم في تحقيق هذه الغاية، وتعتبر اللجنة الاستراتيجية للأمن السيبراني ولجنة إدارة الأزمات والأحداث السيبرانية من الأجهزة التي لا تقل أهمية عما أشرنا إليه في معرض الحديث عن السلطة الوطنية، هذه اللجان التي تلعب أدوارا مهمة في مجال تحقيق الأمن السيبراني ومكافحة الجريمة السيبرانية، وأسند لها القانون بدورها مجموعة من المهام وذلك من خلال المواد من 35 إلى 37 من القانون 05.20، وهي مهام كلها تروم جودة خدمات الأمن السيبراني وتحقيق الثقة الرقمية.

الفقرة الأولى: اللجنة الاستراتيجية للأمن السيبراني

بخصوص اللجنة الاستراتيجية للأمن السيبراني فهي تلعب دورا هاما في هذا المجال، من خلال أنها هي من تقوم على إعداد التوجهات الاستراتيجية للدولة في مجال الأمن السيبراني والسهر على ضمان الحماية للنظم المعلوماتية ووقايتها من المخاطر، وقد حددت المادة 35 من القانون 05.20. مهامها والتي تروم في مجملها تجويد الأمن داخل الفضاء السيبراني[1].

وعموما يمكن القول بأن أدوار اللجنة الاستراتيجية هي في مجملها أدوار تقييمية لأعمال اللجان الأخرى، ويساعدها في مهامها لجانا تحدثها لديها[2].

وبالإضافة إلى اللجان التي تحدثنا عنها سابقا توجد لجنة أخرى لها أدوار مهمة في إطار تحقيق السيبراني والتي تنعت بلجنة إدارة الأزمات والأحداث السيبرانية الجسيمة، والتي حدد لها القانون 05.20 مجال اختصاصها في التصدي لحوادث الأمن السيبراني الجسيمة[3].

وفي إطار الحديث عن هذه اللجان ودورها في تحقيق الأمن السيبراني وحماية أمن المعلومات، ارتأينا التذكير بجهاز أساسي خارج عن نطاق القانون 05.20 والذي يلعب دورا هاما في هذا الإطار ويتعلق الأمر باللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي، المحدثة بموجب القانون 2009 المتعلق بحماية الأشخاص الذاتيين تجاه المعطيات ذات الطابع الشخصي[4]، هذه اللجنة

---

[1] تنص المادة 35 من القانون 05.20 على تحدث لجنة استراتيجية للأمن السيبراني يعهد إليها بالقيام بما يلي:

*إعداد التوجهات الاستراتيجية للدولة في مجال الأمن السيبراني والسهر على ضمان صمود نظم معلومات الهيئات والبنيات التحتية ذات الأهمية الحيوية والمتعهدين المشار إليهم في الفرع الثالث من الفصل الثاني من هذا القانون.

*التقييم السنوي لأنشطة السلطة الوطنية.

*تقييم عمل اللجنة الوطنية لإدارة الأزمات والأحداث السيبرانية الجسيمة، المنصوص عليها في المادة 36 بعده.

*حصر نطاق افتحاصات أمن نظم المعلومات التي تنجزها السلطة الوطنية.

*تشجيع البحث والتطوير في مجال الأمن السيبراني.

*تشجيع برامج وأنشطة التحسيس وتعزيز القدرات في مجال الأمن السيبراني لفائدة الهيئات والبنيات التحتية ذات الأهمية الحيوية.

إبداء الرأي في مشاريع القوانين والنصوص التنظيمية المتعلقة بمجال الأمن السيبراني.

[2] الفقرة الأخيرة من المادة 5 من لمرسوم التطبيقي للقانون 05.20 المتعلق بالأمن السيبراني.

[3] عرف المشرع حادث الأمن السيبراني في المادة الثانية ضمن الفقرة 17 بكونه واقعة أو وقائع غير مرغوب فيها أو غير متوقعة مرتبطة بأمن نظم المعلومات والتي يحتمل يحتمل جدا أن تعرض للخطر أنشطة هيئة ما أو بنية ذات أهمية حيوية أو متعهد أو أن تهدد سلامة نظمهم المعلوماتية.

[4] وقد حدد المرسوم 15-09-2 الصادر بتاريخ 21 ماي 2009، بتطبيق القانون 09- 08أعضاء هذه اللجنة وطريق تعيينها وطريقة عملها.

اللجنة التي تسهر على تطبيق أحكام القانون السالف الذكر والسهر على التقيد به تفعيلا لمقتضيات المادة 27 من هذا القانون من خلال الحرص على تقديم أراءها والإدلاء بها أمام الحكومة أو البرلمان أو أمام الحكومة لوحدها أو أمام السلطة المختصة حسب الحالات المحددة في المادة 27 أعلاه[1]، ثم تلقي التبليغ عن هوية الممثل المستقر في المغرب الذي يحل محل المسؤول عن المعالجة القاطن بالخارج وكذا تلقي التصاريح المنصوص عليها في المادتين 12 و 13 من نفس القانون، ثم هوية المسؤول عن معالجة السجلات الممسوكة لغرض فتحها للعموم[2].

ومن الناحية الزجرية نجد أن هذا القانون ومن خلال بابه السابع خصص حيزا هاما بما يعزز الحماية الجنائية للمعطيات الفردية ذات الطابع الشخصي، فعلى سبيل المثال لا الحصر نجد أن المادة 53 التي عاقب فيها المشرع بغرامة بين 20000 درهم و 200000 درهم كل مسؤول عن المعالجة رفض إعطاء حقوق الولوج أو التصريح أو التعرض المنصوص عليها في المواد 7 و 8 و9 من ذات القانون كما نجد المادة 56 عاقبت بالحبس من 3 أشهر إلى سنة وبغرامة من 20.000 درهم إلى 200.000 درهم أو بإحدى هاتين العقوبتين فقط كل من قام بمعالجة معطيات ذات طابع شخصي خرقا لأحكام المادة الرابعة من نفس القانون، كما جرمت المادة 60 عملية نقل معطيات ذات طابع شخصي نحو دولة أجنبية خرقا لأحكام المادتين 43 و 44 من هذا القانون، حيث عاقب المشرع في هذه الحالة الأخيرة بالحبس من 3 أشهر إلى سنة وبغرامة مالية من 2000 إلى 200000 درهم أو بإحدى هاتين العقوبتين فقط، كما حدد القانون السالف الذكر ظروف التشديد الخاصة بالأفعال الإجرامية التي نص عليها[3]، وبالنسبة لمعاينة مخالفات هذا القانون فإنه بالإضافة إلى ضباط الشرطة القضائية يجوز لأعوان اللجنة الوطنية المؤهلين لهذا الغرض المؤهلين من قبل الرئيس والمحلفين طبقا للأشكال المحددة في القانون العادي القيام بأعمال البحث والمعاينة لمخالفات أحكام هذا القانون والنصوص المتخذة لتطبيقه بواسطة محاضر وتوجه محاضرهم خلال خمسة أيام التي تلي عمليات البحث والمعاينة إلى وكيل الملك.

---

[1] تنص المادة 27.... تكلف اللجنة الوطنية بالإدلاء برأيها:

1-أمام الحكومة أو البرلمان بشأن مشاريع أو مقترحات القوانين أو مشاريع النصوص التنظيمية ذات الصلة بمعالجة المعطيات ذات الطابع الشخصي التي تعرض عليها.

2-أمام السلطة المختصة بشأن مشاريع النصوص التنظيمية الصادرة بإحداث ملفات متعلقة بالمعطيات ذات الطابع الشخصي المجموعة والمعالجة من أجل الوقاية من الجرائم والجنح وزجرها.

3-أمام السلطة المختصة بشأن مشاريع أو مقترحات القوانين بإحداث ومعالجة المعطيات المرتبطة بالتحقيقات والمعطيات الإحصائية التي تم تجميعها ومعالجتها من قبل السلطات المختصة.

[2] الفقرة ب من المادة 27 من القانون 09-08.

[3] نصت المادة 64 على تضاعف عقوبات الغرامة إذا كان مرتكب إحدى المخالفات المنصوص على عقوبتها في هذا الباب شخصا معنويا دون المساس بالعقوبات التي قد تطبق على المسيرين الذين يرتكبون إحدى المخالفات المنصوص عليها أعلاه، "وكما نصت المادة 65" في حالة العود، تضاعف العقوبات المنصوص عليها في هذا الباب".

الفقرة الثانية: اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي.

إيمانا من المشرع المغربي بأهمية الحياة الخاصة للأفراد، وسعيا منه لمواكبة التشريعات المقارنة سعى إلى إصدار القانون رقم 08-2009 الصادر في 18 فبراير 2009 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي والمعطى الشخص هو ذلك العنصر الذي يساهم في التعريف بشخص ما كيف ما كان حامل هذا العنصر؛ ورقي الكتروني...

وقد أقر القانون 08-09-20 جملة من المقتضيات القانونية الهادفة إلى حماية الهوية والحقوق والحريات الفردية والجماعية والحياة الخاصة من كل ما من شأنه أن يمس بها عبر استخدام المعلوميات، وقد بات المغرب، باعتماد هذا القانون واحدا من أول الدول العربية والإفريقية التي تتوفر على نظام كامل للحماية وإحدى الوجهات الآمنة في مجال تداول المعطيات الشخصية.

ويحدد هذا القانون الحق في الولوج إلى القواعد التي تتضمن المعطيات الشخصية، والتعرض على بعض عمليات المعالجة، وطلب تصحيح المعطيات الخاطئة أو مسح المعطيات التي انتهت صلاحيتها أو التي تم تحقيق الغاية من معالجتها.

وقد أحدث هذا القانون لجنة وطنية للسهر على تنزيل قواعده وتنفيذ مقتضياته، ومراقبة التعامل مع أحكامه، وهي **اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي**.

وتتمثل مهمة هذه اللجنة في السهر على تحقيق هدفين[1]؛ **أولهما** حماية الحياة الخاصة للأفراد وحرياتهم الشخصية إزاء الاستعمال المفرط واللامسؤول لمعطياتهم الشخصية خاصة وأن دستور 2011 يؤكد على هذا المقتضى حيث نصت الفقرة الأولى من الفصل 24 من الدستور «**لكل شخص الحق في حماية حياته الخاصة**»، إلى جانب التطور التكنولوجي الكبير الذي يعرفه استعمال هذه المعطيات والتي تعتبر، حسب الجريدة الأمريكية "نيويورك تايمز" بمثابة كنز يمكن تشبيهه بالبترول، حيث مكن بعض الشركات العملاقة "كغوغل".

تتوفر اللجنة الوطنية على: سلط التحري والبحث التي تمكن أعوانها المفوضين لهذا الغرض بصفة قانونية من قبل الرئيس بالولوج إلى المعطيات الخاضعة للمعالجة والمطالبة بالولوج المباشر للمحال التي تتم فيها المعالجة وتجميع جميع المعلومات والوثائق الضرورية للقيام بمهام المراقبة والمطالبة بها، وفق التفويض الذي يمارسونه سلطة الأمر بتزويدها بالوثائق، أيا كانت طبيعتها وكيفما كانت دعاماتها التي تمكنها من دراسة وقائع الشكايات المحالة عليها، وذلك داخل الآجال ووفق الكيفيات أو العقوبات المحتملة التي تحددها سلطة الأمر بالتغييرات اللازمة من أجل حفظ نزيه للمعطيات المحتواة في الملف، أو إجرائها أو العمل على إجرائها سلطة الأمر بإغلاق معطيات أو مسحها أو إتلافها وكذا منع معالجة معطيات ذات طابع شخصي بصفة مؤقتة أو دائمة بما في ذلك المعطيات المتضمنة في شبكات مفتوحة لإرسال المعطيات انطلاقا من خادمات تقع داخل التراب الوطني[2].

[1] سعيد إهراي، ضمانات حماية المعطيات الشخصية مقال منشور على الموقع الالكتروني https://www.hespress.com، تاريخ 13 فبراير 2023.

[2] انظر المادة 30 من القانون قانون رقم 09.08 يتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي.

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 لنظام الحماية الاجتماعية، 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، 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 والحماية الاجتماعية 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، وعدم 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 المتعلقة بالحماية الاجتماعية نظرا لما تخلقه الوسائل التقليدية من إشكالات أمام ضعف نجاعتها في الكشف عن

الجريمة المتعلقة بالأنظمة المتعلقة بالحماية الاجتماعية، وبالتالي الارتقاء بقدرات المحققين، وكذا استغلال الأدلة الرقمية بالوسائل الإجرائية الحديثة في اثبات الجريمة.

- خلق مراكز جديدة وبآليات مستجدة لمواكبة الفضاء السيبراني والمعاملات الرقمية لأنظمة الحماية الاجتماعية ومراقبة التدخل الغير المصرح به.
- منع إختراع 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 ومؤسسات الحماية الاجتماعية.
- 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 الصحية 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؟
- ضرورة خلق خلية خاصة بالمحاكم تهتم بالجرائم المعلوماتية والتهديدات السيبرانية من أجل تخفيف العبء على المنظومة القضائية وتسريع وسائل التدخل الإستباقي.
- 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.
- 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.