

حماية المعطيات الشخصية بالمغرب في ظل تصاعد التهديدات السيبرانية: مقاربة قانونية تقنية لتحقيق التوازن بين الأمن والخصوصية

الباحثة : حسناء الشقوري

باحثة بسلك الدكتوراه كلية العلوم القانونية بطنجة - جامعة عبد المالك السعدي

ملخص:

أصبحت حماية الخصوصية الرقمية من أهم القضايا التي تفرضها التحولات التكنولوجية المتسارعة وتنامي الهجمات السيبرانية التي تستهدف المعطيات ذات الطابع الشخصي. وقد تناول هذا الموضوع الإطار القانوني والمؤسساتي لحماية المعطيات الشخصية، من خلال إبراز المقتضيات القانونية المؤطرة لهذا الحق، خاصة القانون رقم 09.08 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، إلى جانب القانون رقم 05.20 المتعلق بالأمن السيبراني، مع الوقوف على دور المؤسسات المختصة، وفي مقدمتها اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي. كما تم التطرق إلى التحديات التي تعيق تحقيق حماية فعالة للمعطيات الشخصية، سواء المرتبطة بالتطور السريع للتكنولوجيا، أو تنامي الجرائم والهجمات السيبرانية، أو محدودية الوعي الرقمي وصعوبات التنزيل العملي للنصوص القانونية. وفي المقابل، تمت مناقشة سبل تعزيز الحماية، من خلال تطوير الترسنة القانونية، وتعزيز الأمن السيبراني، والاعتماد على التقنيات الحديثة كالشفير والتوقيع الإلكتروني والذكاء الاصطناعي، إضافة إلى نشر الثقافة الرقمية وتعزيز التعاون المؤسساتي والدولي. الكلمات المفتاحية: المعطيات الشخصية؛ الخصوصية الرقمية؛ الأمن السيبراني؛ القانون رقم 09.08؛ اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي.

Protection of Personal Data in Morocco Amid Rising Cyber Threats: A Legal and Technical Approach to
Achieving a Balance Between Security and Privacy

Hassnae Chakkouri

PhD Researcher at the Faculty of Legal Sciences in Tangier, Abdelmalek Essaâdi University.

Abstract

Digital privacy protection has become one of the most significant issues arising from rapid technological developments and the increasing growth of cyberattacks targeting personal data. This study addressed the legal and institutional framework for the protection of personal data by highlighting the legal provisions governing this right, particularly Law No. 09.08 relating to the protection of individuals with regard to the processing of personal data, as well as Law No. 05.20 on cybersecurity. It also examined the role of competent institutions, especially the National Commission for the Control of Personal Data Protection.

The study further discussed the challenges hindering effective personal data protection, including rapid technological evolution, the rise of cybercrimes and cyberattacks, limited digital awareness, and difficulties related to the practical implementation of legal provisions. In parallel, the research explored ways to strengthen protection through the development of the legal framework, reinforcement of cybersecurity mechanisms, reliance on modern technologies such as encryption, electronic signatures, and artificial intelligence, in addition to promoting digital culture and enhancing institutional and international cooperation.

Keywords: Personal Data; Digital Privacy; Cybersecurity; Law No. 09.08; National Commission for the Control of Personal Data Protection.

تقديم

يشهد العالم المعاصر تحولاً رقمياً متسارعاً، أفرز ثورة معلوماتية غير مسبقة جعلت من المعطيات الشخصية مورداً استراتيجياً ومحوراً أساسياً في مختلف المعاملات الاقتصادية والاجتماعية والإدارية. فقد أضحت هذه المعطيات تشكل العمود الفقري للاقتصاد الرقمي، في ظل الانتشار الواسع للتقنيات الحديثة، كالذكاء الاصطناعي والحوسبة السحابية والبيانات الضخمة، مما أسهم في تسهيل تدفق المعلومات وتبادلها عبر الفضاء السيبراني. غير أن هذا التطور، رغم ما يحمله من مزايا، أفرز في المقابل تحديات جسيمة تمس بشكل مباشر الحق في الخصوصية، نتيجة تزايد مخاطر الاختراقات والهجمات السيبرانية وتسريب البيانات.

وفي هذا السياق، سعت مختلف التشريعات إلى إرساء قواعد قانونية تهدف إلى حماية المعطيات الشخصية، ومن بينها التشريع المغربي الذي أقر ترسانة قانونية مهمة، على رأسها القانون رقم 09.08 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، إلى جانب إحداث مؤسسات متخصصة، من أبرزها اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي، التي تضطلع بدور محوري في ضمان احترام قواعد حماية الخصوصية الرقمية. غير أن الطابع المتسارع للتطور التكنولوجي، وتنامي التهديدات السيبرانية، يطرحان تحديات حقيقية حول مدى فعالية هذه المقتضيات القانونية في مواكبة المخاطر المستجدة، خاصة في ظل تعقد الأساليب التقنية للاختراق وصعوبة ضبطها قانونياً.

وتكمن أهمية هذا الموضوع في كونه يتقاطع مع حماية الحقوق والحريات الأساسية، وعلى رأسها الحق في الحياة الخاصة، من جهة، ومتطلبات الأمن السيبراني وحماية الأنظمة المعلوماتية من جهة أخرى، مما يستدعي البحث عن مقاربة متوازنة تضمن الحماية القانونية الفعالة دون عرقلة التطور التكنولوجي. كما تبرز أهميته العملية في ارتباطه المباشر بثقة الأفراد في البيئة الرقمية، وبأمن المعاملات الإلكترونية، خاصة في ظل تنامي الاعتماد على الخدمات الرقمية في مختلف مناحي الحياة. وانطلاقاً من ذلك، تثار الإشكالية الرئيسية التالية:

إلى أي حد يمكن تحقيق التوازن بين متطلبات الأمن السيبراني وضمان حماية المعطيات الشخصية في ظل تصاعد التهديدات الرقمية؟

ويتفرع عن هذه الإشكالية التساؤلان التاليان:

- ما الإطار القانوني والمؤسسي لحماية المعطيات الشخصية لمواجهة التهديدات السيبرانية؟
- وإلى أي حد تسهم الآليات التقنية الحديثة في تعزيز حماية المعطيات الشخصية وضمان الأمن السيبراني دون المساس بالخصوصية؟

وعليه سنتناول الموضوع وفق التصميم التالي:

المبحث الأول: الإطار القانوني لحماية المعطيات الشخصية في مواجهة التهديدات السيبرانية

المبحث الثاني: التحديات القانونية والتقنية لحماية المعطيات الشخصية في ظل التهديدات السيبرانية

المبحث الأول: الإطار القانوني لحماية المعطيات الشخصية في مواجهة التهديدات السيبرانية

إن حماية المعطيات الشخصية لم تعد مجرد مسألة تقنية أو اختيار تنظيمي، بل أضحت التزاماً قانونياً يفرض نفسه في ظل التحولات الرقمية المتسارعة التي يشهدها العالم. فالتوسع في استخدام الوسائط الإلكترونية، وتزايد الاعتماد على النظم المعلوماتية في تدبير مختلف المعاملات، أفرز واقعاً جديداً أصبحت فيه البيانات الشخصية عرضة لمخاطر متعددة، تتراوح بين الاستغلال غير المشروع والاختراقات السيبرانية المعقدة. وهو ما استدعى تدخل المشرع لوضع قواعد قانونية تضبط كيفية جمع هذه المعطيات ومعالجتها، وتضمن حمايتها من كل مساس محتمل.

وفي هذا السياق، سعى المشرع المغربي إلى بناء منظومة قانونية تروم تأطير حماية المعطيات الشخصية، من خلال سن قواعد تشريعية واضحة وإحداث أجهزة رقابية متخصصة، من أبرزها اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي التي تضطلع بمهمة السهر على احترام الضوابط القانونية في مجال حماية الخصوصية الرقمية. غير أن التطور السريع للتهديدات السيبرانية، وما يواكبه من تعقيد في أساليب الاختراق، يطرح تحدياً حقيقياً أمام فعالية هذه الترسنة القانونية، ويكشف عن حدود قدرتها على مواكبة الواقع الرقمي المتجدد.

وعليه، فإن الإحاطة بالإطار القانوني لحماية المعطيات الشخصية تقتضي ليس فقط استعراض الأسس التشريعية والمؤسسية التي يقوم عليها، بل أيضاً تحليل مدى قدرته على التصدي للتهديدات السيبرانية المتزايدة، وهو ما سيتم تناوله من خلال مطلبين أساسيين.

المطلب الأول: الأساس التشريعي لحماية المعطيات الشخصية

تعد الخصوصية امتداداً طبيعياً للحق في الحياة الخاصة في العصر الرقمي، وهي ترتبط أساساً بالمعطيات الشخصية التي يتم تداولها عبر الانترنت. ويقصد بها "حق الفرد في ان يكون له التحكم والسيطرة على بياناته الرقمية، ومعرفة كيفية جمعها، معالجتها وتخزينها، كما ومشاركتها في البيئة الرقمية".

وتشمل هذه البيانات معلومات عن الهوية، السلوك والموقع ثم الأنشطة على الشبكة، بل وحتى البيانات البيومترية. وللحديث عن الأساس التشريعي لحماية المعطيات الشخصية وجب التطرق إلى الإطار القانوني المنظم لها، ثم الحديث عن المؤسسات المتدخلة للرقابة على تطبيق هذه مقتضيات..

الفقرة الأولى: الإطار القانوني لحماية المعطيات الشخصية

يعتبر حق حماية الحياة الخاصة بمثابة ضمانة دستورية لحماية المعطيات الشخصية للأفراد وذلك ما يستفاد من مضمون الفصل 27 من دستور المملكة المغربية لسنة 2011، وعليه فقد ارتكزت مجموعة من القوانين المتعلقة لحماية المعطيات الشخصية بدءاً بقانون 03.03 المتعلق بمكافحة الإرهاب إلى حدود قانون 09.08.

أولاً: حماية المعطيات الشخصية بمقتضى القانونين 03.03 و 07.03

إنّ المشرع المغربي في القانون رقم 03.03 المتعلق بمكافحة الإرهاب قد أشار إلى المعطيات بشكل عام دون تخصيص لطابعها الشخصي، وذلك في سياق استثنائي طبعته الأحداث الإرهابية التي شهدتها المغرب سنة 2003. وقد تضمن هذا القانون مقتضيات تهم الجرائم المرتبطة بنظم المعالجة الآلية للمعطيات، خاصة عندما تُستعمل في إطار مشروع إرهابي، بما يعكس وعي المشرع بخطورة توظيف التكنولوجيا المعلوماتية لأغراض إجرامية أو إرهابية.

ويكتسي هذا القانون أهمية خاصة باعتباره من أوائل التشريعات المغربية التي نصّت صراحة على الإجرام المعلوماتي كوسيلة لارتكاب أفعال إرهابية، سواء في إطار مشروع فردي أو جماعي يستهدف المس الخطير بالنظام العام عبر التخويف أو التهيب أو العنف. وفي هذا الإطار، حدد الفصل 1-218 مجموعة من الأفعال المجرّمة على سبيل الحصر، من بينها الجرائم المتعلقة بنظم المعالجة الآلية للمعطيات. 205

غير أن الإشارة إلى هذا النوع من الجرائم، خاصة في البند السابع من الفصل المذكور، أثارت إشكالاً قانونياً آنذاك، بالنظر إلى غياب تأطير جنائي خاص بها داخل القانون الجنائي المغربي. وهو ما دفع المشرع إلى التدخل لسد هذا الفراغ التشريعي من خلال سنّ القانون رقم 07.03 المتعلق بالإخلال بسير نظم المعالجة الآلية للمعطيات، والذي أصبح يشكل الإطار القانوني المرجعي لتجريم هذا النوع من الأفعال، مع مراعاة خصوصية الإجرام المعلوماتي وتطوره.

204 ظهير شريف رقم 1.03.140 صادر في 26 ربيع الأول 1424 (28 ماي 2003) بتنفيذ القانون رقم 03.03 المتعلقة بمكافحة الإرهاب.

205 خالد عثمان، مكافحة الجريمة المعلوماتية في ضوء التشريع المغربي، مجلة العلوم الجنائية عدد أول 2014 ص 41.

أما قانون 07.03 المتمم لمجموعة القانون الجنائي المغربي فيعد خطوة تشريعية أساسية هدفت إلى سدّ الفراغ القانوني في مجال مكافحة الجرائم الإلكترونية، ولا سيما تلك المرتبطة بالإخلال بسير نظم المعالجة الآلية للمعطيات. وقد تضمن هذا القانون تسعة فصول، تمتد من الفصل 3-607 إلى الفصل 11-607 من القانون الجنائي المغربي، مما يعكس إرادة المشرّع في مواكبة التطورات الدولية والتشريعات المقارنة في مجال مكافحة الجريمة المعلوماتية.

وقد عرفت الجريمة المعلوماتية بالمغرب خلال العقود الأخيرة تطوراً ملحوظاً وتعدداً في أنماطها، الأمر الذي استدعى تدخلاً تشريعياً خاصاً لتنظيمها وتأطيرها. وفي هذا السياق، يُلاحظ أن المشرّع المغربي لم يُقدّم تعريفاً صريحاً لمفهوم "نظم المعالجة الآلية للمعطيات"، ويبدو أن هذا الاختيار كان مقصوداً، حيث ترك مهمة تحديد هذا المفهوم للفقهاء والقضاء، باعتبارهما الجهتين القادرتين على مواكبة التطبيق العملي للنصوص القانونية. كما يمكن تفسير هذا التوجه بكون المجال المعلوماتي يتسم بالدينامية والتطور المستمر، مما يجعل أي تعريف جامد عرضة للتقادم في ظل التسارع الكبير لتكنولوجيا المعلومات والاتصالات، وهو ما يُضفي نوعاً من المرونة على النص القانوني. 206

ومن جهة أخرى، يتقاطع هذا التوجه مع ما سلكه المشرّع المقارن، لاسيما في التشريع الفرنسي المتعلق بالغش المعلوماتي لسنة 1988، حيث لم يتم بدوره وضع تعريف محدد لنظام المعالجة الآلية للمعطيات، بل تم الاكتفاء بتحديد صور الأفعال المجرّمة المرتبطة به والعقوبات المقررة لها. وهو ما يعزز الطابع العملي للتشريع، من خلال التركيز على الأفعال الإجرامية بدل الانشغال بالتعريفات النظرية التي قد لا تواكب التطور التقني. 207

والجدير بالذكر إن القراءة الشمولية لمقتضيات القانون رقم 07.03 تُمكن من استخلاص وتصنيف الأفعال المجرّمة المرتبطة بنظم المعالجة الآلية للمعطيات، سواء في صورتها التامة أو في مرحلة المحاولة، خاصة تلك التي تمسّ المعطيات ذات الطابع الشخصي من حيث الولوج إليها أو معالجتها بمختلف صورها، كالتعديل أو الحذف أو النقل، وذلك انسجاماً مع مقتضيات القانون رقم 09.08 المتعلق بحماية المعطيات ذات الطابع الشخصي.

وفي هذا الإطار، يمكن حصر أبرز هذه الأفعال الإجرامية في مجموعة من الصور، من بينها الولوج الاحتيالي إلى كل أو بعض نظام للمعالجة الآلية للمعطيات، أو البقاء غير المشروع داخله بعد الدخول إليه عن طريق الخطأ، فضلاً عن الأفعال التي تستهدف سلامة المعطيات، كحذفها أو تغييرها أو إتلافها. كما يشمل التجريم كل تدخل من شأنه إحداث خلل في سير النظام المعلوماتي، أو تغيير المعطيات المخزنة فيه عن طريق الإدخال أو الإتلاف أو التعديل، إضافة إلى التلاعب في طرق المعالجة أو نقل المعطيات بشكل احتيالي.

ويتمد نطاق التجريم كذلك ليشمل أفعال التزوير أو التزييف التي تطل الوثائق المعلوماتية، كيفما كان شكلها، متى كان من شأن ذلك إلحاق ضرر بالغير، وهو ما يعكس توجهاً تشريعياً يروم حماية الثقة في المعاملات الرقمية وضمان أمن النظم المعلوماتية. وتجدر الإشارة إلى أن هذا التوجه يتماشى مع ما استقر عليه الفقه المقارن، حيث تُعد جرائم الولوج غير المشروع، وتعديل أو حذف المعطيات، وإعاقة سير الأنظمة المعلوماتية، من أبرز صور الجريمة المعلوماتية التي تحرص التشريعات الحديثة على تجريمها، نظراً لما تُشكّله من تهديد مباشر لسلامة وأمن المعلومات.

ثانياً: حماية المعطيات الشخصية بمقتضى قانون 09.08 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات إلى غاية نهاية سنة 2008، لم يكن الإطار القانوني المغربي يتضمن تنظيمات متكاملة لحماية المعطيات ذات الطابع الشخصي، رغم التحولات المتسارعة التي شهدتها هذا المجال على الصعيد الدولي. وقد كشفت الدراسات التي أنجزتها مديرية الدراسات بوزارة

206 محمد جوهر، خصوصيات زجر الإجرام المعلوماتي، المجلة المغربية للقانون والاقتصاد والتدبير عدد 52 2006 ص 87.

207 لحسن علاوي، حماية المعطيات الشخصية بين القانوني والمؤسسي، رسالة لنيل دبلوم الماستر في القانون الخاص جامعة مولاي إسماعيل مكناس سنة 2021/2022 ص 20.

الاقتصاد والمالية عن ضرورة إرساء منظومة قانونية حديثة تستجيب لمتطلبات حماية الحياة الخاصة، وتنسجم مع المعايير المعتمدة دولياً، خاصة التوجهات الأوروبية والتجربة التشريعية الفرنسية. 208

في هذا السياق، تم اعتماد القانون رقم 09.08 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، متأثراً في بنيته ومضامينه بالقانون الفرنسي رقم 78.17 الصادر سنة 1978 بشأن المعلوماتية والملفات والحريات. ويشكل هذا القانون خطوة نوعية نحو تأطير عمليات جمع ومعالجة البيانات الشخصية من طرف الهيئات العمومية والقطاع الخاص، بما يضمن التوازن بين متطلبات التطور التكنولوجي وحقوق الأساسية للأفراد.

ويستند هذا الإطار القانوني إلى مقتضيات دستورية، لاسيما الفصل 24 من الدستور، الذي يكرس الحق في حماية الحياة الخاصة. ومن ثم، خول القانون للأشخاص المعنيين بالمعالجة مجموعة من الحقوق الأساسية، من قبيل الحق في الموافقة المسبقة، والحق في الإخبار، وحق الولوج إلى المعطيات، فضلاً عن حق التصحيح والتعرض على المعالجة.

وفي مقابل ذلك، رتب القانون مجموعة من الالتزامات على عاتق المسؤول عن المعالجة، من أبرزها ضرورة احترام الغاية المحددة من جمع البيانات، والتقيد بمبدأ التناسب، وضمان جودة المعطيات ودقتها. كما يتضمن هذا النص القانوني جملة من المبادئ والقواعد التي تتماشى مع المعايير الأوروبية والاتفاقيات الدولية ذات الصلة. 210

ولا تقتصر أهمية هذا القانون على حماية الحقوق الفردية فحسب، بل تمتد لتشمل تعزيز جاذبية المغرب في مجال الاستثمار، خاصة في قطاع ترحيل الخدمات، من خلال توفير بيئة قانونية موثوقة تضمن حماية المعطيات وتدعم الثقة بين الفاعلين الاقتصاديين على الصعيدين الوطني والدولي.

المطلب الثاني: الإطار المؤسسي لحماية المعطيات الشخصية

يأتي إقرار القانون رقم 09.08 في سياق سعي المغرب إلى تحديث منظومته القانونية وتعزيز حماية حقوق الإنسان بمختلف أبعادها، بما ينسجم مع التحولات الرقمية المتسارعة، خاصة في مجال التجارة الإلكترونية وتطوير الإدارة الرقمية وجذب الاستثمارات. كما يعكس هذا التوجه انخراط المغرب في المعايير الدولية، لاسيما التوجهات الأوروبية، وتفعيل التزاماته بموجب انضمامه إلى الاتفاقية رقم 108 لمجلس أوروبا.

وفي هذا الإطار، أحدث المشرع مؤسسة محورية تتمثل في :

الفقرة الأولى: اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي (CNDP)

تتكون هذه اللجنة، وفق المادة 32 من القانون 09.08، من سبعة أعضاء يُعينهم الملك، من بينهم الرئيس، وذلك بناءً على اقتراحات صادرة عن رئيس الحكومة ورئيسي مجلسي البرلمان، لمدة انتداب محددة في خمس سنوات قابلة للتجديد مرة واحدة.

أما بخصوص طبيعتها القانونية، فإن المشرع لم ينص عليها صراحة، غير أن الفقه يميل إلى اعتبارها هيئة إدارية مستقلة، تتمتع بسلطات تقريرية واستشارية، دون أن ترقى إلى مستوى هيئة قضائية. فهي تمارس اختصاصاتها باستقلال عن السلطة التنفيذية، ولا تخضع للوصاية الإدارية، مع خضوع قراراتها لرقابة القضاء من خلال الطعون القضائية. 211

وتتوزع اختصاصات اللجنة بين عدة وظائف أساسية، أبرزها:

- وظيفة استشارية: من خلال إبداء الرأي بشأن مشاريع ومقترحات القوانين والنصوص التنظيمية المرتبطة بحماية المعطيات الشخصية؛ 212

208 علي أرجدال، حماية المعطيات الشخصية بالمغرب دراسة تحليلية ومقارنة رسالة لنيل الماستر في القانون الخاص جامعة محمد الخامس بالرباط سنة 2018/2019 ص 78.

209 ظهير شريف رقم 09.15 المؤرخ في 18 فبراير 2009 القاضي بتنفيذ قانون 09.08 منشور في الجريدة الرسمية عدد 5711 بتاريخ 23 فبراير 2009.

210 لحسن علاوي حماية المعطيات الشخصية بين القانوني والمؤسسي مرجع سابق ص 18.

211 لبنى الوزاني، الرقابة القضائية على أعمال اللجنة الوطنية لحماية المعطيات الشخصية، مقال منشور في مجلة القضاء محكمة الاستئناف بالبيضاء عدد 2 سنة 2018 ص 15.

212 إيمان التيس، التجارة الإلكترونية وضوابط حماية المستهلك في المغرب، أطروحة لنيل الدكتوراه في القانون الخاص، جامعة المولى إسماعيل مكناس سنة 2014/2015 ص 228.

• وظيفة تقريرية وتنظيمية: عبر منح التراخيص أو سحبها، واتخاذ التدابير اللازمة لضمان أمن المعطيات واحترام النظام العام؛²¹³

- وظيفة إخبارية: تهدف إلى توعية العموم بحقوقهم والتزاماتهم في مجال حماية المعطيات؛
- وظيفة رقابية وتحقيقية: تخول لأعوانها صلاحيات الولوج إلى أماكن المعالجة وجمع الوثائق الضرورية؛
- وظيفة شبه قضائية: من خلال تلقي الشكايات، والتحقيق فيها، واتخاذ ما يلزم من إجراءات، بما في ذلك إحالة الملفات على النيابة العامة عند الاقتضاء.²¹⁴

الفقرة الثانية: اللجان الوطنية ذات الطابع الأمني

وتنقسم هذه اللجان إلى لجان على مستوى الدفاع الوطني وأخرى محدثة لدى المديرية العامة للأمن الوطني.

أولاً: الهيئات المحدثة لدى الدفاع الوطني

في إطار تعزيز الأمن السيبراني وحماية المعطيات ذات الطابع السيادي، عملت إدارة الدفاع الوطني على إحداث اللجنة الاستراتيجية لأمن نظم المعلومات، باعتبارها هيئة مركزية تضطلع بوضع السياسة العامة للدولة في مجال أمن الأنظمة المعلوماتية. وتضم هذه اللجنة عدداً من المسؤولين والفاعلين الأمنيين والعسكريين، من بينهم الوزير المكلف بإدارة الدفاع الوطني، والمدير العام للدراسات والمستندات، والمدير العام لمراقبة التراب الوطني، إلى جانب رئيس المكتب الخامس لأركان الحرب العامة للقوات المسلحة الملكية، فضلاً عن ممثلي مديرية أمن نظم المعلومات.²¹⁵

وتنص المادة الأولى²¹⁶ على إحداث هذه اللجنة لدى إدارة الدفاع الوطني، مع إسناد مجموعة من الاختصاصات الأساسية إليها، من أبرزها تحديد الاختيارات والتوجهات الاستراتيجية للدولة في مجال أمن نظم المعلومات بما يكفل حماية المعلومات السيادية وضمان استمرارية اشتغال البنيات التحتية الحيوية. كما تتولى المصادقة على برامج عمل المديرية العامة لأمن نظم المعلومات، وتقييم حصيلة أنشطتها ونتائج تدخلاتها، إضافة إلى تحديد نطاق عمليات الافتتاح المتعلقة بأمن المعلومات وكيفية تنفيذها، فضلاً عن إبداء الرأي في مشاريع النصوص القانونية المرتبطة بمجال أمن نظم المعلومات.

ويرأس هذه اللجنة الوزير المكلف بإدارة الدفاع الوطني، بينما تتكون عضويتها من عدد من الوزراء ومسؤولي المؤسسات والهيئات العمومية، وفق ما حددته المادة الثالثة من النص المنظم لها

كما تم إحداث المديرية العامة لأمن نظم المعلومات سنة 2011 لدى إدارة الدفاع الوطني، وأسندت إليها مهام متعددة تروم تعزيز الأمن المعلوماتي على المستوى الوطني. وتتمثل أهم اختصاصاتها في تنسيق الجهود بين مختلف القطاعات الحكومية من أجل إعداد استراتيجية وطنية شاملة لأمن نظم المعلومات، واقتراح المعايير والضوابط التقنية المتعلقة بالحماية المعلوماتية، إلى جانب تدبير التراخيص المرتبطة بخدمات المصادقة الإلكترونية.

كما تضطلع المديرية بمهمة مواكبة المؤسسات العمومية والخاصة عبر تقديم الدعم والاستشارة في مجال تأمين الأنظمة المعلوماتية، فضلاً عن القيام بعمليات التدقيق والافتتاح الأمني داخل المؤسسات العمومية. وتتكلف كذلك بوضع آليات لرصد الهجمات السيبرانية التي قد تستهدف البنيات التحتية المعلوماتية الوطنية، مع العمل على الحد من آثارها وتنسيق عمليات الاستجابة للحوادث المعلوماتية.²¹⁷

213 سكيبة بن الشيخ، الأمن القانوني المعلوماتي، رسالة ماستر في القانون الخاص، جامعة القاضي عياض مراكش، سنة 2014/2015 ص116.

214 المادة 28 من قانون 09.08.

215 لحسن علاوي، حماية المعطيات الشخصية بين القانوني والمؤسسي، مرجع سابق ص31.

216 مرسوم رقم 508-11-2 الصادر في 22 شوال 1431 الموافق ل 21 شتنبر 2011 بإحداث اللجنة الاستراتيجية لأمن نظم المعلومات الجريدة الرسمية عدد 5987 بتاريخ 25 شتنبر 2011.

217 تقرير حماية المعطيات ذات الطابع الشخصي في إطار قطاع الأمن بالمغرب، مركز دراسات حقوق الإنسان والديموقراطية ص26.

ومن بين المهام الموكولة إليها أيضاً تتبع التطورات التقنية في مجال الأمن السيبراني بشكل استباقي، واقتراح الحلول والتدابير الكفيلة بتعزيز الحماية الرقمية، إضافة إلى تنظيم دورات تكوينية وتحسيسية لفائدة موظفي الإدارات والمؤسسات العمومية بهدف نشر ثقافة الأمن المعلوماتي.

وقد أوكلت هذه الاختصاصات إلى المديرية العامة لأمن نظم المعلومات بالنظر إلى الدور المحوري الذي تضطلع به في حماية سلامة الأنظمة المعلوماتية الوطنية²¹⁸. وفي إطار تنفيذ برنامج عملها لسنة 2013، قامت بإعداد وثيقة مرجعية تضمنت التوجيهات الوطنية الخاصة بأمن نظم المعلومات، وهي الوثيقة التي صادقت عليها اللجنة الاستراتيجية لأمن نظم المعلومات خلال اجتماعها الثاني المنعقد بمدينة الرباط بتاريخ 21 يناير 2014.

ثانياً: الهيئات المحدثة لدى المديرية العامة للأمن الوطني

في سياق مواكبة التحولات المتسارعة التي فرضها التطور التكنولوجي وارتفاع مخاطر الجريمة الإلكترونية، عملت الإدارة العامة للأمن الوطني على إحداث مديرية نظم المعلومات والاتصال لمواكبة التطور التكنولوجي ومواجهة الجريمة الإلكترونية. وتتمثل مهامها في تطوير البنية التحتية الرقمية، وتحديث الأنظمة المعلوماتية، وضمان أمن وحماية المعطيات، إضافة إلى إعداد المشاريع التقنية ودعم اتخاذ القرار وتفعيل استراتيجيات الحكومة الإلكترونية، مع التنسيق المستمر مع مختلف الجهات المعنية بمجال تكنولوجيا المعلومات²¹⁹.

كما أحدثت وحدة جرائم المعلومات لدى الفرقة الوطنية للشرطة القضائية لمواجهة الجرائم الإلكترونية المتزايدة. وتشرف عليها أطر متخصصة في الهندسة المعلوماتية وشبكات الإنترنت، وتم تجهيزها بوسائل تقنية حديثة للرصد والتحليل. وتتمثل مهامها أساساً في دعم الأبحاث القضائية ومعالجة الجرائم المعلوماتية، بما يواكب التطور السريع لتقنيات الاتصال والجريمة الإلكترونية²²⁰.

ثالثاً: اللجان المنصوص عليها في القانون 05.20

يشكل القانون 05.20 المتعلق بالأمن السيبراني خطوة مهمة في تعزيز الحماية القانونية للفضاء الرقمي بالمغرب، حيث نص على إحداث لجان متخصصة تتولى تأمين المجال السيبراني وتدبير المخاطر المرتبطة به، وفي مقدمتها اللجنة الاستراتيجية للأمن السيبراني ولجنة إدارة الأزمات والأحداث السيبرانية الجسيمة²²¹.

نصت المادة 35 من القانون 05.20 على إحداث لجنة استراتيجية للأمن السيبراني تتولى إعداد التوجيهات الاستراتيجية للدولة في مجال الأمن السيبراني، والسهر على تعزيز صمود نظم معلومات الهيئات والبنيات التحتية ذات الأهمية الحيوية. كما أحال القانون على نص تنظيمي لتحديد كيفية تأليف هذه اللجنة وتنظيم سيرها.

إلى جانب اللجنة الاستراتيجية، أحدث القانون لجنة خاصة بإدارة الأزمات والأحداث السيبرانية الجسيمة، تتكلف بضمان تدخل منسق في مجال الوقاية وتدبير الأزمات الناتجة عن الحوادث السيبرانية. كما ألزم القانون مستغلي الشبكات العامة للمواصلات ومزودي خدمات الإنترنت والخدمات الرقمية بالامتثال لتعليمات هذه اللجنة وتقديم الدعم والمساعدة التقنية عند الطلب. وقد أحال المشرع بدوره على نص تنظيمي لتحديد تأليف اللجنة وكيفية اشتغالها واختصاصات أعضائها²²².

المبحث الثاني: التحديات القانونية والتقنية لحماية المعطيات الشخصية في ظل التهديدات السيبرانية

218 عدنان الزرزوري، مكافحة الإرهاب المعلوماتي، رسالة لنيل الماستر في القانون الخاص جامعة المولى إسماعيل مكناس سنة 2017/2018 ص 144.

219 مرسوم رقم 2-10-84 صادر في 21 ربيع الثاني 1431 الموافق ل 7 أبريل 2010 بتحديد اختصاصات المديرية المركزية التابعة للمديرية العامة للأمن الوطني.

220 سكيمة بن الشيخ، الأمن القانوني المعلوماتي مرجع سابق ص 131.

221 منشور رقم 3-14 بتطبيق التوجيهات الوطنية لأمن نظم المعلومات، صادر في 10 مارس 2014.

222 لحسن علاوي، حماية المعطيات الشخصية بين القانوني والمؤسسي، مرجع سابق ص 34.

إن تضخم المعطيات الشخصية بفعل التسارع الرقمي قد أفرز تحديات قانونية وتقنية في هذا السياق، خاصة مع تنامي التهديدات السيبرانية التي أصبحت تستهدف المعطيات الشخصية بشكل مباشر، سواء من خلال الاختراقات الإلكترونية أو الاستعمال غير المشروع للبيانات أو الهجمات المعلوماتية التي تمس الحق في الخصوصية الرقمية.

وفي ظل هذا الواقع، برزت الحاجة إلى إرساء منظومة قانونية وتقنية قادرة على تحقيق التوازن بين الاستفادة من التطور الرقمي وضمان حماية المعطيات الشخصية للأفراد. غير أن فعالية هذه الحماية تظل رهينة بمدى نجاعة الآليات المعتمدة وقدرتها على مواكبة التطور المستمر للجرائم السيبرانية والتقنيات الحديثة. وعليه، سيتم التطرق في هذا المبحث إلى محدودية آليات حماية المعطيات الشخصية في مواجهة التهديدات السيبرانية ضمن مطلب أول، على أن يتم في المطلب الثاني تناول دور التقنيات الحديثة في تعزيز الحق في الخصوصية الرقمية وحماية البيانات الشخصية.

المطلب الأول: محدودية آليات حماية المعطيات الشخصية

أفرزت الثورة الرقمية واقعا جديدا أصبحت فيه المعطيات الشخصية تشكل محورا أساسيا في مختلف المعاملات والأنشطة الإلكترونية، الأمر الذي جعلها عرضة لمخاطر متعددة تهدد الحياة الخاصة للأفراد وتمس بحقوقهم وحياتهم الأساسية. فالتطور المتسارع لتكنولوجيا المعلومات والاتصال، وما صاحبه من انتشار واسع للخدمات الرقمية والتجارة الإلكترونية، أدى إلى تضاعف عمليات جمع البيانات ومعالجتها وتبادلها، مما منح المعطيات الشخصية قيمة اقتصادية واستراتيجية متزايدة.

وأمام هذه التحولات، سارعت العديد من التشريعات والهيئات الدولية إلى وضع قواعد قانونية وتنظيمية تهدف إلى حماية الخصوصية المعلوماتية وتأمين المعالجة المشروعة للبيانات الشخصية. كما لعبت عدة منظمات دولية، من بينها منظمة الأمم المتحدة ومنظمة التعاون والتنمية الاقتصادية ومنظمة التجارة العالمية، دورا بارزا في تكريس مبادئ حماية المعطيات الشخصية وتعزيز آليات التصدي للمخاطر الرقمية المرتبطة بها.

ورغم أهمية هذه الجهود وما أفرزته من قواعد قانونية حديثة تروم حماية الأفراد من التجاوزات المرتبطة بمعالجة المعطيات، فإن الواقع العملي يكشف عن استمرار العديد من الثغرات التي تحد من فعالية هذه الحماية، سواء على المستوى القانوني أو التقني، لاسيما في ظل التطور المستمر للجرائم السيبرانية وصعوبة مراقبة التدفقات العابرة للحدود للبيانات الشخصية.

لذلك، سنعمل على إبراز أبرز أوجه القصور التي تعترى آليات حماية المعطيات الشخصية على المستوى الدولي (الفقرة الأولى)، قبل التطرق إلى أهم التحديات والإكراهات التي تواجه الآليات الوطنية في هذا المجال (الفقرة الثانية).

الفقرة الأولى: قصور الحماية الدولية للمعطيات الشخصية

إن مجالات تداول ومعالجة المعطيات الشخصية لم تعد قابلة للحصر أو التقييد، بعدما أصبحت التكنولوجيا الرقمية متغلغلة في مختلف مناحي الحياة العملية والاقتصادية والعلمية. وقد أدى هذا التوسع إلى تعقيد مسألة مراقبة المعطيات الشخصية وتأمين حمايتها، بحيث لم يعد من الممكن الاعتماد على آلية واحدة، سواء كانت تشريعية أو مؤسسية، للتصدي لمخاطر المعالجة غير المشروعة. لذلك، أصبحت حماية المعطيات الشخصية رهينة بتعاون وتكامل جهود مختلف الفاعلين على المستويين الوطني والدولي.

غير أن هذا التعاون يصطدم بتباين المصالح والاستراتيجيات بين الدول والمؤسسات الاقتصادية والتكنولوجية، خاصة في ظل التنافس المتزايد حول استغلال المعطيات الشخصية لتحقيق أهداف تجارية أو علمية أو اقتصادية. فالمعطيات الرقمية أضحت موردا استراتيجيا يساهم في فتح أسواق جديدة وتطوير مجالات البحث والاستثمار، الأمر الذي يجعل بعض التدخلات التشريعية الرامية إلى حماية الخصوصية تُعتبر أحيانا عائقا أمام هذه المصالح.

وفي هذا الإطار، تبرز مجموعة من المعوقات التي تحد من فعالية التعاطي الدولي مع حماية المعطيات الشخصية على المستوى التشريعي، من أهمها:

أولاً: محدودية الإلزامية في النصوص القانونية الدولية المتعلقة بحماية المعطيات الشخصية

يلاحظ أن أغلب القواعد والاتفاقيات الدولية المنظمة لحماية المعطيات الشخصية لا تتخذ طابعاً إلزامياً، بل تظل في كثير من الأحيان مجرد مبادئ توجيهية أو توصيات موجهة للدول، دون وجود آليات فعالة لإجبارها على التطبيق أو معاقبة المخالفين لها. ويتجلى ذلك خاصة في التوصيات الصادرة عن منظمة التعاون والتنمية الاقتصادية ومنظمة العمل الدولية ومنظمة التجارة العالمية، إضافة إلى المبادئ التوجيهية الصادرة عن منظمة الأمم المتحدة.

ورغم انتماء العديد من الدول إلى هذه المنظمات، فإن عدداً منها لا يزال يفتقر إلى تشريعات وطنية خاصة بحماية المعطيات الشخصية، وهو ما يبرز محدودية فعالية هذه التوصيات على المستوى العملي. في المقابل، تتميز التوجيهات ذات الطابع الأوروبي بقدر أكبر من الإلزامية، غير أن نطاقها يظل محصوراً أساساً في الدول الأعضاء، التي تلتزم بملاءمة تشريعاتها الداخلية مع الحد الأدنى من معايير الحماية المقررة.²²³

ثانياً: اختلاف الأنظمة القانونية وأثره على الحماية الدولية للمعطيات الشخصية

يشكل اختلاف الأنظمة القانونية والإجرائية بين الدول أحد أبرز العوائق التي تواجه إرساء حماية دولية موحدة للمعطيات الشخصية. فالإجراءات التي تعتبر مشروعة وفعالة في دولة معينة قد تكون غير قانونية أو غير معترف بها في دولة أخرى، سواء تعلق الأمر بوسائل البحث والتحقيق أو بطرق جمع الأدلة والإثبات.

ومن ثم، قد ترفض بعض الدول الاعتماد على أدلة تم الحصول عليها وفق إجراءات تراها دول أخرى قانونية، وهو ما يعرقل التعاون الدولي في مواجهة الجرائم والاعتداءات الإلكترونية.

ويبرز ذلك بوضوح من خلال قضية "الدودة الحاسوبية" التي شهدتها العالم سنة 2000، حيث تسببت برمجية خبيثة في إصابة عدد كبير من الحواسيب عبر عدة دول. غير أن اختلاف الأنظمة القانونية للدول المتضررة، وغياب تجريم بعض هذه الأفعال آنذاك في عدد من التشريعات الوطنية، أدى إلى إضعاف إمكانية التصدي السريع لهذه الهجمات والحد من أثارها.²²⁴

وعليه، فإن تباين التشريعات القانونية عبر العالم يظل من أبرز العوامل التي تحول دون وضع إطار قانوني دولي موحد وفعال لمواجهة الاعتداءات الإلكترونية التي تستهدف الحياة الخاصة والمعطيات الشخصية، أو على الأقل الحد من مخاطرها.²²⁵

الفقرة الثانية: محدودية الآليات الوطنية لحماية المعطيات الشخصية

رغم الجهود التي بذلها المشرع المغربي من خلال إرساء منظومة قانونية ومؤسسية لحماية المعطيات ذات الطابع الشخصي، فإن هذه الآليات لا تزال تواجه عدة صعوبات تحد من فعاليتها في تحقيق حماية حقيقية للحق في الخصوصية الرقمية. فالتطور المتسارع للتكنولوجيا الرقمية، وتنامي أساليب المعالجة الإلكترونية للبيانات، يفرضان تحديات متجددة تجعل من الصعب مواكبتها تشريعياً ومؤسسياً بالسرعة المطلوبة.

وتتجلى محدودية الحماية الوطنية أساساً في الإشكالات المرتبطة بتنزيل مقتضيات القانون رقم 09.08، إضافة إلى الإكراهات التي تعترض عمل اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي، سواء في الظروف العادية أو خلال الفترات الاستثنائية، كما هو الشأن أثناء تدبير حالة الطوارئ الصحية المرتبطة بجائحة كوفيد-19.

223 حسن الحافظي، الحماية القانونية للمعطيات ذات الطابع الشخصي بين التشريع الوطني والاتفاقيات الدولية، رسالة لنيل الماستر في القانون الخاص جامعة المولى إسماعيل بمكناس سنة 2017/2017 ص 101.

224 سكينه بن الشيخ، الأمن القانوني المعلوماتي، مرجع سابق ص 173.

225 لحسن علاوي، حماية المعطيات الشخصية بين القانوني والمؤسسي، مرجع سابق ص 37.

أولاً: إشكالات تنزيل القانون 09.08

يرتبط التطبيق الفعلي لمقتضيات القانون رقم 09.08 بمدى وعي مختلف المتدخلين، سواء المسؤولين عن معالجة المعطيات أو الأشخاص المعنيين بها، بأهمية الحقوق والضمانات التي يقرها هذا القانون، وكذا بالآثار القانونية المترتبة عن مخالفتها. غير أن التطور المستمر للتقنيات المعلوماتية يجعل النصوص القانونية، مهما بلغت درجة دقتها، عاجزة أحياناً عن مواكبة التحولات التكنولوجية المتسارعة. ويزداد هذا الإشكال بالنظر إلى كون القانون المغربي استلهم بدرجة كبيرة من التوجيهات والتشريعات الأوروبية التي تعود إلى فترات سابقة، الأمر الذي جعل مقتضياته تواجه اليوم تحديات جديدة، خاصة بعد صدور نظام RGPD، الذي فرض معايير أكثر صرامة في مجال حماية المعطيات الشخصية. وهو ما يدفع المغرب، باعتباره شريكاً اقتصادياً للاتحاد الأوروبي، إلى ضرورة مراجعة تشريعاته وملاءمتها مع المستجدات الدولية حتى لا يتأثر تعامله الاقتصادي والتجاري مع الفضاء الأوروبي. 226

ومن جهة أخرى، فإن الجرائم المرتبطة بمعالجة المعطيات الشخصية تندرج ضمن الجرائم المعلوماتية التي تتميز بصعوبة اكتشافها وإثباتها، لكونها غالباً لا تترك أثراً مادية واضحة، كما أن البيانات الرقمية يمكن تعديلها أو محوها بسهولة من الأنظمة المعلوماتية. إضافة إلى ذلك، قد يتم ارتكاب هذه الأفعال من خارج الحدود الوطنية، وهو ما يظهر بوضوح مع بعض المنصات والشركات الرقمية العالمية التي تتهم مراراً بانتهاك الخصوصية الرقمية واستغلال المعطيات الشخصية لأغراض تجارية. 227

كما تبرز محدودية وسائل الإثبات التي اعتمدها القانون رقم 09.08، خاصة اعتماد المحاضر كوسيلة أساسية للإثبات، رغم أن هذا النوع من الجرائم يتطلب خبرات تقنية متخصصة وآليات بحث وتحقيق متطورة. فمحاضر الشرطة القضائية تعاني أحياناً من ضعف التكوين والخبرة التقنية في مجال الجرائم المعلوماتية، في حين أن محاضر أعوان اللجنة الوطنية لا تتمتع بحجية صريحة وواضحة بمقتضى القانون. أما على مستوى العقوبات، فقد اتجه المشرع إلى اعتماد مقارنة مستمدة من القانون الجنائي للأعمال، من خلال إقرار عقوبات مخففة نسبياً تجمع بين الغرامة والعقوبة الحبسية أو تكتفي بإحداهما، وهو توجه وإن كان يراعي خصوصيات المجال الاقتصادي والاستثماري، فإنه لا ينسجم دائماً مع خطورة الاعتداءات التي قد تمس الحقوق والحريات الأساسية للأفراد وتهدد أمنهم الاجتماعي وكرامتهم.

ثانياً: محدودية دور اللجنة الوطنية لحماية المعطيات الشخصية

رغم الأهمية التي تضطلع بها اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي في السهر على احترام قواعد حماية المعطيات الشخصية، فإن القانون رقم 09.08 أورد مجموعة من المقتضيات التي تكشف محدودية الدور الممنوح لها. ويظهر ذلك أساساً من خلال غياب التنصيص الصريح على استقلاليتها بالشكل الذي يضمن لها هامشاً واسعاً من الفعالية، خلافاً لبعض الهيئات المقارنة، كالنموذج الفرنسي. كما أن اللجنة لا تتوفر على صلاحيات زجرية واسعة تمكنها من فرض احترام مقتضيات القانون بشكل مباشر، إذ يقتصر دورها أساساً على اتخاذ قرارات إدارية وتأديبية أو إحالة بعض الأفعال على النيابة العامة المختصة، فضلاً عن خضوع قراراتها للرقابة القضائية، مما يحد من قوة تدخلها وفعاليتها العملية في ضمان حماية المعطيات الشخصية. 228

226 خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، طبعة أولى دار الجامعة، الإسكندرية 2008 ص 47.

227 لحسن علاوي، حماية المعطيات الشخصية بين القانوني والمؤسسي، مرجع سابق ص 39.

228 عبد المجيد كوزي، الحماية القانونية للبيانات والمعطيات ذات الطابع الشخصي، أطروحة لنيل الدكتوراه في القانون الخاص جامعة محمد بن عبد الله فاس سنة 2014/2015 ص 358.

ومن أبرز مظاهر القصور كذلك ضعف الدور التحسيبي والتوعوي الذي يفترض أن تضطلع به اللجنة لنشر الثقافة القانونية المرتبطة بحماية المعطيات الشخصية داخل المجتمع المغربي، خاصة وأن هذا المجال لا يزال حديثا نسبيا، في ظل محدودية الوعي المجتمعي بخطورة تداول المعطيات الشخصية وآثارها على الحقوق والحريات الفردية. ولا تقتصر هذه الصعوبات على الجانب المؤسسي فقط، بل تمتد أيضا إلى السلطة القضائية باعتبارها الضامن الأساسي لحماية الحقوق والحريات، حيث يلاحظ استمرار ضعف التكوين والخبرة التقنية في مجال الجرائم المعلوماتية وجرائم معالجة المعطيات الشخصية، وهو ما يؤثر على فعالية تطبيق القانون وتحقيق الأهداف التي توخاها المشرع من خلال القانون رقم 229.09.08

وقد برزت هذه الإشكالات بشكل أوضح خلال فترة انتشار جائحة كوفيد-19، وما رافقها من إعلان حالة الطوارئ الصحية بموجب مرسوم رقم 2.20.293 بتاريخ 24 مارس 2020، حيث اضطرت السلطات العمومية إلى اعتماد مجموعة من التدابير الرقمية والاحترازية التي استندت إلى معالجة المعطيات الشخصية للأفراد، خاصة المعطيات المرتبطة بالحالة الصحية والتنقل.

وفي هذا السياق، أثار اعتماد تطبيق WIQAYTNA، وكذا فرض الجواز الصحي، نقاشا حقوقيا وقانونيا واسعا بشأن مدى احترام الحق في الخصوصية وحماية المعطيات الشخصية. وقد دافعت اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي عن مشروعية استعمال الجواز الصحي باعتباره وسيلة تهدف إلى حماية الصحة العامة وإنعاش النشاط الاقتصادي، مؤكدة أن استعمال رمز QR لا يسمح بتتبع تحركات المواطنين أو الولوج إلى معطيات إضافية غير تلك الظاهرة داخل الجواز. 230

غير أن هذه التبريرات لم تمنع من استمرار الانتقادات الحقوقية التي اعتبرت بعض التدابير المتخذة خلال حالة الطوارئ مسا بالحرريات الفردية وحرية التنقل والحق في حماية الحياة الخاصة، خاصة في ظل التخوف من استعمال المعطيات الصحية خارج الأهداف التي جُمعت من أجلها.

ومهما كانت المبررات المرتبطة بالوضع الصحي الاستثنائي، فإن المعطيات الشخصية المرتبطة بالصحة تظل من أكثر البيانات حساسية، الأمر الذي يفرض ضرورة إخضاع معالجتها لرقابة قانونية دقيقة، وضمان استعمالها فقط في الحدود التي تقتضيها المصلحة العامة، مع تعزيز وعي الأفراد بأهمية حماية معطياتهم الشخصية في البيئة الرقمية.

المطلب الثاني: دور التقنيات الحديثة في تعزيز الحق في الخصوصية الرقمية

إن تزايد المخاطر التي تهدد المعطيات الشخصية والخبرات في الخصوصية الناتج عن التطور التكنولوجي، أدى إلى ضرورة الاعتماد على التقنيات الحديثة لتعزيز الحماية المعلوماتية، وعكف بهذا الإطار ظهرت مجموعة من التقنيات والتي يمكن تصنيفها في صنفين: أولا: التقنيات الوقائية لتعزيز المعطيات الشخصية

ويقصد بالتقنيات الوقائية تلك التي تهدف إلى منع الاختراقات والتقليل من مخاطر الوصول غير المشروع إلى البيانات، ومن أبرزها: 1- التوقيع الإلكتروني

بعد التوقيع الإلكتروني من أبرز الوسائل التقنية الحديثة التي تساهم في تعزيز حماية المعطيات الشخصية وتأمين المعاملات الرقمية، إذ يتيح التحقق من هوية الأطراف وضمان سلامة الوثائق الإلكترونية من أي تعديل أو تزوير. كما يوفر مستوى متقدما من الثقة والأمان في البيئة الرقمية، من خلال تأكيد صدور التصرف الإلكتروني عن صاحبه الحقيقي وعدم إمكانية إنكاره لاحقا، الأمر الذي يجعله أداة فعالة لحماية الحقوق الشخصية وتعزيز الأمن القانوني للمعاملات الإلكترونية، خاصة في ظل تنامي استخدام الخدمات الرقمية والتبادل الإلكتروني للبيانات.

وقد كرس المشرع المغربي الحماية القانونية للتوقيع الإلكتروني من خلال القانون رقم 43.20 المتعلق بخدمات الثقة بشأن المعاملات الإلكترونية، الذي جاء لتعزيز الأمن القانوني والرقمي للمعاملات الإلكترونية ومواكبة التطور التكنولوجي المتسارع. وقد اعترف هذا

229 عبد المجيد كوزي، الحماية القانونية للبيانات والمعطيات ذات الطابع الشخصي، مرجع سابق ص 358.

230 لحسن علاوي، حماية المعطيات الشخصية بين القانوني والمؤسسي، مرجع سابق ص 40.

القانون بالحجة القانونية للتوقيع الإلكتروني، متى استوفى الشروط التقنية والقانونية المنصوص عليها، وجعله يقوم مقام التوقيع الخطي التقليدي في إثبات التصرفات والمعاملات الإلكترونية.

وفي نفس السياق فقد اتجهت محكمة النقض المغربية نحو تأكيد حجية المراسلات الإلكترونية في الإثبات متى ثبت صدورها عن صاحبها، انسجاماً مع مقتضيات القانون رقم 53.05 المتعلق بالتبادل الإلكتروني للمعطيات القانونية. 231

وتعتبر درجات التوقيع الإلكتروني أبرز الضمانات الحمائية في المعاملات الإلكترونية. فمن خلال المادة 4 من قانون 43.20 المتعلق بخدمات الثقة في المعاملات الإلكترونية 232 نجد أن التوقيع الإلكتروني إما يكون بسيطاً أو مؤهلاً أو متقدماً، كما أنه اشترط في كل توقيع ليعتد به مجموعة من الشروط 233 من قبيل أن يكون خاصاً بالموقع نفسه بشكل يسمح بتحديد هويته، مما يتيح اكتشاف أي تغيير يطرأ على المعطيات الموقع عليها إلكترونياً.

كما أن خدمة حفظ التوقيعات المؤهلة لا تقدم إلا من طرف مقدمي خدمات الثقة كجهة رسمية عهد إليها بالقيام بهذه المهمة وفقاً للقانون.

2- تقنية التشفير

يعد التشفير أحد التقنيات الحديثة التي تسهم في حماية المعطيات الخصوصية للأفراد، ذلك أن هذا النظام هو عبارة عن خدمات تهدف إلى تغيير البيانات أو الإشارات الواضحة إلى بيانات أو إشارات غير مفهومة من الغير بفضل برامج ومعدات مخصصة لهذا الغرض. 234

وفي هذا الإطار، عمل المشرع المغربي على تأطير وسائل التشفير باعتبارها من الوسائل الوقائية الأساسية لحماية الأنظمة المعلوماتية، حيث تتمثل هذه الوسائل في المعدات أو البرمجيات المصممة أو المعدة لتحويل المعطيات الإلكترونية أو أي معلومات أخرى، بهدف ضمان سلامة تبادل المعطيات المشفرة بطريقة إلكترونية أو تخزينها 235 ونظراً لما تكتسبه هذه الوسائل من أهمية بالغة ارتباطاً بحماية الأمن المعلوماتي والدفاع الوطني، ألزم المشرع كل من يرغب في استيرادها أو استعمالها بالخضوع لتصريح مسبق لدى السلطة الوطنية المختصة، مع تنظيم كيفية الإدلاء بهذا التصريح وتسليم الترخيص بموجب نص تنظيمي. 236

ويبرز من خلال هذا التنظيم حرص المشرع المغربي على إخضاع خدمات التشفير وتحليل الشفرات لنظام رقابي دقيق، بما يحقق التوازن بين متطلبات حماية المعطيات الشخصية والأمن السيبراني من جهة، ومتطلبات الأمن الداخلي والدفاع الوطني من جهة أخرى. لذلك، اشترط أن يتضمن التصريح جميع البيانات التي تمكن من التعرف على صاحب الترخيص ورقمه وتاريخ الحصول عليه ومدة صلاحيته، إضافة إلى تحديد الخدمات والوسائل موضوع الترخيص 237، وهو ما يعكس رغبة المشرع في الحد من أي استعمال غير مشروع أو غير مراقب لهذه الوسائل الحساسة.

كما قيد المشرع إجراءات التصريح بأجال محددة، إذ أوجب إيداع التصريح داخل أجل ثلاثين يوماً قبل إنجاز العملية المراد تنفيذها، مع منح وصل مؤقت إلى حين الحصول على الترخيص النهائي، فضلاً عن إلزام المعني بالأمر بإشعار السلطة الوطنية بكل تغيير يطرأ داخل أجل ثمانية أيام من وقوعه 238. وإلى جانب ذلك، حددت المادة 48 البيانات الواجب تضمينها في التصريح، كما

231 قرار محكمة النقض عدد 83 صادر في 8 فبراير 2023 في الملف التجاري عدد 1717/3/1/2021.

232 ظهير شريف رقم 1.20.100 صادر في 16 جمادى الأولى 1442 (31 دجنبر 2020) القاضي بتنفيذ القانون رقم 43.20 المتعلق بخدمات الثقة بشأن المعاملات الإلكترونية جريدة رسمية عدد 6051 في 27 جمادى الأولى 1442 الموافق لـ (11 يناير 2021) ص 271.

233 المادة 5 من قانون 43.20 - أن يكون خاصاً بصاحب التوقيع / أن يسمح بتحديد هوية الموقع / أن يتم إنشاؤه بواسطة معطيات إنشاء التوقيع الإلكتروني التي يمكن أن يستعملها صاحب التوقيع تحت مراقبته بصفة حصرية، وبدرجة عالية من الثقة تحدد من قبل السلطة.

234 Loi n 90-1170 du 29/12/1990 sur le réglementation de la télécommunication 7.0 de la république française n303 du 30/12/1990.

235 المادة 45 من قانون 43.20 المتعلق بخدمات الثقة في المعاملات الإلكترونية.

236 المادة 46 من قانون 43.20 المتعلق بخدمات الثقة في المعاملات الإلكترونية.

237 المادة 48 من قانون 43.20 المتعلق بخدمات الثقة في المعاملات الإلكترونية.

238 المادة 47 من قانون 43.20.

تم تحديد مدة الترخيص في خمس سنوات كحد أقصى، مع إمكانية توقيفه مؤقتا لمدة ثلاثة أشهر 239، شريطة إشعار السلطات المختصة بذلك داخل أجل ثمانية أيام.

وفي المقابل، منح المشرع للإدارة إمكانية سحب الترخيص بصفة نهائية كلما أخل صاحبه بالشروط القانونية المؤطرة لهذا المجال، ويتعلق الأمر خاصة بحالة الإدلاء ببيانات غير صحيحة للحصول على الترخيص، أو مخالفة أحكام القانون، أو التوقف عن النشاط المرخص له 240. ويقصد بالتوقف هنا تجاوز مدة التعليق المؤقت المحددة في ثلاثة أشهر دون استئناف النشاط، الأمر الذي يبرر سحب الترخيص حفاظا على الأمن السبراني وضمانا لسلامة البنية الرقمية الوطنية.

ثانيا: دور الذكاء الاصطناعي في حماية المعطيات الشخصية

إن الذكاء الاصطناعي كتقنية من التقنيات الحديثة هو سلاح ذو حدين ولا يمكن الجزم بإيجابياته أو سلبياته على الأنظمة المستخدمة بواسطتهما، ونفس الشيء ما يتعلق بحماية المعطيات الشخصية وعليه سنبرز هذه الإردواجية في نقطتين

1- الذكاء الاصطناعي والحفاظ على الخصوصية

كما سبق الذكر فإنه رغم ما يوفره الذكاء الاصطناعي من إمكانيات تقنية متقدمة لتحسين جودة الحياة وتيسير الخدمات، فإنه في المقابل يساهم في تعميق مخاطر انتهاك المعطيات الشخصية. فقد أدى الاعتماد المتزايد على الكاميرات الذكية، والهواتف المحمولة، والأنظمة المتصلة بالإنترنت إلى تضخم عمليات جمع البيانات وتحليلها، بما يسمح بمراقبة سلوك الأفراد وتتبع تحركاتهم بشكل دقيق، وهو ما يحد من المجال الخاص ويؤثر على الحريات الفردية. كما أن اشتغال أنظمة الذكاء الاصطناعي على كميات ضخمة من البيانات (Big Data) يزيد من احتمالات تسريب المعلومات أو الوصول غير المصرح به إليها، خاصة عندما تكون هذه البيانات حساسة مثل المعطيات الصحية أو المالية، مما يرفع من مخاطر سرقة الهوية أو إساءة الاستخدام.

ومن جهة أخرى، يفاقم الطابع السحابي لتخزين بيانات ونماذج الذكاء الاصطناعي من التهديدات السبرانية، حيث تصبح هذه الأنظمة عرضة للاختراق وسرقة الخوارزميات أو التلاعب بنتائجها، خصوصا في التطبيقات ذات الحساسية العالية مثل الأنظمة الصحية أو القيادة الذاتية. كما أن وجود العنصر البشري داخل منظومة المعالجة قد يشكل تهديدا إضافيا من خلال سوء الاستخدام أو التسريب غير المقصود للبيانات. ويزداد هذا الوضع تعقيدا بسبب الطبيعة "الصندوق الأسود" لبعض نماذج الذكاء الاصطناعي، التي تفتقر إلى الشفافية وقابلية التفسير، مما يجعل المستخدم غير قادر على معرفة كيفية معالجة بياناته أو تتبع مسارها. وبالتالي، فإن توسع الذكاء الاصطناعي يطرح إشكالية دقيقة تتمثل في التوازن بين التطور التقني وحماية الخصوصية الرقمية، في ظل الحاجة المتزايدة إلى كميات ضخمة من البيانات لضمان فعالية هذه الأنظمة.

2- الذكاء الاصطناعي وتعزيز الخصوصية

تساهم تقنيات الذكاء الاصطناعي الحديثة في تطوير آليات متقدمة لحماية المعطيات الشخصية والحد من مخاطر انتهاك الخصوصية، من خلال اعتماد مقاربات تقنية تهدف إلى تأمين دورة حياة البيانات بكامل مراحلها، بدءا من جمعها وتخزينها إلى معالجتها واستعمالها. ومن بين أبرز هذه الآليات نجد الخصوصية التفاضلية التي تسمح بتحليل البيانات بشكل إحصائي دون الكشف عن هوية الأفراد، مما يضمن تحقيق الاستفادة من المعطيات مع الحفاظ على سرية المعلومات الشخصية. 241 كما يعد التعلم الفيدرالي (التعلم الموحد) من أهم الابتكارات في هذا المجال، إذ يتيح تدريب نماذج الذكاء الاصطناعي على أجهزة متعددة دون الحاجة إلى نقل البيانات الأولية إلى خوادم مركزية، حيث يتم الاكتفاء بمشاركة التحديثات أو التدرجات فقط، وهو ما يقلل بشكل كبير من مخاطر تسريب البيانات أو إساءة استخدامها، خاصة في قطاعات حساسة مثل الصحة والمالية. 242

239 المادة 49 من نفس القانون.

240 المادة 50 من نفس القانون.

241 Palle R.R and Kathala K.C.R 2024, Privacy-preserving AI information security po47-61 Berkeley CA Après.

242 Bonawitz K 2019 Towards federated learning at scale style m design ar XIV preprint ar XIV 190201046.

إلى جانب ذلك، يبرز التشفير المتماثل والحوسبة الآمنة متعددة الأطراف كآليات فعالة تمكن من إجراء عمليات حسابية على بيانات مشفرة دون كشف محتواها، مما يعزز سرية المعطيات أثناء معالجتها داخل أنظمة الذكاء الاصطناعي. ورغم الفوائد الكبيرة لهذه التقنيات في حماية الخصوصية، فإنها تطرح في المقابل تحديات تتعلق بارتفاع الكلفة الحسابية وتعقيد النماذج وصعوبة تفسيرها، خصوصا في الأنظمة المعقدة التي تعتمد على عدة أطراف أو أجهزة. ومع ذلك، فإن هذه المقاربات تمثل تحولا نوعيا في دور الذكاء الاصطناعي، حيث لم يعد مجرد مصدر للتهديدات المحتملة للخصوصية، بل أصبح أداة مركزية في حمايتها وتعزيز الأمن الرقمي، شريطة تحقيق توازن بين الفعالية التقنية ومتطلبات الشفافية والقبالية للتفسير 243.

خاتمة:

أضحى الحق في الخصوصية الرقمية من أبرز الحقوق الأساسية التي تواجه تحديات متزايدة في ظل التطور التكنولوجي المتسارع وتنامي التهديدات السيبرانية، الأمر الذي فرض على التشريعات الوطنية، ومن بينها التشريع المغربي، ضرورة إرساء منظومة قانونية وتقنية متكاملة لحماية المعطيات ذات الطابع الشخصي وتأمين الفضاء الرقمي. وقد عمل المشرع المغربي من خلال القانون رقم 09.08 والقانون رقم 05.20 المتعلق بالأمن السيبراني، إلى جانب آليات التشفير والرقابة المؤسسية، على وضع إطار قانوني يهدف إلى تحقيق التوازن بين متطلبات الأمن المعلوماتي وضمان الحقوق والحريات الفردية.

ورغم أهمية هذه المقترضات، فإن الواقع العملي يكشف عن استمرار مجموعة من الإكراهات المرتبطة بالتطور المستمر للجرائم السيبرانية، وضعف الوعي الرقمي، وصعوبة مواكبة النصوص القانونية للتحويلات التقنية المتسارعة، مما يجعل حماية الخصوصية الرقمية رهينة بتعزيز التنسيق بين المقاربة القانونية والتقنية والمؤسسية. ومن ثم، فإن تحقيق حماية فعالة للمعطيات الشخصية لا يقتصر فقط على سن القوانين، بل يتطلب أيضا تطوير آليات الوقاية الرقمية وتحديث البنيات التقنية وتعزيز الثقافة السيبرانية داخل المجتمع. وعليه نقترح التوصيات التالية:

- تعزيز الترسانة القانونية المتعلقة بحماية المعطيات الشخصية والأمن السيبراني بما يواكب التطورات التكنولوجية الحديثة والتهديدات الرقمية المستجدة.
- مراجعة بعض مقتضيات القانون رقم 09.08 بما ينسجم مع المعايير الدولية الحديثة لحماية البيانات، خاصة في ظل تنامي استعمال تقنيات الذكاء الاصطناعي والحوسبة السحابية.
- تقوية دور اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي من خلال توسيع صلاحياتها الرقابية والتحسيسية وتوفير الموارد التقنية والبشرية الكفيلة بأداء مهامها بفعالية.
- دعم استعمال تقنيات التشفير والتوقيع الإلكتروني داخل الإدارات والمؤسسات العمومية والخاصة لتعزيز أمن المعاملات الرقمية والحد من مخاطر الاختراق وتسريب المعطيات.
- تكثيف برامج التوعية والتحسيس بالأمن الرقمي لفائدة الأفراد والمؤسسات، ونشر الثقافة القانونية المرتبطة بحماية الحياة الخاصة والخصوصية الرقمية.
- تعزيز التعاون الدولي والإقليمي في مجال مكافحة الجرائم السيبرانية وتبادل الخبرات التقنية والمعلوماتية لمواجهة التهديدات العابرة للحدود.
- تشجيع البحث العلمي الأكاديمي في مجالات الأمن السيبراني وحماية المعطيات الشخصية، وربط الجامعة بالتطورات الرقمية والقانونية الحديثة.

❖ المراجع المعتمدة

أولا: الكتب

243 رانيا عبد المنعم عبد الحميد، الأمن السيبراني وحماية الحق في الخصوصية الرقمية "الضوابط والتحديات" ص 2025 ص 233.

- خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، الطبعة الأولى، دار الجامعة الجديدة، الإسكندرية، 2008.
- خالد عثمان، مكافحة الجريمة المعلوماتية في ضوء التشريع المغربي، مجلة العلوم الجنائية، العدد الأول، 2014.
- رانيا عبد المنعم عبد الحميد، "الأمن السيبراني وحماية الحق في الخصوصية الرقمية: الضوابط والتحديات"، 2025.
- ثانيا: الرسائل والأطاريح الجامعية
- إيمان التيس، التجارة الإلكترونية وضوابط حماية المستهلك في المغرب، أطروحة لنيل الدكتوراه في القانون الخاص، جامعة المولى إسماعيل، مكناس، 2014-2015.
- حسن الحافظي، الحماية القانونية للمعطيات ذات الطابع الشخصي بين التشريع الوطني والاتفاقيات الدولية، رسالة لنيل الماستر في القانون الخاص، جامعة المولى إسماعيل، مكناس، 2017-2018.
- سكيمة بن الشيخ، الأمن القانوني المعلوماتي، رسالة ماستر في القانون الخاص، جامعة القاضي عياض، مراكش، 2014-2015.
- عبد المجيد كوزي، الحماية القانونية للبيانات والمعطيات ذات الطابع الشخصي، أطروحة لنيل الدكتوراه في القانون الخاص، جامعة محمد بن عبد الله، فاس، 2014-2015.
- عدنان الزرزوري، مكافحة الإرهاب المعلوماتي، رسالة لنيل الماستر في القانون الخاص، جامعة المولى إسماعيل، مكناس، 2017-2018.
- علي أرحال، حماية المعطيات الشخصية بالمغرب: دراسة تحليلية ومقارنة، رسالة لنيل الماستر في القانون الخاص، جامعة محمد الخامس، الرباط، 2018-2019.
- لحسن عالي، حماية المعطيات الشخصية بين القانوني والمؤسسي، رسالة لنيل دبلوم الماستر في القانون الخاص، جامعة المولى إسماعيل، مكناس، 2021-2022.
- ثالثا: المقالات والدوريات
- لبنى الوزاني، "الرقابة القضائية على أعمال اللجنة الوطنية لحماية المعطيات الشخصية"، مجلة القضاء، محكمة الاستئناف بالدار البيضاء، العدد 2، 2018.
- محمد جوهر، خصوصيات زجر الإجرام المعلوماتي، المجلة المغربية للقانون والاقتصاد والتدبير، العدد 52، 2006.
- رابعا: القوانين والظواهر والمراسيم
- ظهير شريف رقم 1.03.140 صادر في 26 ربيع الأول 1424 (28 ماي 2003) بتنفيذ القانون رقم 03.03 المتعلق بمكافحة الإرهاب.
- القانون رقم 07.03 المتعلق بالإخلال بسير نظم المعالجة الآلية للمعطيات.
- ظهير شريف رقم 1.09.15 صادر في 18 فبراير 2009 بتنفيذ القانون رقم 09.08 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية عدد 5711 بتاريخ 23 فبراير 2009.
- القانون رقم 05.20 المتعلق بالأمن السيبراني.
- ظهير شريف رقم 1.20.100 صادر في 16 جمادى الأولى 1442 (31 دجنبر 2020) بتنفيذ القانون رقم 43.20 المتعلق بخدمات الثقة بشأن المعاملات الإلكترونية، الجريدة الرسمية عدد 6051 بتاريخ 11 يناير 2021.
- القانون رقم 53.05 المتعلق بالتبادل الإلكتروني للمعطيات القانونية.
- مرسوم رقم 2.11.508 صادر في 22 شوال 1432 (21 شتنبر 2011) بإحداث اللجنة الاستراتيجية لأمن نظم المعلومات، الجريدة الرسمية عدد 5987 بتاريخ 25 شتنبر 2011.
- مرسوم رقم 2.10.84 صادر في 21 ربيع الثاني 1431 (7 أبريل 2010) بتحديد اختصاصات المديريات المركزية التابعة للمديرية العامة للأمن الوطني.
- مرسوم رقم 2.20.293 بتاريخ 24 مارس 2020 المتعلق بإعلان حالة الطوارئ الصحية.
- منشور رقم 3-14 بتطبيق التوجيهات الوطنية لأمن نظم المعلومات، صادر في 10 مارس 2014.
- خامسا: التقارير

• تقرير حماية المعطيات ذات الطابع الشخصي في إطار قطاع الأمن بالمغرب، مركز دراسات حقوق الإنسان والديمقراطية.

سادسا: القرارات القضائية

• قرار محكمة النقض عدد 83 صادر بتاريخ 8 فبراير 2023 في الملف التجاري عدد 2021/1/3/1717.

سابعا: المراجع الأجنبية

- Loi n° 90-1170 du 29 décembre 1990 sur la réglementation des télécommunications, République française.
- Bonawitz K., "Towards Federated Learning at Scale: System Design", *arXiv preprint*, 2019.
- Palle R.R & Kathala K.C.R., "Privacy-Preserving AI Information Security", Berkeley CA Press, 2024.