المملكة المغربية

جامعة عبد المالك السعدي

كلية العلوم القانونية والاقتصادية

والاجتماعية بتطوان

رسالة لنيل شهادة الماستر

تخصص: ماستر قانون الرقمنة والمعاملات الالكترونية، الفوج الأول

القوانين الرقمية لمراقبة وحماية التطبيقات الإلكترونية للمؤسسات العمومية ومستخدميها كوريا الجنوبية واليابان نموذجا

إعداد الطالبة الباحثة

مريم مشبال

تحت إشراف الدكتور

ذ. هشام العزوزي الإدريسي

أعضاء لجنة المناقشة

ذ. هشام العزوزي الإدريسي : أستاذ باحث بكلية العلوم القانونية والاقتصادية والاجتماعية بتطوان...رئيسا ومشرفا

ذ. محمد القواق : أستاذ باحث بكلية العلوم القانونية والاقتصادية والاجتماعية بتطوان.....عضوا

ذ. مصطفى ميمون : أستاذ باحث بكلية العلوم القانونية والاقتصادية والاجتماعية بتطوان .....عضوا

السنة الجامعية: 2024/ 2025

﴿... سُبْحَانَكَ لَا عِلْمَ لَنَا إِلَّا مَا عَلَّمْتَنَا إِنَّكَ أَنتَ الْعَلِيمُ الْحَكِيمُ﴾

الآية 32 من سورة البقرة

إهداء

اللهم بارك لي في أمي وارحم لي يا ربي أبي، إلى والدي من في الأرض ومن في السماء،

يطيب لي أن أتقدم وأن أهدي لكما ثمرة جهدي العلمي المتواضع، فنجاحي نجاحكما،

ولا حول ولا قوة إلا بالله العليم، والحمد لله دائما وأبدا،

فلا قول أو عمل يوفي حقيكما علي،

إلى كل فرد في عائلتي وأصدقائي وكل شخص، من ساهم من قريب أو من بعيد

ولو بالكلمة الطيبة، أهدي لكم الثمرة العلمية وشرفها حضوريا وغيابيا.

مع طول مسار البحث العلمي، ومن أول الطريق بنجاحاته وإخفاقاته، بمعاناته الحلوة تارة والمرة تارة أخرى، أهدي ثمرة جهدي المولود العلمي الذي بين أيديكم،

لكل طالب علم، فاحفظ عهد آداب العلم، قبل قطف العلم.

تجلي نور العلم في عقول وقلوب العالمين باقتدار

تجلو به سحائب الشكوك بعد طول اجتهاد وانتظار

قد كان ولازال وسيكون اقتطاف ثمر المعرفة والعلم

بعد طفح مر العلقم العرمرم بفم ونفوس طلبة العلم الكرام

طلب العلم جهد يضني البدن ويوقد عزائم الروح والنفس

لعل به ترتقي عزائم الأمة لصالح الأعمال وما هو نفيس

شكر وتقدير

أتقدم بجزيل الشكر إلى أستاذي هشام العزوزي الإدريسي،

الذي لطالما شجع فينا التفاني في العمل بالتجديد والابتكار دائما،

قدوتي في حب الترجمة والتطلع للأحسن،

كما يسعدني أن أتقدم بالشكر الجزيل للأساتذة الكرام الذين ساهموا

في إخراج الرسالة إلى مسار ومضمار الأطروحات العلمية.

المقدمة

تعد استراتيجية المغرب الرقمي 2030[1] خطة تهدف إلى رقمنة الخدمات العامة وتنمية الاقتصاد الرقمي ودعم الشركات الناشئة وتعزيز الخدمات في البلاد، وتشمل الاستراتيجية تحسين مؤشرات الخدمات وتطوير التصدير الرقمي والإنترنت وتعزيز السيادة الرقمية واللحاق بركب الذكاء الاصطناعي، علاوة على أن الأمن السيبراني يعد أساس الحماية للتقنيات، ويشير معناه إلى حماية أنظمة الحاسوب والشبكات والمعلومات الرقمية من الوصول غير المصرح به، وتسريب البيانات، والهجمات الإلكترونية، وغيرها من التهديدات[2]، وخاصة عندما نصطدم بمبدأ الخصوصية تبقى قوانين حماية البيانات الشخصية طوق النجاة للأفراد، إن لم تكن كذلك فللدفاع عن المكتسبات والحقوق، عند وقوع تسريب أو انتهاك للبيانات.

وضعت الرؤية المتبصرة لصاحب الجلالة الملك محمد السادس، نصره الله التحول الرقمي في صلب الأولويات الوطنية، وقد أكد ذلك في عدة مناسبات بأنه: " *... يتعين تعميم الإدارة الإلكترونية بطريقة مندمجة، تتيح الولوج المشترك للمعلومات بين مختلف القطاعات والمرافق، فتوظيف التكنولوجيات الحديثة، يساهم في تسهيل حصول المواطن، على الخدمات، في أقرب الآجال، دون الحاجة إلى كثرة التنقل والاحتكاك بالإدارة، الذي يعد السبب الرئيسي لانتشار ظاهرة الرشوة، واستغلال النفوذ* "[3].

هذه الرؤية الملكية التي تم تكريسها من خلال النموذج التنموي الجديد، الذي جعل من الرقمنة رافعة حقيقية للتغيير والتنمية، وفي نسق هذا النموذج اعتمدت الوزارة المنتدبة لدى رئيس الحكومة المكلفة بالانتقال الرقمي وإصلاح الإدارة مقاربة تشاركية تقوم على الانصات، واللقاءات التشاورية في مختلف جهات المملكة، والبناء المشترك من خلال إشراك المجتمع المدني والقطاعين العام والخاص، لصياغة استراتيجية المغرب الرقمي، وتهدف استراتيجية المغرب الرقمي 2030 إلى "جعل المغرب قطبا رقميا لتسريع التنمية الاجتماعية والاقتصادية للمملكة"، وكشفت الحكومة عن الاستراتيجية المعنية في نشاط رسمي عقدته الأربعاء 25 شتنبر عام 2024، ترتكز على محورين استراتيجيين

---

[1] استراتيجية المغرب الرقمي 2030، على موقع المملكة المغربية maroc.ma: https://h1.nu/12rdF ، (2025/07/05) على الساعة 18:15 مساءا.

[2] هند الإدريسي، الأمن السيبراني في المغرب: بين الإنجازات والتحديات، 2024/04/15، المعهد المغربي لتحليل الدراسات: https://mipa.institute/?p=11681&lang=ar ، تاريخ الاطلاع: 2025/07/07، على الساعة 46:03 صباحا.

[3] مقتطفات من نص الخطاب الملكي السامي الذي ألقاه صاحب الجلالة الملك محمد السادس في افتتاح الدورة الأولى من السنة التشريعية الأولى من الولاية التشريعية العاشرة بالرباط بتاريخ 14 أكتوبر 2016.

هما: الأول يتعلق ب" رقمنة الخدمات العمومية"، ويتعلق الثاني ب" بث دينامية قوية في الاقتصاد الرقمي"، وفيما يخص محفزات الاستراتيجية فحددت في ثلاثة، هي المواهب الرقمية والخدمات السحابية والاتصالات، تتخللهم أحدث الابتكارات التكنولوجية المتمثلة في الرافعات العرضانية التي تجسدت في عنصرين هما الذكاء الاصطناعي والاستخدام الرقمي الشامل، وقد تأسست محاور الاستراتيجية ومحفزاتها ورافعاتها على رؤية لكل واحد منها وأهداف إجرائية وتدابير عملية.[4]

على نفس النسق، تهدف الاستراتيجية على الخصوص، إلى رقمنة الخدمات العمومية وتجويدها وتقريبها من المواطنين، وتقليص آجال المعالجة لخدمة المواطن، كما تروم الاستراتيجية أيضا تنمية الاقتصاد الرقمي للمغرب من أجل خلق مناصب شغل وتكوين الشباب المغربي في مجال الرقمنة.

إضافة إلى أن المملكة وقعت العديد من الاتفاقيات مع مجموعة من الشركات متعددة الجنسيات الرائدة في المجال الرقمي والبحث والتطوير والابتكار، من أجل تسريع التحول الرقمي وتعزيز الرأسمال البشري المحلي، كما تتطلع إلى تطوير الخدمات السحابية بتقديم خدمات حوسبة سحابية متنوعة تحترم السيادة الوطنية، تستجيب للمعايير الدولية وتلبي احتياجات القطاعين العام والخاص، وتغطية مختلف التراب الوطني بشبكة الإنترنيت، وتحسين جودة الاتصال للاستخدامات الأساسية، بهدف مواصلة توسيع هذه التغطية في المناطق القروية، لا سيما الجيل الخامس والألياف البصرية.[5]

في الواقع، يمكن استخدام تقنيات الحكومة الإلكترونية بسرعة وفقا للتغيرات في السياسة أو المجتمع، ومع تغيرها ليس من السهل التمييز بين هذه التقنيات وتنظيمها، تقوم شركة Gartner وهي شركة استشارية تقوم بتحليل اتجاهات التكنولوجيا في الحكومة الإلكترونية بشكل مستمر، لتحقيق حكومة المنصة الرقمية، بالإضافة إلى ذلك، يتم عرض اتجاهات تكنولوجيا المعلومات الأساسية[6] التي يجب على مديري تكنولوجيا المعلومات الذين يستخدمون هذه المنصات في القطاع العام، فقد توقع *بيل فينيرتي* محلل بشركة غارتنر بأنه: "*بحلول عام 2023، فإن أكثر من 80% من التطبيقات*

---

[4] العرض الرسمي للإستراتيجية الوطنية المغرب الرقمي 2030 (التغطية الكاملة)، Transition Numérique et Réforme de l'Administration (Ministère_TNRA)، على تطبيق يوتيوب YoutYoub: https://www.youtube.com/watch?v=gma9OzisnxA، تم الاطلاع بتاريخ 2025/07/06، على الساعة 04:21 مساء.

[5] استراتيجية المغرب الرقمي 2030، مرجع سابق.

[6] بارك هيون سون، أعلنت شركة جارتنر عن أهم 12 اتجاها استراتيجيا للتكنولوجيا لعام 2022، تاريخ النشر: 2021/10/22، على موقع NextDaily، باللغة الكورية: https://www.nextdaily.co.kr/news/articleView.html?idxno=200342 ، تاريخ الاطلاع: 2025/07/06، على الساعة 05:20 مساء.

الرقمية الحكومية التي لا تعتمد على منصة تكنولوجية سوف تفشل في تحقيق الأهداف" [7]، كما أنه لابد من حماية التقنيات من الهجمات السيبرانية، فقد قال *إيرل بيركنز* المدير التنفيذي لشركة غارتنر: *" ...، إن الفكرة الأساسية يجب أن تترسخ ما لم يكن لديك أساس متين للأمن السيبراني لمعالجة التهديدات الأكثر شيوعا ويمكن التنبؤ بها، فلن تكون قادرا على معالجة تهديدات الأمن السيبراني الأكثر تعقيدا وتحديا، والتي تظهر اليوم من خلال الإنفاق على التكنولوجيا، وتغيير العمليات، والتغيير التنظيمي، أو الاستعانة بمصادر خارجية*[8]".

يركز المغرب على "توفير القيمة" عبر خلق مناصب الشغل، وقبله تحقيق "التغيير الثقافي" امتدادا من العالم المحيط بنا عبر تطوير أنماط إنتاجية واستهلاكية جديدة، ويظهر جليا بنص الخطاب الملكي لصاحب الجلالة الملك محمد السادس الذي يقول: *" فالتكنولوجيا الرقمية تشكل بالفعل، تحولا بنيويا في مقاربتنا للعالم الذي يحيط بنا، إذ تسمح بتطوير أنماط إنتاجية واستهلاكية جديدة، من شأنها أن تخلق المزيد من مناصب الشغل"* ،[9] بمعنى أن توفير القيمة متمثل في خلق مناصب الشغل.

في المقابل، نظرا لكون وجود اختلافات بين الخبراء الكوريين في وجهات النظر المختلفة حول التقنيات الأساسية، ورغم الاهتمام الفعلي لكن يبقى هذا المجال ليس منظما بشكل شامل لتحليل هاته التوجهات، بداية مع التحول الرقمي، فقد تم ذكر التكنولوجيا بشكل شائع في تعريف التحول الرقمي منذ منتصف عام 2010 بالقطاع الخاص، و تطور الاستخدام النشط بتطبيقه في القطاع العام، وقبل ذلك فقد تم تحقيق الغرض الرئيسي من خلال التمييز بين "توفير القيمة" و"التغيير الثقافي"، وتم تحقيق "تغييرات جديدة في الأنظمة الاجتماعية والصناعية"[10].

---

[7] Finnerty, B. "A Digital Government Technology Platform Is Essential to Government Transformation", *Gartner*, Retrieved from: https://www.gartner.com/en/doc/344044-a-digital-government-technology-platform-is-essential-to-government-transformation , accessed 06 june 2025 – 19 :40am.

[8] Perkins, E. Articles by Earl Perkins, *Gartner* : https://muckrack.com/earl-perkins/articles, accessed 06 june 2025 – 19 :39am.

[9] جلالة الملك يوجه رسالة إلى المشاركين في أشغال اجتماع التجمع الإفريقي لوزراء المالية ومحافظي البنوك المركزية للدول الأفريقية، الأعضاء في البنك وصندوق النقد الدوليين 5 يوليوز 2022.

[10] سون سونغ هيون وآخرون، تقرير حول مشكلة توحيد معايير المنصات الرقمية الحكومية، جمعية تكنولوجيا المعلومات والاتصالات الكورية، نظام إدارة أداء البحث والتطوير لمعايير تكنولوجيا المعلومات والاتصالات"، تاريخ النشر 2023، باللغة الكورية، على الرابط التالي:
file:///C:/Users/pc/Downloads/%EB%94%94%EC%A7%80%ED%84%B8%ED%94%8C%EB%9E%AB%ED%8F%BC%EC%A0%95%EB%B6%80%ED%91%9C%EC%A4%80%ED%99%94%EC%9D%B4

لقد برز التحول الرقمي كقوة مؤثرة في مشهد الخدمات الحكومية سريع التطور بالمغرب، حيث أحدث ظهور الخدمات العامة الرقمية اتجاها مختلفا في الطريقة التي يتفاعل بها المواطنون مع الحكومة، وتبسيط العمليات، وتحسين إمكانية الوصول، وتحسين الكفاءة العامة.

تمتد الخطط والاستراتيجيات بالترتيب التالي: الخطة الخمسية 1999-2003 لتطوير قطاع الاتصالات والتكنولوجية الحديثة و الخطة الاستراتيجية للإدارة الإلكترونية "*إدارتي*" 2003-2007، مخطط المغرب الرقمي 2005-2010(e-Maroc) ، استراتيجية المغرب الرقمي 2009-2013، و مخطط المغرب الرقمي 2020، توجهات التنمية الرقمية بالمغرب في عام 2025، وجاءت استراتيجية المغرب الرقمي 2030 كتتويج لهذه المخططات والاستراتيجيات، الذي عقد لها نشاط رسمي بتاريخ الأربعاء 25 شتنبر عام 2024 بالعاصمة الإدارية - الرباط.[11]

اعتمد المغرب نصوصا قانونية تؤطر الجوانب الأساسية للتكنولوجيات الرقمية، إلا أن كوريا الجنوبية تعمقت بشكل كبير من حيث التقنيات وتأطيرها القانوني، على أساس ما سابق، يهدف القانون رقم 20-43 المتعلق بخدمات الثقة بشأن المعاملات الإلكترونية إلى تحديد النظام المطبق على كل من خدمات الثقة بشأن المعاملات الإلكترونية، ووسائل وخدمات التشفير وتحليل الشفرات، والعمليات المنجزة من قبل مقدمي خدمات الثقة والقواعد الواجب التقيد بها من لدن هؤلاء ومن لدن أصحاب الشهادات الإلكترونية، كما يحدد كذلك هذا القانون اختصاصات السلطة الوطنية لخدمات الثقة بشأن المعاملات الإلكترونية[12]، يمكن القول بأن هذا القانون الحالي التأطير العام للبيانات بالمغرب.

بالمقابل فيما يتعلق بنظام إدارة البيانات المتكاملة بكوريا الجنوبية، تنص المادة 23 في قانون توفير واستخدام البيانات العامة على توحيد البيانات العامة، إذ تم وضع الأساس بإنشاء أو الحصول على "المبادئ التوجيهية لتوحيد قواعد البيانات للمؤسسات العامة"، من قبل المؤسسات العامة، لأنها تحدد التفاصيل اللازمة لذلك.[13]

%EC%8A%88%EB%B3%B4%EA%B3%A0%EC%84%9C%20(2).pdf، تاريخ الاضطلاع: 2025/07/06، على الساعة 03:29 صباحا.

[11] حميد بحكاك، المغرب والتحول الرقمي، الإطار التشريعي والمؤسساتي والاستراتيجي، تاريخ النشر: 20 سبتمبر 2024 - 13:00، موقع حزب العدالة والتنمية: https://n9.cl/0atfwz ، تاريخ الاطلاع: 2025/07/06، على الساعة 41:21 مساء.

[12] القانون رقم 20-43 المتعلق بخدمات الثقة بشأن المعاملات الإلكترونية، على موقع المديرية العامة لأمن نظم المعلومات: https://www.dgssi.gov.ma/ar/alqanwn-rqm-20-43-almtlq-bkhdmat-althqt-bshan-almamlat-alalktrwnyt ، تاريخ الاطلاع: 2025/07/06، على الساعة 21:51 مساء.

[13] سون سونغ هيون وآخرون، مرجع سابق.

من جهة أخرى رغم اعتماد المغرب قانون للأمن السيبراني عام 2020، بحيث تكون مؤهلة لتقنيات الذكاء الاصطناعي، إلا أنه ليس هناك إلى يومنا هذا قانون مؤطر للذكاء الاصطناعي بالمغرب، على عكس كوريا الجنوبية إذ تم سن قانون الإطار بشأن الذكاء الاصطناعي كمشروع قانون، باعتباره امتدادا لقانون الإطار بشأن تعزيز المعلومات والاتصالات (الذي صدر في عام 1995)، وهو السلف لقانون الإطار بشأن المعلوماتية الوطنية (الذي تمت مراجعته بشكل شامل في عام 2009)، وقانون الإطار بشأن المعلومات والاتصالات الذكية، الذي صدر في عام 2020.

بعبارة أخرى، وكما يمكن رؤيته مع استخدام المصطلحات القانونية مثل مجتمع الذكاء الاصطناعي وأخلاقياته، يبدو من المحتم أن تكون هناك قضايا تعديل في القانون لأنه حاول الضفر بتطوير الذكاء الاصطناعي وضمان السلامة في نفس الوقت على المستوى الكلي للمعلوماتية الذكية بكوريا بأكملها، وبطبيعة الحال، فإن الوزارة المختصة هي وزارة العلوم وتكنولوجيا المعلومات والاتصالات، وتبقى وزارة الداخلية والأمن، الوزارة المختصة المسؤولة عن المعلوماتية العامة، مطلوب منها أيضا المشاركة كمحور مركزي عند وضع خطة التنفيذ بموجب قانون الإطار بشأن المعلومات الذكية.[14]

من هذا المنحى، قامت المؤسسات الإدارية والعامة المحلية بتطوير وتوزيع العديد من الأدلة في الماضي للتطبيق الفعال لمفاهيم إمكانية الوصول وراحة المستخدم (UI/UX) عند بناء أنظمة المعلومات العامة لأسباب "المصلحة العامة"، بدءا بالحكومة الإلكترونية على وجه الخصوص، ومن خلال إضفاء الطابع المؤسسي على المعايير وحل فجوة المعلومات تم توضيح أهميته كالتزام قانوني، ومع ذلك، بدلا من تحديد معايير فنية دقيقة، يتم تقديم الإشعارات التنظيمية والمبادئ التوجيهية أو الأدلة لتوفير إمكانية الوصول (الويب وكذلك الهاتف المحمول).[15]

علاوة على ذلك، هناك تشريعات عامة تطبق على الحوسبة السحابية بالمغرب بما في ذلك قانون الأمن السيبراني رقم 20-05 الذي ينظم حماية المعطيات الحساسة، بالإضافة إلى قوانين أخرى تركز على حماية البيانات الشخصية تتمثل في قانون حماية الأشخاص الذاتيين لمعالجة المعطيات ذات الطابع الشخصي08-09[16]، ولا يوجد قانون خاص بالحوسبة السحابية بالمغرب حاليا، على عكس

---

[14] نفس المرجع.

[15] سون سونغ هيون وآخرون، نفس المرجع.

[16] التكنولوجيا السحابية(cloud)، رافعة استعجالية لتسريع التحول الرقمي، رأي المجلس الاقتصادي والاجتماعي والبيئي، إحالة ذاتية رقم 2023/71، المجلس الاقتصادي والاجتماعي والبيئي، على الرابط التالي: https://www.cese.ma/media/2023/10/AvAs71a1-P1.pdf ، تاريخ الاطلاع: 2025/07/06، على الساعة 09-23 مساء.

كوريا الجنوبية، إذ أعلنت وزارة العلوم وتكنولوجيا المعلومات والاتصالات بكوريا عن "الخطة الأساسية الثالثة للحوسبة السحابية (2022-2024) في 6 سبتمبر 2021[17]، بناء على "قانون تعزيز الحوسبة السحابية وحماية المستخدمين (قانون تطوير السحابة/ قانون الحوسبة السحابية)" الصادر في عام 2015، وتهدف هذه الخطة إلى تعزيز القدرة التنافسية في الصناعة السحابية من خلال أولوية استخدام السحابة الخاصة في القطاع العام، والتحول السحابي في صناعة البرمجيات السحابية، والتحول الرقمي لجميع الصناعات، واقترحت تعزيز وإنشاء نظام بيئي سحابي يمكنه دعم البيانات والذكاء الاصطناعي.[18]

باعتبار تكنولوجيا المعلومات الذكية متعلقة بالبيانات قانونيا وتنظيميا والتي تعتمد المرونة، فقد سنت كوريا الجنوبية ما مجموعه 9 قوانين تخضع لسلطة 6 وكالات، بما في ذلك قانون البيانات العامة كقوانين متعلقة بالبيانات، الذي تم سنه وتنقيحه، وكذا قانون صناعة البيانات، (صدر في 19 أكتوبر 2021) بغرض إنشاء أساس لتطوير صناعة البيانات، بما في ذلك خلق قيمة اقتصادية منها.[19]

وآخر تقنية، تتجسد في نموذج الثقة الصفرية، بحيث تدعم وكالة الانترنت والأمن الكورية التحقق منه، كما أن أمن تطوير البرمجيات العامة يقوم على تعزيز قدرات الوقاية من التهديدات السيبرانية المحتملة والاستجابة لها من خلال التشخيص المسبق والقضاء على نقاط ضعف أمن البرامج، والتي تعد السبب الرئيسي لانتهاكات الأمن، منذ مرحلة التطوير، وتقوم وكالة الانترنت والأمن الكورية بتشخيص ثغرات أمن البرمجيات ودعم السياسات للمؤسسات الإدارية والعامة، وبالتالي يرجع الأساس القانوني لذلك وفقا للمادتين 24 و45 من قانون الحكومة الإلكترونية، المعنونة بالمبادئ التوجيهية لبناء وتشغيل أنظمة المعلومات الإدارية ونظم المعلومات للمؤسسات العامة.[20]

يتكون القانون رقم 20-05 المتعلق بالأمن السيبراني بالمغرب، من 53 مادة موزعة على ستة فصول وهي: الفصل الأول: أحكام عامة، الفصل الثاني: إجراءات حماية نظم المعلومات، الفصل

---

[17] الخطة الأساسية الثالثة للحوسبة السحابية (ما بين عامي 2022-2024)، لجنة استراتيجية المعلومات والاتصالات، تاريخ النشر: شهر 9 سنة 2021، باللغة الكورية على الرابط التالي: file:///C:/Users/pc/Downloads/R2109209-1.pdf، تاريخ الاضطلاع: 2025/06/30، على الساعة 00:43 صباحا.

[18] سون سونغ هيون وآخرون، مرجع سابق.

[19] سون سونغ هيون وآخرون، مرجع سابق.

[20] نفس المرجع.

الثالث: حكامة الأمن السيبراني، الفصل الرابع: التكوين والتحسيس والتعاون، الفصل الخامس: معاينة العقوبات والمخالفات، الفصل السادس: أحكام ختامية.

في نفس السياق ينص قانون الأمن السيبراني بالمغرب، على مجموعة من تدابير الأمان ذات الطبيعة التنظيمية والتقنية التي تهدف إلى تعزيز القدرات الوطنية في مجال الأمن السيبراني، وتنسيق جهود الوقاية والحماية من الهجمات والحوادث المتعلقة بالأمن السيبراني.

يحدد هذا القانون كما جاء في المادة الأولى منه، قواعد ومقتضيات الأمن المطبقة على نظم معلومات إدارات الدولة والجماعات الترابية والمؤسسات والمقاولات العمومية وكل شخص اعتباري آخر خاضع للقانون العام؛ وقواعد ومقتضيات الأمن المطبقة على البنيات التحتية ذات الأهمية الحيوية؛ وقواعد ومقتضيات الأمن المطبقة على مستغلي الشبكات العامة للمواصلات ومزودي خدمات الإنترنت ومقدمي خدمات الأمن السيبراني ومقدمي الخدمات الرقمية وناشري منصات الإنترنت؛ والإطار الوطني لحكامة الأمن السيبراني.[21]

في الإطار ذاته فإن إهمال الأمن السيبراني يمكن أن يؤدي إلى أزمة أمنية وطنية، وتحدد الدول الأجنبية المتقدمة الهجمات السيبرانية باعتبارها التهديد الأكثر خطورة وتبذل جهودا لحماية المعلومات والمرافق الوطنية الرئيسية من هجمات القوى التخريبية، على سبيل المثال: أصدرت اليابان "القانون الأساسي للأمن السيبراني" في 12 نوفمبر 2014، والذي ينص على مسؤوليات كل كيان عن الأمن السيبراني، ويثبت هذا الأمر الأهمية المتزايدة للأمن السيبراني ويظهر قدرة الجمعية الوطنية على الاستجابة التشريعية النشطة باليابان.[22]

في المقابل ينحصر الأمن السيبراني بكوريا الجنوبية في القيم الدستورية المتعلقة بالسلامة الوطنية وسلامة المواطنين، وضمان الحقوق الأساسية، وسيادة القانون، والسلم الدولي، بحيث أنه تجسيد لهذه

---

[21] القانون رقم 20-05 المتعلق بالأمن السيبراني، على الموقع الرسمي المديرية العامة لأمن نظم المعلومات: https://www.dgssi.gov.ma/ar/alqanwn-rqm-0520-almtlq-balamn-alsybrany ، تاريخ الاطلاع: 2025/07/06، على الساعة 09:23 مساء.

[22] جونغ تاي جين، "دراسة حول أنظمة الاستجابة للأمن السيبراني في الدول الكبرى"، مجلة قانون وسياسة الأمن السيبراني، المجلد 2 (الجمعية الكورية لقانون وسياسة الأمن السيبراني، ديسمبر 2016)، ص 93، باللغة الكورية، على الرابط التالي: http://www.kcsa2012.or.kr/wp-content/uploads/2019/01/2nd.pdf?ckattempt=1 ، تاريخ الاطلاع: 2025/09/09، على الساعة 15:43 مساء.

القيم،[23] ويمكن القول بأنه استراتيجية استجابة حديثة للأمن الوطني لديهم لحماية الدستور، إذ نشر مكتب الأمن القومي التابع للبيت الأزرق "الاستراتيجية الوطنية للأمن السيبراني" في أبريل 2019، وتتكون "الاستراتيجية الوطنية للأمن السيبراني" من الأهداف والمبادئ الأساسية والمهام الاستراتيجية وخطط التنفيذ، وتتضمن هاته الاستراتيجية مبادئها الأساسية (1) الانسجام بين الحقوق الأساسية للشعب والأمن السيبراني، (2) تطوير الأنشطة الأمنية القائمة على سيادة القانون، و(3) إنشاء نظام للمشاركة والتعاون.

إضافة إلى ذلك، فإن إنشاء "الاستراتيجية الوطنية للأمن السيبراني" مهم للغاية لأنه بمثابة شرط أساسي لإنشاء تشريعات الأمن السيبراني، في حالة كوريا الجنوبية، فإن الأمن السيبراني لديهم مبني على نظام مزدوج حيث ينظم المرسوم الرئاسي "لوائح إدارة الأمن السيبراني الوطنية" القطاع العام بشكل مباشر، ويتم تنظيم القطاع الخاص من خلال "قانون تعزيز استخدام شبكة المعلومات والاتصالات وحماية المعلومات، وفي ضوء ذلك فإن تنظيم الأمن السيبراني في القطاع العام من خلال المراسيم الرئاسية بدلا من القوانين واللوائح له قيود متأصلة في نطاق تأثير اللوائح ذات الصلة، وبالتالي لا يمكن اعتباره في نهاية المطاف متوافقا مع مبادئ سيادة القانون وإدارتها.

جاء تقييم "الاستراتيجية الوطنية للأمن السيبراني" بكوريا الجنوبية على النحو التالي: أولا؛ كان لهذا القرار آثار سياسية كبيرة من حيث أنه أعلن عن الرغبة في تحقيق الأمن السيبراني الوطني على المستويين المحلي والدولي من خلال إنشاء "الاستراتيجية الوطنية للأمن السيبراني"، ثانيا؛ إنها ذات أهمية كبيرة من حيث السياسة التشريعية حيث يمكن أن تكون الاستراتيجية بمثابة شرط أساسي لإرساء تشريعات الأمن السيبراني، ثالثا؛ من الجدير بالملاحظة أنه ينص بوضوح على أن برج المراقبة للأمن السيبراني هو مكتب الأمن القومي في البيت الأزرق، رابعا؛ إن المبادئ الأساسية لـ "استراتيجية الأمن السيبراني الوطنية" مهمة لأنها تعكس آراء الفقهاء.[24]

---

[23] بارك إن-سو، "الدستور والأمن السيبراني"، "دراسات قانون وسياسة الأمن السيبراني"، المجلد 3 (جمعية قانون وسياسة الأمن السيبراني الكورية، أبريل 2018)، ص 19، باللغة الكورية، على الرابط التالي: http://www.kcsa2012.or.kr/wp-content/uploads/2019/01/3rd.pdf، تاريخ الاطلاع: 2025/09/09، على الساعة 15:50 مساء.

[24] لي سونغ يوب، "ضرورة واعتبارات سن قانون الأمن السيبراني الوطني استجابةً للتهديدات السيبرانية"، مجلة سياسة قانون الأمن السيبراني، المجلد 2 (رابطة سياسة قانون الأمن السيبراني الكورية، ديسمبر 2016)، ص 402-405، باللغة الكورية، على الرابط التالي: http://www.kcsa2012.or.kr/wp-content/uploads/2019/01/2nd.pdf?ckattempt=1، تاريخ الاطلاع: 2025/09/09، على الساعة 15:59 مساء.

نتيجة للانتشار الواسع للهجمات الإلكترونية بغض النظر عن القطاع العام أو الخاص، تحدث أضرار اقتصادية هائلة، ومن أجل صد هاته الهجمات التي تهدد الأمن القومي بسرعة وتقليل الأضرار، تم إنشاء اللجنة الوطنية للأمن السيبراني، وتم تكليف المنظمات المسؤولة بمسؤولية حماية الفضاء الإلكتروني ضمن اختصاص الوكالات الحكومية والحكومات المحلية والمؤسسات التي تمتلك أو تدير التقنيات ذات الأهمية الوطنية.

بالإضافة إلى ذلك، تم اقتراح "قانون الأمن السيبراني الوطني" كتشريع حكومي في يناير 2017 لإنشاء مسائل متعلقة بتنظيم وتشغيل الأمن السيبراني بكوريا الجنوبية بشكل منهجي، مثل تبادل معلومات التهديد السيبراني، واكتشاف الهجمات السيبرانية والرد عليها، والإبلاغ عن الحوادث الناجمة عن الهجمات السيبرانية والتحقيق فيها، ومع ذلك، فإن التقدم التشريعي يمر حاليا بمرحلة بطيئة، وتشمل أسباب ذلك، أولا: المشكلة المزمنة المتمثلة في تحويل الجمعية الوطنية لتشريعات الأمن السيبراني إلى نقاش سياسي، وثانيا: المخاوف بشأن انتهاكات الخصوصية، وثالثا: وجهات النظر المتضاربة حول دور جهاز الاستخبارات الوطني.[25]

من المتوقع أن يكون قانون الأمن السيبراني الأساسي في اليابان مرجعا مهما لإصدار قانون الأمن السيبراني الأساسي في كوريا الجنوبية، كما أن البيئة التشريعية للقوانين العامة المتعلقة بالأمن السيبراني فقد نضجت، مع قيام كوريا الشمالية وغيرها من الدول بشن هجمات سيبرانية عشوائية، وبالتالي نظرا للواقع القانوني الملح المتمثل في الحاجة إلى ضمان سلامة الرياضيين المشاركين في الأحداث الدولية واسعة النطاق مثل أولمبياد بيونج تشانج،[26] وذلك ما لا نحبذه أن يقع في بلادنا أثناء تظاهرات كأس العالم 2030، فإن الفشل في سن التشريعات يمكن انتقاده باعتباره تخليا عن مسؤولية كبيرة كعضو في المجتمع الدولي، ولحد عام 2025 لم يتم سن قانون الأمن السيبراني بكوريا الجنوبية، لكن لأسباب حقيقة متعلقة بالشأن الداخلي لها، إلا أن كوريا الجنوبية تعرف استقرارا داخليا في وقتنا الحالي، أما المغرب بالرغم من وجود قانون الأمن السيبراني إلا أنه يعرف بعض القصور.

---

[25] كيم جاي كوانج، الاعتبارات الإدارية والقانونية لقانون الأمن السيبراني الوطني، تاريخ التقديم: 2019/08/10، تاريخ المراجعة وتأكيد النشر: 2019/08/31، باللغة الكورية، على الرابط التالي: http://itnlaw.knu.ac.kr/?task=json&cmd=board-file-download&fid=237&filename=7.%EA%B9%80%EC%9E%AC%EA%B4%91.pdf، تاريخ الاضطلاع: 2025/07/05، على الساعة 21:43 صباحا.

[26] كيم جاي كوانج، نفس المرجع، ص 145-177.

من هذا المنعطف أعلنت نقابة المحامين اليابانية في عام 2003، عن مشروع قانون يتكون من سبعة فصول وأحكام تكميلية إلى جانب بيان رأي يطلب إصدار القانون الأساسي للأمن السيبراني،[27] وعلى الرغم من ذلك، لم تصدر اليابان قانونا أساسيا في مجال الأمن السيبراني لفترة طويلة، ولكنها أنشأت منظمات ذات صلة ونفذت سياسات وفقا للقانون الأساسي بشأن تشكيل مجتمع شبكات المعلومات والاتصالات المتقدمة (الصادر في نوفمبر 2000)، وهو القانون الأساسي في مجال المعلوماتية،[28] جوهر هذا القانون هو إنشاء مجلس سياسة الأمن السيبراني ومركز الأمن السيبراني، مع تعزيز السياسات ذات الصلة التي تركز على هذه المنظمات.

على نفس السياق، تم اتخاذ التدابير اللازمة في مجال الأمن السيبراني، مثل معاقبة أولئك الذين ارتكبوا أعمالا غير قانونية بناء على قانون حظر الوصول غير المصرح به،[29] ومع تزايد الهجمات السيبرانية، اقترحت "استراتيجية الأمن القومي" التي أُعلن عنها في عام 2013 تعزيز الأمن السيبراني، واقترحت "مخطط خطة الدفاع" الذي أُعلن عنه في نفس الوقت للاستجابة الفعالة لمختلف المواقف في الفضاء الإلكتروني كأحد وسائل الردع.

وهكذا، في 12 نوفمبر/تشرين الثاني 2014، سنت اليابان "القانون الأساسي للأمن السيبراني"، الذي ينص على مسؤوليات كل كيان فيما يتعلق بالأمن السيبراني، ويعد هذا القانون بمثابة قانون أساسي في مجال الأمن السيبراني ويعزز فعاليته.[30]

---

[27] بارك سانغ دون، "دراسة حول قانون الأمن السيبراني الأساسي في اليابان: التركيز على آثار إعادة تنظيم نظام قانون الأمن السيبراني في كوريا"، مجلة كيونغهي للقانون، المجلد 50، العدد 2 (معهد أبحاث القانون بجامعة كيونغهي، 2015)، ص 148، باللغة الكورية، على موقع kci: https://www.kci.go.kr/kciportal/ci/sereArticleSearch/ciSereArtiView.kci?sereArticleSearchBean.artiId=ART002003738 ، تاريخ الاطلاع: 2025/09/09، على الساعة 16:00 مساء.

[28] كيم جاي كوانغ وكيم جونغ إيم، " الوضع الحالي وآفاق التشريعات المتعلقة بالجرائم الإلكترونية في اليابان"، مجلة دراسات القانون، المجلد 33، العدد 1 (معهد أبحاث القانون بجامعة دانكوك، يونيو/حزيران 2009)، ص 43، باللغة الكورية، على موقع kci: https://www.kci.go.kr/kciportal/ci/sereArticleSearch/ciSereArtiView.kci?sereArticleSearchBean.artiId=ART001362217، تاريخ الاطلاع: 2025/09/09، على الساعة 16:34 مساء.

[29] كيم جاي كوانغ وكيم جونغ إيم، المرجع نفسه، ص 47-50.

[30] كيم جاي كوانغ، مرجع سابق.

ومع ذلك، فقد تم تحليل أن دورة الألعاب الأولمبية والبارالمبية في طوكيو الذي تم عقدها في عام 2020 كانت بمثابة عامل مباشر في تسليط الضوء على الحاجة إلى سن قانون أساسي في مجال الأمن السيبراني، مع الاعتراف بأن هذا النوع من تدابير الأمن السيبراني له حدود.[31]

تظهر الحكومة الإلكترونية في عدة أشكال من قبيل البوابات الإلكترونية، على سبيل المثال البوابة الإلكترونية للوكالة الحضرية بتطوان، هاته الأخيرة التي التحقت بها كمتدربة، وأعددت تقريرا وضعته في الفصل الثاني للرسالة، وعند تعرفي على المهام المنوطة بالوكالة الحضرية، والتطبيقات الوطنية التي تستعملها من قبل موقع *تعمير* وموقع *رخص*، كذلك موقع *إدارتي* الذي يشترك مع جميع التطبيقات الأخرى سواء المحلية منها أو الوطنية في وثيقة رخصة البناء.

في حين تمثل سياسة الخصوصية للبوابات والتطبيقات الإلكترونية، طوق الحماية لحقوق المؤسسات، مع حفظ حقوق المواطنين والمواطنات من جهة، وكذا الطرف الثالث، لذلك سنعمل على التعرف على موقع حكومة *24* الكوري الذي يوازي موقع *إدارتي* المغربي من حيث الكينونة والطبيعة، وتجدر الإشارة بأن موقع *إدارتي* ليس له سياسة خصوصية، حتى أنه لازال في طور الإنجاز، والذي سيكون قانون رقم 08-09 أساس بنائها.

ثم أن منصة *الحكومة 24* بكوريا الجنوبية (المشار إليها فيما يلي باسم *"Government24"*)، تقوم بمعالجة المعلومات الشخصية وإدارتها بشكل قانوني وآمن وفقا لقانون حماية المعلومات الشخصية والقوانين واللوائح ذات الصلة لحماية حرية وحقوق أصحاب المعلومات، ووفقا للمادة 30 من قانون حماية البيانات الشخصية، تم وضع سياسة الخصوصية والإفصاح عنها لإعلام أصحاب البيانات بإجراءات ومعايير معالجة البيانات الشخصية والتعامل مع الشكاوى المتعلقة بها بسرعة وسلاسة.[32]

على غرار ما أتى سلفا، سنعمد على مقاربة التطبيقات الإلكترونية بالمغرب وكوريا الجنوبية على أساس التشابه في الكينونة والأهداف التي تروم تحقيقها، بحيث تمثل منصة حكومة *24* المنصة الموحدة التي تقدم خدمات عامة للمواطنين بكوريا الجنوبية، في حين أن المغرب يتطلع إلى توحيد

---

[31] بارك سانغ دون، مرجع سابق، ص 149.

[32] المادة 30 (وضع سياسة معالجة المعلومات الشخصية والإفصاح عنها) من قانون حماية المعلومات الشخصية، [تاريخ التنفيذ: 13 مارس 2025] [القانون رقم 19234، 14 مارس 2023، التعديل الجزئي]، على موقع المركز الوطني للمعلومات القانونية بوزارة التشريع الحكومي، موقع رسمي للحكومة الإلكترونية لجمهورية كوريا الجنوبية: https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EA%B0%9C%EC%9D%B8%EC%A0%95%EB%B3%B4%EB%B3%B4%ED%98%B8%EB%B2%95، تاريخ الاضطلاع: 2025/07/06، على الساعة 15:12 صباحا.

الإجراءات الإدارية عبر بوابة موحدة تدمج مختلف الخدمات الرقمية في جميع مراحلها[33] المتمثلة في موقع *إدارتي*، وموقع *رخص* المغربي الذي يوافقه نظام إدارة الوثائق المعمارية- المسمى ب"*نظام سوميتيو*" بكوريا الجنوبية، مع العمل على سياسة الخصوصية للتطبيقات وفقا لقوانين حماية البيانات الشخصية بالمغرب، دأبا على التوجه التي تعمل عليه منظمة التعاون الاقتصادي والتنمية لحماية الخصوصية من أجل: "*توحيد التشريعات الوطنية المتعلقة بالخصوصية، وفي الوقت نفسه دعم هذه الحقوق الإنسانية، الذي من شأنه أن يمنع في الوقت نفسه الانقطاعات في التدفقات الدولية للبيانات*[34]".

تشمل الخدمات الرقمية أو الحكومة الإلكترونية بطبيعتها الشمولية جميع القوانين الرقمية بالمغرب من القانون رقم 54.19 بمثابة ميثاق المرافق العمومية الذي ارتكز على الرقمنة للتأسيس لخدمة عمومية ذات جودة عالية، سهلة الولوج وشفافة، كما تمت بلورة وصياغة القانون رقم 55.19 المتعلق بتبسيط المساطر والإجراءات الإدارية اعتمادا على الرقمنة كآلية لتفعيل هذا القانون ولبلوغ أهدافه المتمثلة في تعزيز الثقة بين الإدارة والمتعاملين معها، لكن يبقى القانون رقم 08-09 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، والقانون رقم 20-05 المتعلق بالأمن السيبراني، أبرز القوانين المؤطرة لموضوع الرسالة.

في نفس السياق لا يوجد قانون مؤطر للحكومة الإلكترونية بالمغرب، وغيرها من القوانين التي أصدرتها الدول المتقدمة في مجال الرقمنة التي تتصف بصفة الجدة، خاصة وأن مواكبة التطور التكنولوجي شيء، ومواكبة التشريع لهذا التطور شيء آخر، ففي كوريا الجنوبية مثلا لديها قانون الحكومة الإلكترونية، وقانون تعزيز التحول الرقمي الصناعي لتعزيز التحول الرقمي للصناعات الذي تم سنه في عام 2021، وقد أرسى هذا القانون الذي صدر في ديسمبر/ كانون الأول، الأساس لدعم استخدام المعلومات الصناعية بشكل شامل ومنهجي بمعنى التأطير التشريعي للتحول الرقمي على مستوى الصناعة بكوريا الجنوبية.

---

[33] يونس أبا علي ومحمد شافعي، "أخنوش يوضح أهداف الاستراتيجية الوطنية للتحول الرقمي"، على موقع SNRT NEWS: https://snrtnews.com/article/103530 ، تاريخ الاطلاع: 2025/07/11، على الساعة 13:09 مساء.

[34] Privacy principles, Organisation for Economic Co-operation and Development (OECD), Retrieved from :https://www.oecd.org/en/topics/privacyprinciples.html#:~:text=They%20set%20out%20eight%20basic,%2C%20individual%20participation%2C%20and%20accountability. accessed 06 july 2025– 15 :12am.

وفقا لأحكام المادة 27 من الدستور المغربي،[35] والقانون 31.13 المتعلق بالحق في الوصول إلى المعلومات نطاق الحق في الوصول إلى المعلومات التي تحتفظ بها الإدارات العامة والمؤسسات والهيئات المنتخبة التي تقدم الخدمة العامة، وكذلك شروط وإجراءات ممارسة هذا الحق، وبالتالي يمكن القول بأن المغرب أطر قانونيا لإدارة البيانات في الجانب المرتبط في الحصول عليها، أما في إطار الحماية القانونية للبيانات الشخصية فمؤطر بقانون رقم 08-09.

على هذا المنوال يعد تحسين جودة وكفاءة الخدمات الحكومية أحد الأهداف الرئيسية للخدمات العامة الرقمية، وذلك من خلال وضع احتياجات المواطنين وتفضيلاتهم في مرتبة مهمة، لكنه يطرح أيضا تحديات وفرصا جديدة لواضعي السياسات والمنظمين، الذين يجب عليهم التأكد من أن الخدمات العامة الرقمية فعالة وشاملة وآمنة وأخلاقية.

وذلك، بمعالجة تهديدات الأمن السيبراني، والمخاوف المتعلقة بالخصوصية، والفجوة الرقمية، ومن المهم أيضا ضمان وجود واجهة سهلة الاستخدام وآليات دعم قوية، والبيئة الديناميكية للخدمات العامة الرقمية، كما يلعب التعاون والشراكات دورا محوريا في دفع الابتكار والكفاءة والحلول التي تركز على المواطن، بينما تتبنى الحكومات في جميع أنحاء العالم التحول الرقمية من بينهم المغرب، في كوريا يدركون الحاجة إلى إشراك أصحاب المصلحة بشكل فعال لتحقيق أهدافهم.

يبقى الدافع الأساسي لكتابة الرسالة التي بين أيديكم هو الإشارة إلى الأهمية التي تحتلها التقنيات الرقمية التي تشكل أساس بناء وتطوير التطبيقات والمنصات الإلكترونية، مع العمل على التأسيس التشريعي فيما بعد للتقنيات الرقمية ببلادنا المغرب، مثل قانون الذكاء الاصطناعي وقانون الحوسبة السحابية، بناء على التجارب السابقة للدولة المتقدمة في هذا المجال على الصعيد العالمي، ثم الارتقاء بمبدأ الخصوصية والأمن السيبراني على المستوى التشريعي، وحتى القضائي بما يمكن الاشتغال عليه لتحسينه على الوجه الذي يرفع ببلدنا نحو الصدارة إفريقيا واحتلال مراتب عالمية محترمة.

من الدافع الذي انطلقت منه، أرجو بأن أصيب الهدف المرجو المتعلق أساسا بتطوير القوانين الرقمية ببلادنا المغرب، وفسح المجال لرفع الضبابية عن الرؤيا القانونية، والتوجهين الفقهي،

---

[35] الفصل 27 من دستور المملكة المغربية (1 يوليوز 2011): «للمواطنين والمواطنات الحق في الحصول على المعلومات الموجودة في حوزة الإدارات العمومية، والمؤسسات المنتخبة، والهيئات المكلفة بمهام المرفق العام، لا يمكن تقييد الحق في المعلومة إلا بمقتضى القانون، بهدف حماية كل ما يتعلق بالدفاع الوطني، وحماية أمن الدولة الداخلي والخارجي، والحياة الخاصة للأفراد، وكذا الوقاية من المس بالحريات والحقوق الأساسية المنصوص عليها في الدستور، وحماية مصادر المعلومات والمجالات التي يحددها القانون بدقة.»

والقضائي في مجال الرقمنة والتكنولوجيا بالدول الأجنبية أمام كل باحث قانوني وطالب علم مهتم بميدان القانون والرقمنة، من منظور سياسة الخصوصية والأمن السيبراني.

على الأقل قد تساهم هاته الرسالة ولو بالنزر اليسير في توجيه الدفة نحو التجارب الأكثر نجاحا حسب الرؤية والأهداف والطموحات، إضافة إلى كل تقنية بعينها تميزت دولة معينة فيها بامتلاك الصدارة عالميا، على سبيل المثال: الذكاء الاصطناعي بالصين، ونظام السحابة بكوريا الجنوبية، الأمن السيبراني بروسيا وكوريا الشمالية، ...، للأخذ بيد الاستراتيجية الوطنية للمغرب الرقمي 2030 نحو الصدارة على المستوى القاري، والريادة عالميا.

مع مرور الوقت أثناء دراسة موضوع الحكومة الإلكترونية بشموليته التقنية المتمثلة في التقنيات الإلكترونية، وتأطيرها القانوني، توضح أن التطور التكنولوجي لا يعني بالضرورة التقدم التشريعي دائما، على سبيل المثال الوضع القانوني للأمن السيبراني بكوريا الجنوبية، لذلك لا يمكن الجزم حتى بعكس ذلك، بأن التطور التشريعي لا يعني أيضا بالضرورة التطور التكنولوجي، على سبيل المثال الوضع التكنولوجي بالمغرب رغم وجود قانون للأمن السيبراني.

رغم صدور عدة قوانين متعلقة بالرقمنة بالمغرب، ووضوح اهتمام المشرع بهذا المجال، إلا أن الكتابات الفقهية تظل قليلة وشحيحة في محتوياتها ومضامينها، وكذا الأحكام والقرارات القضائية، نسترجع فنقول بأن موضوعات التكنولوجيا بما لها من جدة وتعقيد، تبقى حبيسة تخصصها بعيدة عن أصحاب القانون، لذلك يبقى الحل هو الانفتاح على المستجدات العالمية للتكنولوجيا والرقمنة، وما يربطها بتأطيرها القانوني والاجتهادات قضائية بالدول الرائدة.

عمليا يهدف هذا الموضوع إلى النظر في عدة جوانب بطريقة شمولية، تبين مكمن الخلل أو النقص، وحتى مراكز القوة، من خلال الوقوف على التقنيات الإلكترونية مع النظر لتجربة كوريا الجنوبية وآفاقها، للأخذ من هذا النموذج ما يمكن الاستفادة من إيجابياته على المواطنين والمقاولات، من خدمات توفر الوقت والجهد والمال، على مستوى التصنيع فإن نظام الحوسبة السحابية بكوريا الجنوبية يعتبر الأكثر تطورا، وأمنيا لكن من جهة النموذج الياباني فيما يتعلق بالأمن السيبراني، ومجتمعيا تتغلغل التكنولوجيات بالمجتمع حتى تصير ثقافة، واقتصاديا تخلق فرص مناصب شغل.

تم الاعتماد في الرسالة باعتباري طالبة بهذا الماستر، حيث كنا ملزمين بوضع تقرير حول التدريب الميداني، لاكتساب بعض المهارات على أرض الواقع، وبالجمع بين الجانب النظري والجانب التطبيقي، بدل الاقتصار على ما هو تطبيقي فقط؛ فقد عملت على الشق الأول من الرسالة ووضعه نظريا، أما الشق الثاني تطبيقيا على أساس تقرير ميداني.

عند الرجوع للأساس الإداري لديهم، فقط للتعرف على مسار التسلسل الإداري، للوصول إلى المؤسسة المنشودة التي تشابه الوكالة الحضرية والتي ستكون فيما بعد وكالة جهوية مع الاحتفاظ بنفس المهام، لكن لم تظهر إلا شركة الأراضي والإسكان، وإن أطلق عليها صفة شركة إلا أنها مؤسسة عمومية شبه تجارية، رأس مالها استثمار حكومي محض، وبالتالي تم التوصل لنقطة التشابه من حيث المهام والإجراءات والخدمات الإلكترونية التي تقدمانها كلتا المؤسستين، وكل هذا راجع لاختلاف التوجهات، كما عملت على ترجمة التقارير الداخلية للوكالة الحضرية بتطوان من اللغة الفرنسية للغة العربية، ليتسنى لي إدماجها بالرسالة.

في المقابل، فإن إطار القوانين التي قد تكون مشابهة بين البلدين في بعض الأحيان يتم نسخها بصيغة بعيدة كل البعد عن سابقتها ومشابهتها لقانون بلادنا، في البداية أثناء الاطلاع على القوانين بكوريا الجنوبية تجد بأنها قوانين جديدة ومستحدثة وفقا للسياسات العمومية المختلفة عما في المغرب، إلا أنها أثر لمسار قديم لديهم حديث لدينا، بمعنى أنها نفس القوانين التي لدينا إلا أنه تم نسخها كليا.

مع التجربة المتواضعة المرافقة للأحكام والقرارات القضائية لكوريا الجنوبية، فقد كانت عبارة عن مقررات طويلة جدا، قد يختلط فيها ما هو قانوني وواقعي وما هو مرتبط بمجال معين كمجال التكنولوجيا والرقمنة الذي يكون معقدا في كثير من الأحيان، مما يصعب معها الاحتفاظ بتتبع خطى سير القضية، حتى يتم تلخيص فكرتها أو القضية كلها بصيغة تحمل الطبيعة القانونية، إلا أنه يمكن الجزم بالتطور الذي لاقاه القضاء الكوري من حيث استيعابه للكم الهائل من المعلومة، وإن كانت خارج إطار الطبيعة القانونية لتكوين القاضي من حيث الدقة في المعلومة وصياغتها في مقرر قضائي.

في الأخير، فمن بين الصعوبات التي تواجه أي طالب باحث في الترجمة والتصحيح والتدقيق اللغوي بهذا الجانب فقد أخذت وقتا ليس بالهين، كما لا ننسى أنه من بين العراقيل التي تواجه أي طالب باحث في المصادر الإلكترونية التي يشتغل عليها وبناء عليها يقوم ببناء تصميم الموضوع، ثم تصير خارج الخدمة، وبالتالي فقد المعلومة المفيدة، الذي يضطر الطالب الباحث بالتبع لإعادة صياغة التصميم، لكن لا يمكن استرجاع مصدر المعلومة.

من هذا المنطلق سأعمل على طرح إشكالية الموضوع، كالتالي:

ما مدى تطور النظام التشريعي المؤطر للتقنيات في حماية الحكومة الإلكترونية، وخصوصية الأفراد بالمغرب وبالدول المتقدمة في التصنيف العالمي من التسريبات والهجمات السيبرانية؟

بناء على إشكالية الموضوع، نقوم بطرح الفرضيات التالية:

يعرف المغرب تقدما على المستوى التشريعي في سن قانون الأمن السيبراني منذ عام 2020 مقابل تأخر كوريا الجنوبية في إصداره حتى الآن (عام 2025)، إلا أن مكنتها التشريعية تبقى من أدق وأسرع المكنات التشريعية بالعالم، من حيث إصدار القوانين ونسخها وتعديلها، وبذلك يمكن الاستفادة من التطور التشريعي لكوريا الجنوبية واليابان أيضا لسن القوانين الرقمية بالمغرب.

تعد التجربة اليابانية من الناحية التشريعية في مجال الأمن السيبراني، وجهة للمشرع الكوري وليس ببعيد عن المشرع المغربي رغم الفجوة التصنيعية والتكنولوجية والتوعوية والتشريعية، خاصة وأن التجربة اليابانية مشابهة للتجربة المغربية من حيث الارهاصات والأحداث الأولى التي واجهتها من قبل مثل الهجمات السيبرانية، وإقبالها لاحتضان حدث عالمي.

تبرز سياسة الخصوصية للموقع الكوري *"حكومة 24"* القائم على قانون حماية البيانات الشخصية، التأخر في إعداد تطبيق موحد للخدمات العامة بالمغرب، ومكامن النقص التشريعي بقانون 09-08 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي.

يعرف الاجتهاد القضائي والوساطة بكوريا الجنوبية، تطورا شبيها بتطوره التشريعي، الذي قد يستفيد منه المغرب في تحسين اجتهاده القضائي والتحكيمي لحل نزاعات التكنولوجيا والرقمنة.

سنعمد إلى صياغة الرسالة على منهجية المقارنة الخارجية العمودية بين المغرب و كوريا الجنوبية واليابان، مع استعمال أداة الاستقراء أي من الخاص إلى العام، لاستخلاص الاختلافات الفقهية خاصة في التوجه المرتبط بقانون الأمن السيبراني، أينتمي للقانون العام كما هو متعارف عليه بين فقهاء كوريا الجنوبية، أم ينتمي للقانون الخاص؟، إضافة للتعرف على الديناميكية التشريعية الحاصلة بكوريا الجنوبية واليابان، والتطور الحاصل في الاجتهاد القضائي بكوريا الجنوبية حول القوانين الرقمية، وكذا مستويات التقنيات الإلكترونية المتباينة بين البلدين.

سنعمل على طرح استراتيجية المغرب الرقمي 2030 في شقها المرتبط بالتقنيات المتعلقة بالحكومة الإلكترونية وإطارها القانوني بالمغرب وكوريا الجنوبية، ثم ترجمة قوانين ولوائح الأمن السيبراني فقهيا وقانونيا وواقعيا عبر بعض الهجمات السيبرانية التي تستهدف الحكومات الإلكترونية بالمغرب وكوريا الجنوبية واليابان، مع تحديد العقوبات الرادعة لبعض الجرائم الإلكترونية (الفصل الأول)، إضافة إلى الشق الثاني من الموضوع عبر تحديد التطبيقات الإلكترونية وسياسة خصوصيتها وفقا لقانون رقم 09-08 المتعلق بحماية الأشخاص الذاتيين لمعالجة المعطيات ذات طابع شخصي وقانون حماية البيانات الشخصية بكوريا الجنوبية مع بعض المقررات القضائية من كوريا الجنوبية، مع النظر في بعض التسريبات التي وقعت للحكومة الإلكترونية (الفصل الثاني).

الفصل الأول: الإطار القانوني للتكنولوجيات الرقمية والأمن السيبراني كوريا الجنوبية واليابان نموذجا

انصرفت جهود المغرب، تحت القيادة الرشيدة لجلالة الملك محمد السادس، نحو ترسيخ ثقافة التحول الرقمي على جميع المستويات واستثمار الفرص التي تتيحها لفتح آفاق جديدة للدفع قدما بعجلة التنمية ببلادنا، وقد كان جلالته قد أشار في عدة مناسبات إلى الدور الذي تلعبه التكنولوجيا الرقمية في تعزيز النجاعة، والارتقاء بجودة الخدمات العمومية وتيسير الولوج إليها، وكذا زيادة الإنتاجية والقدرة التنافسية للاقتصاد، كما أكد على ضرورة تعميم الإدارة الرقمية بطريقة مندمجة تمكن مختلف القطاعات والمرافق من الولوج المشترك للمعلومات.

في نفس السياق، يطمح النموذج التنموي الجديد الذي وضعه المغرب سنة 2019 إلى استثمار كل الإمكانات التحويلية للتكنولوجيات الرقمية وجعلها ركيزة أساسية ومحفزا لتسريع التنمية وتمكين شرائح واسعة من المواطنين من جني ثمارها، كما جعل منها أحد ركائز تحسين علاقة الإدارة بالمرتفقين وإعادة بناء الثقة بين المواطن والإدارة العمومية، وقد تجسدت هذه التوجهات في أولويات البرنامج الحكومي الذي جعل من تسريع التحول الرقمي أحد أهدافه الأساسية، وقد تم إحداث وزارة الانتقال الرقمي وإصلاح الإدارة لتعنى بهذا الورش الهيكلي من هذا المنطلق.[36]

إن التحول الرقمي (DX. DT. Digital Transformation) الذي ظهر كمفهوم يدمج الحلول، هو مفهوم اجتماعي وطني بكوريا الجنوبية، ويدعو إلى الابتكار والتغيير الثقافي، يتجاوز مجرد الاستخدام البسيط للتكنولوجيا الرقمية في صناعة أو عمل معين، ويشمل نطاقا وطنيا أو مجتمعيا، إنه مفهوم شامل يحدث التغيير الثقافي، ويختلف عن الرقمنة البسيطة، بحيث يمكن القول، أن الخطوة الأولى المهمة في عملية التحول الرقمي هي "الرقمية" والتي تشير إلى "العملية"، ويمكن القول إنها عملية بسيطة تحول الجانب المادي لتدفق العمل إلى الجانب الرقمي على غرار التحول الرقمي، وتشمل المفاهيم النموذجية للحوسبة والرقمنة، والتي تنطوي فقط على اتصال بسيط بالتكنولوجيا الرقمية، بل لعبت دور المحفز لتغيير البنية الاجتماعية بأكملها في جميع أنحاء البلاد.[37]

---

[36] الإدارة الرقمية، موقع رئيس الحكومة، وزارة الانتقال الرقمي وإصلاح الإدارة:https://h1.nu/133-r ، تاريخ الاضطلاع: 2025/06/29، على الساعة 22:13 مساء.

[37] جونغ مي-آي وآخرون، التغيرات في أنشطة الابتكار المؤسسي واستراتيجيات الاستجابة في عصر التحول الرقمي، أبحاث سياسات 7-2021، مجلة STEPI، تاريخ النشر: 30 ديسمبر 2012، باللغة الكورية، على موقع STEPI:

تشير التكنولوجيا السحابية إلى استخدام الموارد الرقمية عبر الإنترنت بشكل فعال ومشترك بين مختلف المستخدمين على اختلاف متطلباتهم، وهناك العديد من النماذج الخاصة للتكنولوجيا السحابية على غرار التكنولوجيا السحابية المتطورة التي تتيح معالجة الحاجيات الخاصة للمستعملين، والتكنولوجيا السحابية القطاعية.

نظام الذكاء الاصطناعي هو نظام آلي قادر، لأهداف معينة، على تقديم توقعات أو توصيات أو اتخاذ قرارات تؤثر على البيئة المحيطة، ويستخدم المعطيات والخدمات التي تولدها الآلة و/أو يقدمها الإنسان من أجل إدراك بيئات حقيقية و/أو افتراضية؛ وإنتاج تصور مجرد لذلك الإدراك في شكل نماذج ناتجة عن التحليل الآلي (مثل التعلم الآلي) أو اليدوي؛ واستخدام النتائج المستخلصة من النماذج لصياغة خيارات نتائج مختلفة، وقد تم تصميم أنظمة الذكاء الاصطناعي لتعمل بدرجات متفاوتة من الاستقلالية.[38]

تشير التكنولوجيا في مجال راحة المستخدم (UX/UI) إلى التكنولوجيا اللازمة لتقديم الخدمات العامة من خلال نافذة متكاملة على مستوى الحكومة، تتطلبها حكومة المنصة الرقمية لتطوير خدمات شخصية استباقية مخصصة، ولتحقيق هذه الغاية، تحدد هذه الجزئية مفهوم راحة المستخدم (UI/UX) بالإضافة إلى منهجية تجربة المستخدم الفردية وتصميم واجهة المستخدم، المفتاح هو فهم العناصر، ومن خلال تنفيذ وتخصيص حكومة منصة رقمية تنافسية عبر تطوير الخدمة.

إمكانية وصول المستخدم (UI) هي مصطلح يستخدم عند إنشاء وتقييم المنتجات والخدمات، بحيث يتمكن أكبر عدد ممكن من المستخدمين من استخدامها دون إنزعاج مع مراعاة القيود، مثل: الخصائص الجسدية للمستخدم، المنطقة، العمر، مستوى المعرفة، التكنولوجيا، والخبرة، ومع ذلك، مع ظهور الويب والأجهزة المحمولة الشخصية توسعت المنتجات والخدمات الرقمية بشكل كبير، حيث تم توسيع نطاق التطبيق ليأخذ بعين الاعتبار احتياجات المستخدم وراحته.

---

https://www.stepi.re.kr/site/stepiko/report/View.do?cbIdx=1292&reIdx=996&cateCont=A0201، تاريخ الاضطلاع: 2025/06/29، على الساعة 22:11 مساء.

[38] تعريف الذكاء الاصطناعي (منظمة التعاون والتنمية الاقتصادية)، الذكاء الاصطناعي بالمغرب: أي استخدامات وأي آفاق للتطوير؟، رأي المجلس الاقتصادي والاجتماعي والبيئي، إحالة ذاتية رقم 2024/78، المجلس الاقتصادي والاجتماعي والبيئي، على الرابط التالي: https://tanmia.ma/wp-content/uploads/2025/03/AVAS78VAP1.pdf، بتاريخ: 2025/06/29، على الساعة 22:13 مساء.

وتعد Agile نموذجا تقنيا لإدارة ذكية مرنة، وهي طريقة لتطوير البرمجيات تهدف إلى تطوير برامج قابلة للتشغيل وتوفيرها بشكل مستمر من خلال التكرار السريع، في نفس سياق Agile تم تقديم DevOpsبوتيرة سريعة جدا مؤخرا.

من جهة أخرى ظهر نموذج Zero trust وهو نموذج جديد لشبكة الأمان المقترح ليكون آمنا من الهجمات السيبرانية، وتعتمد الثقة المعدومة على الفرضية الأساسية التي تقول "لا أحد موثوق به"، عند الوصول إلى منطقة خاصة داخلية من منطقة عامة خارجية، حتى المستخدمين المصرح لهم أو حركة مرور الشبكة لا يتم الثقة بهم، وبشكل غير مشروط، وتتم الموافقة عليهم من خلال التحقق الذي يضمن السلامة.[39]

تشير الثقة المعدومة إلى "لا شيء خارج الحدود بدلا من مفهوم التقنيات الأساسية مثل الذكاء الاصطناعي والبيانات الضخمة والسحابة، هذا هو مفهوم نموذج أمن تكنولوجيا المعلومات غير الموثوق به"، بحيث يكون الهدف هو قمع نطاق الهجمات السيبرانية من خلال النظر في طبقات أمنية إضافية **(المبحث الأول).**

يمكن تعريف الأمن السيبراني على أنه عبارة عن مجموع الوسائل التقنية والإدارية التي يتم استخدامها لمنع الاستخدام غير المصرح به، وسوء الاستغلال واستعادة المعلومات الالكترونية، ونظم الاتصالات والمعلومات التي تحتويها، بهدف توافر واستمرارية عمل نظم المعلومات، وتأمين حماية سرية وخصوصية البيانات الشخصية لحماية المواطنين.

كما أن إهمال الأمن السيبراني يمكن أن يؤدي إلى أزمة أمنية وطنية، وتبذل الدول الأجنبية المتقدمة جهودا لحماية المعلومات والمرافق الوطنية الرئيسية من هجمات القوى التخريبية، على سبيل المثال: أصدرت اليابان "القانون الأساسي للأمن السيبراني" في 12 نوفمبر 2014.

ينحصر الأمن السيبراني بكوريا الجنوبية في القيم الدستورية المتعلقة بالسلامة الوطنية وسلامة المواطنين، وضمان الحقوق الأساسية، وسيادة القانون، والسلم الدولي،[40] فقد نشر مكتب الأمن القومي التابع للبيت الأزرق "الاستراتيجية الوطنية للأمن السيبراني" في أبريل 2019، ويعد الأمن السيبراني بكوريا الجنوبية نظاما مزدوجا حيث ينظم المرسوم الرئاسي "لوائح إدارة الأمن السيبراني الوطنية"

---

[39] Kerman, A. Zero Trust Cybersecurity : Never Trust, Always Verify, 2020.08.28, NIST, Retrieved from: https://www.nist.gov/blogs/taking-measure/zero-trust-cybersecurity-never-trust-always-verify , accessed 06 june 2025 – 00 :32pm.

[40] بارك إن سو، "الدستور والأمن السيبراني"، مرجع سابق.

القطاع العام بشكل مباشر، فحين يتم تنظيم القطاع الخاص من خلال "قانون تعزيز استخدام شبكة المعلومات والاتصالات وحماية المعلومات".

إن التقدم التشريعي يمر حاليا بمرحلة بطيئة، وتشمل ثلاثة أسباب: المشكلة المزمنة المتمثلة في تحويل الجمعية الوطنية لتشريعات الأمن السيبراني إلى نقاش سياسي، والمخاوف بشأن انتهاكات الخصوصية، ووجهات النظر المتضاربة حول دور جهاز الاستخبارات الوطني.

في الوقت نفسه، تم تقديم مشروع قانون تعديل قانون جهاز الاستخبارات الوطني الذي اقترحه النائب كيم بيونغ جي في الجمعية الوطنية العشرين، ويعتبر هذا مشروعا تشريعيا صحيحا من حيث أنه يوفر أساسا قانونيا للأمن السيبراني من خلال تحديد "الوقاية والرد على الهجمات السيبرانية التي تستهدف المؤسسات الحكومية والعامة المرتبطة مباشرة بالأمن الوطني" (البند 4 من الفقرة 1 من المادة 3) كواحدة من واجبات جهاز المخابرات الوطني.

في عام 2003، أعلنت نقابة المحامين اليابانية عن مشروع قانون يتكون من سبعة فصول وأحكام تكميلية إلى جانب بيان رأي يطلب إصدار القانون الأساسي للأمن المعلوماتي، وعلى الرغم من ذلك، لم تصدر اليابان قانونا أساسيا في مجال الأمن السيبراني لفترة طويلة، بالإضافة إلى ذلك، تم اتخاذ التدابير اللازمة في هذا مجال، مثل معاقبة أولئك الذين ارتكبوا أعمالا غير قانونية بناء على قانون حظر الوصول غير المصرح به.

ومع تزايد الهجمات السيبرانية، اقترحت "استراتيجية الأمن القومي" التي أُعلن عنها في عام 2013 تعزيز الأمن السيبراني، واقترحت "مخطط خطة الدفاع" الذي أُعلن عنه في نفس الوقت كأحد وسائل الردع والاستجابة الفعالة لمختلف المواقف على الإنترنت، ومن تم سنت اليابان "القانون الأساسي للأمن السيبراني" بتاريخ 12 نوفمبر/تشرين الثاني 2014 **(المبحث الثاني).**

المبحث الأول: الإطار التقني والقانوني لتكنولوجيات الحكومة الإلكترونية بالمغرب وكوريا الجنوبية

إن نطاق التقنيات والمعايير المتعلقة بالحكومة الإلكترونية بالمغرب وكوريا الجنوبية واسع جدا بحيث يصعب تغطيتها جميعا، لذلك سنستعرض هنا التقنيات التي تتوافق نسبيا مع تعريف وأهداف وأهمية الحكومة الإلكترونية، وبعد ذلك تأطيرها تشريعيا.

يطمح النموذج التنموي الجديد الذي وضعه المغرب سنة 2019 إلى استثمار كل الإمكانات التحويلية للتكنولوجيات الرقمية وجعلها ركيزة أساسية ومحفزا لتسريع التنمية وتمكين شرائح واسعة

من المواطنين من جني ثمارها، كما عكفت الوزارة المعنية على إعداد خارطة طريق على المدى القصير، والمتوسط، والبعيد، تتكامل فيها مختلف المخططات القطاعية للتحول الرقمي لمسار المرتفق سواء كان مواطنا أو مقاولة.

امتدادا مما سبق، فإن المغرب يتوفر على مؤهلات مهمة تخول له التموقع بشكل جيد في مجال الذكاء الاصطناعي، إذ اعتمد نصوصا قانونية تؤطر الجوانب الأساسية للتكنولوجيا الرقمية، من قبيل الأمن السيبراني وحماية المستهلكين، ومع ذلك، لا تزال هناك العديد من العقبات، لعل أهمها غياب إطار تنظيمي خاص بالذكاء الاصطناعي وبطء وتيرة تحرير المعطيات العمومية.

ويتم حاليا العمل على إحداث مديرية متخصصة في الذكاء الاصطناعي، والتكنولوجيات الناشئة ضمن المديرية العامة للانتقال الرقمي تعنى بوضع السياسة العمومية في مجال البيانات الوطنية والذكاء الاصطناعي والتكنولوجيات الناشئة ووضع البرنامج والمشاريع والتدابير التنفيذية، وإعطاء وإعداد الإطار التشريعي والتنظيمي والمعايير الأخلاقية، وتعزيز البحث العلمي والابتكار والتعاون الدولي، مع الرصد واليقظة لضمان استخدام مسؤول وآمن للذكاء الاصطناعي، وبذاك داعية إلى استخدام مسؤول لهذه التقنيات الجديدة.

في المقابل تفرض حكومة المنصة الرقمية بكوريا الجنوبية قانونا لإضفاء الطابع الإلكتروني على الإدارة غير المتصلة بالإنترنت، وفي الوقت نفسه الذكاء الاصطناعي والبيانات الضخمة والسحابة، بحيث يتم السعي إلى خلق بيئة يمكن للجميع الاستمتاع فيها بفوائد الخدمات العامة، من خلال دمج وربط جميع البيانات الضرورية باستخدام التقنيات الجديدة، مثل: بناء نظام تعاوني يعتمد على التعاون بين القطاعين العام والخاص لحل المشكلات الاجتماعية المختلفة وتم وضع خطة التنفيذ.

وأهم ما في تعزيز خطة التنفيذ هو التحديد الدقيق لمعوقات الخدمات الحالية من وجهة نظر المواطنين المستفيدين من الخدمات العامة، والتأكد من أن أي شخص يمكنه الوصول إلى الخدمات العامة بسهولة ويسر من خلال خبرات متكاملة وعناصر تصميمية موحدة تكون مضمونة، يطلق عليها راحة المستخدم (UI/UX) (المطلب الأول).

علاوة على ما سبق، تم اعتماد عدد من المحفزات ووضعها في صلب الاستراتيجية الوطنية أبرزها استخدام الخدمات الرقمية السحابية وذلك عن طريق تشجيع الإدارات والمؤسسات العمومية والمقاولات إلى اللجوء الى استخدام هذه التكنولوجيا في حال الاستعانة بمصادر خارجية لإدارة نظم المعلومات.

وتعتبر التكنولوجيا السحابية (كلاود) آلية لتوفير خدمات تكنولوجيا المعلومات والبرمجيات على الانترنت بدل جهاز الحاسوب الخاص أو الخادم المحلي، باستخدام شبكة من الحواسيب (مزرعة خوادم) بعيدة عن المستخدم ويتم إيواؤها على الانترنت.

تطبق على الحوسبة السحابية بالمغرب تشريعات عامة، بما في ذلك قانون الأمن السيبراني رقم 05-20 الذي ينظم حماية المعطيات الحساسة، إضافة إلى قوانين أخرى تركز على حماية البيانات الشخصية تتمثل في قانون حماية الأشخاص الذاتيين لمعالجة المعطيات ذات الطابع الشخصي08-09، ولا يوجد قانون خاص بالحوسبة السحابية بالمغرب.

على عكس كوريا الجنوبية التي أعلنت وزارتها للعلوم وتكنولوجيا المعلومات والاتصالات عن "الخطة الأساسية الثالثة للحوسبة السحابية (2022-2024) في 6 سبتمبر 2021، بناء على "قانون تعزيز الحوسبة السحابية وحماية المستخدمين" الصادر في عام 2015.

ومن خلال "الاستراتيجية الرقمية لكوريا" التي تم الإعلان عنها في مؤتمر الطوارئ الثامن للاقتصاد وسبل العيش الذي ترأسه الرئيس جمهورية كوريا في 28 سبتمبر 2022، تعمل على تعزيز الاستخدام اليومي للسحابة في القطاعين العام والخاص، وتسعى هذه الاستراتيجية إلى تعزيز تطوير تقنيات المصدر لتأمين تكنولوجيا الذكاء الاصطناعي ذات المستوى العالمي، وخلق بيئة لدمج البيانات العامة والخاصة.

وفقا لخطة تحقيق حكومة المنصة الرقمية بتاريخ 14/ 2023/04، تعتبر الطريقة الحالية لتعزيز المعلومات العامة التي تعتمد على النظام (نظام متجانس)، تم تشخيص صعوبات من بينها صعوبة إعادة تأهيل وظائف النظام، وأن هناك قيودا على إدخال أحدث التقنيات والتطوير السريع للخدمات، ففي الآونة الأخيرة، أصبحت بنية النظام معقدة، مثل: دمج الأنظمة العامة المماثلة أو إدخال التقنيات المتطورة مثل الذكاء الاصطناعي، ومع زيادة عدد الأجهزة، تتزايد أيضا حالات الإعاقة.

يعد Agile كمنظور يتجه إلى التعاون وسير العمل بدلا من مجموعة من اللوائح التي تحدد العمل المطلوب لتطوير البرمجيات، وهي عملية تنظيمية، بحيث يكون هو أقرب إلى "نظام القيم الذي يوجه الاختيارات حول ما يجب صنعه وكيفية صنعه"، بمعنى آخر، كما هو الحال في استراتيجية "مخطط الحكومة الرقمية" في سنغافورة، فمن المستحسن التعامل معها من مستوى أعلى، مثل: مستوى الثقافة والقيم التي تعزز حكومة المنصة الرقمية بدلا من منهجية تطوير البرمجيات.

في نفس سياق Agile تم تقديم DevOps الأكثر فعالية في الاستجابة بسرعة للمتطلبات العالية والمتغيرة بشكل متكرر، بفضل مجموعة متنوعة من التجارب التي يمكن أن تساعد وتضمن القدرة

التنافسية لمؤسسات تطوير البرمجيات، قامت كوريا مؤخرا بتطوير السحابة، وتتضح الأمور مع إدخال تكنولوجيا الحوسبة.

سنت الدولة ما مجموعه 9 قوانين متعلقة بالبيانات تخضع لسلطة 6 وكالات، بما في ذلك قانون البيانات العامة كقوانين متعلقة بالبيانات، تم سنه وتنقيحه، بما في ذلك قانون البيانات العامة، وقانون إدارة البيانات والقانون الإطار بشأن المعلومات الذكية، وقانون صناعة البيانات، والقانون الرقمي الصناعي، إضافة إلى أن هناك قانون تعزيز التحويل، وقانون المعايير الوطنية، وقانون حماية المعلومات الشخصية، وقانون شبكة المعلومات والاتصالات، وقانون المعلومات الائتمانية، من بينها قانون صناعة البيانات، الذي صدر في 19 أكتوبر 2021، لعرض إنشاء أساس لتطوير صناعة البيانات، بما في ذلك خلق قيمة اقتصادية من البيانات.

هناك تهديدات مستمرة للفضاء السيبراني الرقمي، مثل: القرصنة، لذا فإنه ولتكون الشبكات آمنة من هذه التهديدات السيبرانية، هناك حاجة ملحة لتهيئة البيئة، بحيث ظهر نموذج Zero trust الذي تكمن أهمية بنيته في الابتعاد عن النموذج الأمني الحالي القائم على المحيط، حيث يكون الوصول إلى الموارد أو البيانات داخل الحدود غير مؤكد، مع إلى الانتقال إلى نموذج أمن تكنولوجيا المعلومات الذي "لا يثق في الحدود أو أي شيء خارج الحدود" (المطلب الثاني).

المطلب الأول: الإطار التشريعي للبيانات والذكاء الاصطناعي والتوحيد القياسي لراحة المستخدم

من أجل إنشاء نظام متكامل لإدارة البيانات، يتم تقييم حالة إدارة البيانات وفقا للسياسات الوطنية، مع القوانين والأنظمة والسياسات الرقمية ذات الصلة، ويتم تنفيذ أنشطة المتابعة مثل تحديد وتحليل ممارسات إدارة البيانات المتقدمة، ووضع خطة تنفيذ متكاملة لها، فمن الضروري فهم مبادئ إدارة الدولة للحكومة الجديدة واتجاه السياسة الرقمية، بمعنى تحليل الأنظمة القانونية المتعلقة بالبيانات (قانون صناعة البيانات، قانون استخدام البيانات العامة) وخلفية إدارة جودة البيانات العامة على مستوى الحكومة، كما هو مطلوب تحليل السياسات ذات الصلة.

لقد أدى التقدم التكنولوجي حتى الآن إلى رفع مستوى خدمات الذكاء الاصطناعي حول العالم من مستوى بسيط إلى مستوى تكنولوجيا يساعد الناس، وعلى وجه الخصوص، فإن إدخال تقنيات مبتكرة مثل نماذج الذكاء الاصطناعي الضخمة له تأثير كبير حتى على القطاع العام الذي يتسم بالتحفظ في تقديم تقنيات جديدة في القطاع العام.

هناك العديد من المهام المتكررة والبسيطة، بدءا من تطبيقات الإدارة الداخلية والخدمة المدنية وحتى الموافقة والإخطار، بيد أن تطبيق نموذج ذكاء اصطناعي فائق الضخامة على هذه المهام يمكن أن يؤدي إلى تحسين كفاءة العمل بشكل كبير، ومن خلال الاستفادة من الوقت الذي توفره، يمكن للموظفين العموميين التركيز على مهام أكثر إبداعا وأهمية، وستزيد كفاءة العمل في القطاع العام بشكل كبير، وسيؤدي هذا في النهاية إلى فتح الفرص لتقديم خدمات أفضل للجمهور (الفقرة الثانية).

تفرض حكومة المنصة الرقمية بكوريا الجنوبية قانون إضفاء الطابع الإلكتروني على الإدارة غير المتصلة بالإنترنت، وفي الوقت نفسه الذكاء الاصطناعي والبيانات الضخمة والسحابة، وعموما يتم السعي إلى خلق بيئة يمكن للجميع فيها الاستمتاع بفوائد الخدمات العامة من خلال دمج وربط جميع البيانات الضرورية باستخدام التقنيات الجديدة.

أهم ما في تعزيز خطة التنفيذ هو التحديد الدقيق لمعوقات الخدمات الحالية من وجهة نظر المواطنين المستفيدين من الخدمات العامة، والتأكد من أن أي شخص يمكنه الوصول إلى الخدمات العامة بسهولة ويسر من خلال خبرات متكاملة وعناصر تصميمية موحدة تكون مضمونة، يطلق عليها راحة المستخدم (UI/UX)، ويشرح هذا الجزء الإطار التشريعي المرتبط بها (الفقرة الثالثة).

الفقرة الأولى: الإطار القانوني لنظام متكامل لإدارة البيانات بكوريا الجنوبية

يتم تطبيق مجموعة واسعة من التقنيات على حكومة المنصات الرقمية، ويمكن استخدام هذه التقنيات بسرعة وفقا للتغيرات في السياسة أو المجتمع، ومع تغيرها ليس من السهل التمييز بين هذه التقنيات وتنظيمها، تقوم شركة Gartner وهي شركة استشارية بتحليل اتجاهات التكنولوجيا في الحكومة الإلكترونية بشكل مستمر، اتجاهات التكنولوجيا للحكومة الرقمية وتحقيق حكومة المنصة الرقمية.

بالإشارة إلى مهام تنفيذ الخطة، تم تحديد القضايا الرئيسية المتعلقة بالتكنولوجيا وتوحيد حكومة المنصة الرقمية وتم تلخيص الاتجاهات ذات الصلة[41]، تقترح شركة Gartner الاستشارية العالمية منصة تقنية حكومية رقمية للتحول الرقمي للحكومة[42]، بالتالي سنتعرف على النظام المتكامل لإدارة

---

[41] *جارتنر تعلن عن "12 اتجاها للتكنولوجيا الحكومية لعام 2022"*، باللغة الكورية على موقع brunch story: https://brunch.co.kr/@choimeal/10، تاريخ الاطلاع: 2025/06/03، على الساعة 00:36 صباحا.

[42] Finnerty, B. opicit.

البيانات للحصول على خدمات بيانات عالية الجودة وإطارها القانوني، بالمغرب بشكل مختصر (أولا)، وبكوريا الجنوبية(ثانيا).

أولا: إطار قانوني لإدارة البيانات بالمغرب

وفقا لأحكام الدستور المغربي، لا سيما المادة 27 منه، يحدد القانون 31.13 المتعلق بالحق في الوصول إلى المعلومات[43] نطاق الحق في الوصول إلى المعلومات التي تحتفظ بها الإدارات العامة والمؤسسات والهيئات المنتخبة التي تقدم الخدمة العامة، وكذلك شروط وإجراءات ممارسة هذا الحق، وبالتالي يمكن القول بأن المغرب أطر قانونيا لإدارة البيانات في الجانب المرتبط في حق الحصول عليها، أما في إطار الحماية القانونية للبيانات الشخصية فمؤطر بقانون رقم 08-09.

ثانيا: الإدارة القائمة على البيانات بكوريا الجنوبية وإطارها التشريعي

1- الإدارة القائمة على البيانات بكوريا الجنوبية

مع تزايد استخدام البيانات وتسليط الضوء على أهميتها في جميع أنحاء الإدارة الحكومية وحياة الناس، أصبحت البيانات هي محور التركيز، وتبذل جهودا لتعزيز الإدارة العلمية في العديد من البلدان، وقد أصدرت الولايات المتحدة الرائدة في هذا المجال، "قانون أسس صنع السياسات المبنية على الأدلة لعام 2018".

تعزز كوريا الجنوبية الشفافية الحكومية والإدارة العلمية من خلال البيانات، علما أن لديها قانون للبيانات لعام 2020، ومن أجل زيادة المسؤولية الإدارية والاستجابة والموثوقية من خلال تفعيل إدارة البنية التحتية وتحسين نوعية حياة الناس، تم سن "قانون تفعيل الإدارة القائمة على البيانات" (المشار إليه فيما يلي باسم قانون الإدارة القائمة على البيانات)، وتم وضع الخطة الأساسية وتنفيذها.

- الخطة الأساسية لتنشيط الإدارة القائمة على البيانات

تعتمد الخطة الأساسية لتنشيط الإدارة القائمة على البيانات على "قانون الإدارة القائمة على البيانات"، وتعزز نظام الاستخدام المشترك للبيانات وقدرات تحليلها واستخدامها في نظام الاستخدام المشترك للمعلومات الإدارية الحالي، لتحقيق الابتكار الإداري القائم على البيانات مثل حل القضايا الاجتماعية والخدمات الحكومية المخصصة.

---

[43] القانون رقم 31.13 المتعلق بالحق في الوصول إلى المعلومات، على موقع acaps: https://h1.nu/16N2E ، تاريخ الاطلاع: 2025/07/06، على الساعة 21:23 مساء.

تتضمن الخطة الأساسية رؤية "تنفيذ خدمات حكومية ذكية تعمل على تحسين نوعية حياة الناس من خلال وضع أربع استراتيجيات لتعزيز الخدمات الإدارية الذكية: "الإدارة العلمية القائمة على البيانات"، و"تنفيذ الإدارة العلمية التي تستخدم البيانات بشكل فعال في قرارات السياسة"، و"ثقة المواطنين وتعاطفهم".

من أجل الاستخدام المشترك للبيانات تم إنشاء منصة متكاملة لإدارة البيانات، وإنشاء منصة بيانات لكل مجال وتعزيز الاتصال:

- تعزيز اكتشاف الأسس والمهام المؤسسية للإدارة القائمة على البيانات، من أجل إنشاء نظام لتنشيط الإدارة القائمة على البيانات.
- اكتشاف مهام التحليل التي يمكن أن تواجهها مهام السياسة العامة ولتوفير الخدمات الذكية.
- تعزيز العمليات الإدارية وقدرات الابتكار والثقافة الإدارية العلمية لابتكار أساليب العمل القائمة على البيانات.[44]

ب- الإطار التشريعي لإدارة قائمة على البيانات بكوريا الجنوبية

بناء على ما تقدم، ومن أجل تحقيق خدمة بياناتي بكوريا الجنوبية، هناك حاجة إلى أساس قانوني يتطلب من صاحب المعلومات إرسال معلومات الفرد وفقا لطلبه، عودا على بدء فإن قانون معالجة الشكاوى المدنية وقانون الحكومة الإلكترونية، فقط هما اللذان يحكمان المعلومات في القطاع العام، ويوفران أساس قانوني ينص على "الحق في طلب المعلومات".

تم تقديم "*بياناتي*" في القطاع العام لأول مرة من خلال "خطة تعزيز الابتكار في الحكومة الرقمية" بتاريخ أكتوبر 2019، وتستهدف المؤسسات الإدارية والعامة المرتبطة بشبكة الحكومة الإلكترونية العامة My Data، فإن معظم المعلومات التي يتم الكشف عنها هي معلومات عن شهادات مختلفة يمكن إصدارها عبر الانترنت، مما يجعل تعزيز عبء الأمن الإداري بسرعة ممكنا، والبيانات في حد ذاتها ليست معلومات مفيدة للاستفسار أو التحليل المتكامل، ولكنها مرتبطة بخدمات وتستخدم كمعلومات يجب إثباتها علنا.

من الناحية المتعلقة بمراجعة القوانين العامة لتعزيز *"بياناتي"* في كافة المجالات، فنظرا لأن الحق في نقل المعلومات الشخصية هو حق أساسي لصاحب المعلومات، فهو مرتبط بقانون حماية المعلومات الشخصية، وهو قانون عام يتعلق بالمعلومات الشخصية تم التوصل إلى توافق في الآراء

---

[44] سون سونغ هيون، مرجع سابق.

بشأن ضرورة تنظيم محتوياته في يناير 2021، ومن أجل ضمان الاتساق في الاتجاه القانوني والمؤسسي، تم التنصيص على حق نقل المعلومات الشخصية، كما تم تنظيم التفاصيل التي تأخذ في الاعتبار خصائص كل مجال من خلال الإخطار من قبل الوزارات المختصة في كل صناعة.[45]

الفقرة الثانية: الإطار التشريعي للذكاء الاصطناعي

سنعمل على التعرف على الإطار العام للذكاء الاصطناعي وارهاصاته بالعالم (أولا)، ثم مشروع قانون الذكاء الاصطناعي بكوريا الجنوبية (ثانيا)، ومضامينه (ثالثا)، خاصة وأن المغرب لازال لم يضع قانونا للذكاء الاصطناعي ولو مشروع قانون.

أولا: الإطار العام للذكاء الاصطناعي

تقدم المخابرات الكورية عبر وكالة مجتمع المعلومات الكورية خريطة مفاهيمية للذكاء الاصطناعي الفائق العام، وتستند إلى البنية التحتية/ المنصة الحكومية الضخمة للذكاء الاصطناعي، واقترح الرأي أنه من خلال الجمع بين البيانات المنتجة في الميدان مع الذكاء الاصطناعي الضخم ينبغي تطبيق التكيف من قبل كل إدارة حكومية، كما ينبغي توفير خدمات الذكاء الاصطناعي التي تجمع بين الخبرة العامة والمجال.[46]

في المقابل فإن المغرب لا زال يعرف العديد من العقبات، لعل أهمها غياب إطار تنظيمي خاص بالذكاء الاصطناعي وبطء وتيرة تحرير المعطيات العمومية، كما أن الخصاص الواضح في الكفاءات والمكونين المؤهلين يعيق أيضا تطوير منظومة فعالة للذكاء الاصطناعي، علاوة على ذلك، وعلى الرغم من بعض المبادرات المعزولة في مجالي البحث والتطوير، فإن غياب التجانس بين المشاريع وعدم ملاءمتها للاحتياجات الصناعية، في ظل عدم وجود رؤية وطنية واضحة ومتجانسة، يعيق تنفيذ حلول تنسجم مع الأولويات الاقتصادية لبلادنا.[47]

---

[45] لي جاي دو، معايير المرجع ومواقع البيانات في سياسة البيانات الوطنية، تاريخ النشر: 2022/10، باللغة الكورية، على الرابط التالي: https://h1.nu/10hnW، تاريخ الاضطلاع: 2025/06/29، على الساعة 00:37 صباحا.

[46] وكالة مجتمع المعلومات الاستخباراتية الكورية، اتجاه تقديم الذكاء الاصطناعي واسع النطاق في القطاع العام استنادا إلى نموذج اللغة واسع النطاق، استراتيجية تكنولوجيا المعلومات والمستقبل، العدد 3، تاريخ النشر: 2023/04/07، على موقع وكالة مجتمع المعلومات الاستخباراتية الكورية NIA: https://www.nia.or.kr/site/nia_kor/ex/bbs/View.do?cbIdx=25932&bcIdx=25490&parentSeq=25490 ، تاريخ الاضطلاع: 2025/06/30، على الساعة 00:37 صباحا.

[47] الذكاء الاصطناعي بالمغرب: أي استخدامات وأي آفاق للتطوير؟، رأي المجلس الاقتصادي والاجتماعي والبيئي، مرجع سابق.

كشفت الوزيرة المنتدبة لدى رئيس الحكومة المكلفة بالانتقال الرقمي وإصلاح الإدارة الحالية، عن إحداث مديرية متخصصة في الذكاء الاصطناعي، عموما فإن التكنولوجيات الناشئة ضمن المديرية العامة للانتقال الرقمي تعنى بوضع السياسة العمومية في مجال البيانات الوطنية والذكاء الاصطناعي والتكنولوجيات الناشئة، ووضع البرنامج والمشاريع والتدابير التنفيذية، وإعطاء وإعداد الإطار التشريعي والتنظيمي والمعايير الأخلاقية، وتعزيز البحث العلمي والابتكار والتعاون الدولي مع الرصد واليقظة لضمان استخدام مسؤول وآمن للذكاء الاصطناعي، وبذاك داعية إلى استخدام مسؤول لهذه التقنيات الجديدة، وفي هذا السياق، لفتت الوزيرة إلى أن "الذكاء الاصطناعي يشكل جزء لا يتجزأ من استراتيجية "المغرب الرقمي 2030"، كما سيتم استخدام الذكاء الاصطناعي في مجالات رئيسية مثل: الخدمات العمومية، ولازال المغرب يعمل على وضع الاستراتيجية الخاصة بالذكاء الاصطناعي، والقانون المؤطر.[48]

في المقابل فإن العديد من البلدان، فضلا عن الإدارات الحكومية في كوريا الجنبية، تمنع الوصول إلى DeepSec من أجهزة الكمبيوتر ذات الوصول الخارجي، فإن الشركات المالية تمنع أيضا DeepSec لمنع إمكانية تسريب معلومات تجارية حساسة أو معلومات شخصية،[49] تم تعليق الخدمة المحلية مؤقتا في 15 فبراير 2025 بقرار من لجنة حماية المعلومات الشخصية في جمهورية كوريا، ومن المقرر استئناف الخدمة بعد إجراء التحسينات والإضافات وفقا لقانون حماية المعلومات الشخصية المحلي،[50] بمعنى أن الأمر يدخل في الصراع على الخصوصية والأمن القومي والهيمنة على التكنولوجية العالمية.

قامت لجنة حماية المعلومات الشخصية بكوريا بإرسال استفسار للتأكد من شرعية طرق جمع ومعالجة المعلومات الشخصية التي تتبعها شركة DeepSeek وهي خطوة نحو مراجعة ممارسات الخصوصية الخاصة بشركةDeepSec هذا على مستوى الحكومة، أما على مستوى الأوساط السياسية فيشعر حزب قوة الشعب الحاكم بالقلق إزاء تأثير ظهور DeepSec على صناعة الذكاء الاصطناعي

---

[48] الذكاء الاصطناعي بالمغرب.. السغروشني تعلن إطلاق خمس مبادرات، Medi1News، 2025/05/20، YouTube: https://h1.nu/10hp5، تاريخ الاضطلاع: 2025/06/29، على الساعة 22:15 مساء.

[49] جو جي وان، المؤسسات المالية تشارك أيضا في "منع الوصول إلىDeepSec ، تاريخ النشر: 6 فبراير 2025، باللغة الكورية، على موقع هانكيوريه: https://www.hani.co.kr/arti/economy/economy_general/1181020.html، تاريخ الاضطلاع: 2025/06/30، على الساعة 00:37 صباحا.

[50] لي سانغ سيو، أوقفت لجنة حماية المعلومات الشخصية (PIPC) الخدمة المحلية الجديدة لشركةDeepSeak، مشيرة إلى سياسة معلومات شخصية غير كافية، تاريخ النشر: 17 فبراير 2025، باللغة الكورية، على موقع وكالة يونهاب للأنباء: https://www.yna.co.kr/view/AKR20250217066600530 ، تاريخ الاضطلاع: 2025/06/30، على الساعة 00:39 صباحا.

المحلية ويحث الحكومة على تعزيز مشاريع البحث والتطوير متوسطة وطويلة الأجل ومعالجة الفواتير ذات الصلة بسرعة، وأشار حزب المعارضة الديمقراطي الكوري وحزب ابتكار الوطن إلى أن استجابة الحكومة غير كافية، مطالبا بزيادة ميزانية البحث والتطوير ومنح اللجنة الوطنية للذكاء الاصطناعي دورا أكثر نشاطا.

يشكل ظهور DeepSec في المنافسة العالمية لتكنولوجيا الذكاء الاصطناعي، تحديا لهيكل احتكار تكنولوجيا الذكاء الاصطناعي المتمركز في الولايات المتحدة وأوروبا، مما يبشر بتغيير في توازن سوق الذكاء الاصطناعي العالمي، تتبنى بعض البلدان استراتيجيات لحجب الأمن العميق لحماية قيادتها التكنولوجية، كما أن المناقشة حول حظر DeepSec تتجاوز القضايا التقنية البسيطة وتتوسع إلى مشكلة مرتبطة بشكل مباشر بالمنافسة على هيمنة تكنولوجيا الذكاء الاصطناعي العالمية، ومن المتوقع في المستقبل تعزيز اللوائح الخاصة بتقنيات الذكاء الاصطناعي الصينية مثل DeepSec، وهو ما سيكون له تأثير كبير على سرعة التطور التكنولوجي والتغيرات في النظام البيئي العالمي للذكاء الاصطناعي.[51]

ثانيا: الإطار العام لمشروع قانون الذكاء الاصطناعي بكوريا الجنوبية

ينص قانون الإطار بشأن الذكاء الاصطناعي على أنه عند إنشاء وتنفيذ خطة ترويجية على مستوى الحكومة مثل الخطة الأساسية، يجب أخذ الخطة الشاملة وخطة التنفيذ لـ "القانون الأساسي بشأن المعلومات الذكية" الحالي في الاعتبار، ويجب اعتبار الخطة الأساسية بمثابة خطة ترويجية خاصة بالقطاع لـ "القانون الأساسي بشأن المعلومات الذكية"، ومن خلال هذا، يتم هيكلة الأمر منطقيا بحيث لا يمكن تنفيذ الخطة الأساسية للحكومة بموجب القانون الإطار بشأن الذكاء الاصطناعي إلا إذا تم أولا إنشاء الخطة الشاملة وخطة التنفيذ لـ "القانون الأساسي بشأن المعلومات الذكية".

علاوة على ذلك، ينص قانون الإطار بشأن الذكاء الاصطناعي على إنشاء لجنة وطنية للذكاء الاصطناعي تحت إشراف الرئيس باعتبارها أعلى هيئة لمناقشة السياسات واتخاذ القرارات، ومع ذلك، بما أن لجنة استراتيجية المعلومات والاتصالات، وهي أعلى هيئة للتداول واتخاذ القرار بموجب قانون الإطار بشأن المعلومات الذكية، يمكنها بالفعل الإشراف على مجال الذكاء الاصطناعي، فإن تنسيق الحوكمة التشغيلية يبدو ضروريا أيضا.

---

[51] *مشكلة حظر Deepseek: مرحلة جديدة في سباق الذكاء الاصطناعي العالمي*، تاريخ النشر: 1 فبراير 2025، باللغة الكورية، على موقع Blog: https://inblog.ai/ringo/deepseek-blockade-issue ، تاريخ الاضطلاع: 2025/09/10، على الساعة 19:54 مساء.

تنص الأحكام التكميلية على أن القانون سيدخل حيز التنفيذ بعد عام واحد من تاريخ إصداره، وهو ما يبدو وكأنه حساب زمني لا مفر منه نظرا لعلاقته بقانون الإطار بشأن المعلومات الذكية، لأن المادة 5 من المرسوم التنفيذي لقانون الإطار بشأن المعلومات الذكية تنص على أن "رؤساء الوكالات الإدارية المركزية ورؤساء الحكومات المحلية يجب أن يستكملوا خطة التنفيذ للعام التالي بحلول 31 ديسمبر من كل عام ويقدموها إلى وزير العلوم وتكنولوجيا المعلومات والاتصالات ووزير الداخلية والأمن بحلول 31 يناير من العام التالي"، لذلك يحسب أنه لا يمكن وضع الخطة الأساسية للحكومة بموجب قانون الإطار بشأن الذكاء الاصطناعي إلا في عام 2026.

تم التعامل مع نموذج سن قانون الإطار بشأن الذكاء الاصطناعي باعتباره امتدادا لقانون الإطار بشأن تعزيز المعلومات والاتصالات (الذي صدر في عام 1995)، وهو السلف لقانون الإطار بشأن المعلومات والاتصالات الذكية، الذي صدر في عام 2020، وقانون الإطار بشأن المعلوماتية الوطنية (الذي تمت مراجعته بشكل شامل في عام 2009)، والذي كان بمثابة مراجعة شاملة له.

بعبارة أخرى، عند استخدام المصطلحات القانونية مثل مجتمع الذكاء الاصطناعي وأخلاقيات الذكاء الاصطناعي، يبدو أنه من المحتم أن تكون هناك قضايا تعديل في تشغيل القانون لأنه حاول الضفر بتطوير الذكاء الاصطناعي وضمان السلامة في نفس الوقت على المستوى الكلي للمعلوماتية الذكية بكوريا بأكملها.

وبطبيعة الحال، فإن الوزارة المختصة هي وزارة العلوم وتكنولوجيا المعلومات والاتصالات، لكن وزارة الداخلية والأمن، تبقى الوزارة المختصة المسؤولة عن المعلوماتية العامة، ومطلوب منها أيضا المشاركة كمحور مركزي عند وضع خطة التنفيذ بموجب قانون الإطار بشأن المعلومات الذكية، وبالتالي فإن تعاون وزارة الداخلية والأمن أمر لا مفر منه في ظل النظام القانوني الحالي من أجل تشغيل قانون الإطار بشأن الذكاء الاصطناعي بشكل صحيح.[52]

[52] المستشار بانغ سوك-هو، "خصائص القانون الأساسي للذكاء الاصطناعي، والتحديات التشريعية المستقبلية، وتداعياتها على الشركات"، تاريخ النشر: 14 يناير 2025، باللغة الكورية، على موقع صحيفة قانونية 75 -المجلة الوحيدة للمهنة القانونية التي تأسست عام 1950: https://www.lawtimes.co.kr/LawFirm-NewsLetter/204689، تاريخ الاضطلاع: 2025/06/30، على الساعة 00:40 مساء.

ثالثا: مضامين مشروع قانون الذكاء الاصطناعي بكوريا الجنوبية

أقرت لجنة العلوم والتكنولوجيا والمعلومات والإذاعة والاتصالات في الجمعية الوطنية، مشروع القانون بشأن "القانون الأساسي لتطوير الذكاء الاصطناعي وإنشاء قاعدة ثقة" في الجلسة العامة المنعقدة في 26 نوفمبر 2024 .

يعد القانون الأساسي للذكاء الاصطناعي بديلا أعدته اللجنة الفرعية لمراجعة قانون المعلومات والاتصالات والإذاعة التابعة لوزارة الدفاع الوطني من خلال دمج وتنسيق 19 مشروع قانون مقدم إلى الجمعية الوطنية الثانية والعشرين بحلول 21 نوفمبر 2024، ومن المقرر أن يخضع لعملية مراجعة النظام والصياغة من قبل لجنة التشريع والقضاء في الجمعية الوطنية وعملية مداولات الجلسة العامة.

ينص مشروع القانون الأساسي للذكاء الاصطناعي على البنود التالية لدعم التنمية السليمة لصناعة الذكاء الاصطناعي والتنظيم الذاتي للصناعة:

يقوم وزير العلوم وتكنولوجيا المعلومات والاتصالات بإنشاء خطة أساسية للذكاء الاصطناعي، وإنشاء لجنة وطنية للذكاء الاصطناعي تحت إشراف الرئيس، وتعيين مركز لسياسة الذكاء الاصطناعي، وتوفير الأساس لتشغيل معهد أبحاث سلامة الذكاء الاصطناعي؛ تقديم الدعم للصناعات ذات الصلة لتطوير وتفعيل تكنولوجيا الذكاء الاصطناعي ووضع أسس لوضع المعايير المتعلقة بتكنولوجيا الذكاء الاصطناعي؛ وإنشاء وإعلان "مبادئ أخلاقيات الذكاء الاصطناعي"، ودعم أنشطة التحقق والشهادات المستقلة للمنظمات ذات الصلة بالذكاء الاصطناعي لضمان سلامة وموثوقية الذكاء الاصطناعي، وإنشاء أساس لإنشاء لجنة أخلاقيات مستقلة خاصة بالذكاء الاصطناعي.

بالإضافة إلى ذلك، ينص مشروع قانون الذكاء الاصطناعي الأساسي أيضا على التزامات مختلفة لمشغلي أعمال الذكاء الاصطناعي، كما ينص على أن مشغل أعمال الذكاء الاصطناعي، الذي هو موضوع التطبيق، هو الشخص الذي يدير أعمالا مرتبطة بصناعة الذكاء الاصطناعي، ويقسمه إلى فئتين (المادة 2، الفقرة 7) مشغل أعمال تطوير الذكاء الاصطناعي، ومشغل أعمال مستخدمي الذكاء الاصطناعي.

يعرف "نظام الذكاء الاصطناعي" بأنه نظام قائم على الذكاء الاصطناعي يستنتج نتائج مثل التنبؤات والتوصيات والقرارات التي تؤثر على البيئات الحقيقية والافتراضية بمستويات مختلفة من الاستقلالية والقدرة على التكيف لتحقيق هدف معين، وعليه، فمن الضروري النظر فيما إذا كان هذا التعريف ينطبق على القانون الأساسي المقترح بشأن الذكاء الاصطناعي، في هذه الأثناء، على الرغم

من أن مشروع قانون الذكاء الاصطناعي الأساسي لا يميز بين التزامات مطوري الذكاء الاصطناعي ومستخدمي الذكاء الاصطناعي، إلا أن هناك احتمالا بأن يتم تقديم لوائح تميز طبيعة العمل في المستقبل من خلال المراسيم الرئاسية، لذلك من الضروري مراقبة هذا.

يتضمن مشروع القانون المؤطر للذكاء الاصطناعي أحكاما للتطبيق خارج الإقليم، وينص على أنه حتى لو تم تنفيذ فعل في الخارج، يمكن تطبيق المشروع إذا كان يؤثر على السوق المحلية أو المستخدمين (المادة 4) وبالإضافة إلى ذلك، ولضمان فعاليته، يتم إدخال نظام الوكيل المحلي التالي (المادة 36).

التزامات الشركات المتعلقة بالذكاء الاصطناعي عالي التأثير بحيث تم التعريف بالذكاء الاصطناعي عالي التأثير (الفقرة 4 من المادة 2)، ثم الالتزامات المتجسدة في الالتزام بالمراجعة المسبقة (المادة 33)، واجب الإخطار المسبق (الفقرة 1 من المادة 31) في حالة المخالفة، سيتم فرض غرامة تصل إلى 30 مليون وون (البند 1 من الفقرة 1 من المادة 43)، الالتزام بتنفيذ تدابير السلامة والموثوقية (المادة 34)، وتقييم الأثر (المادة 35)، والحق في طلب التوضيح (الفقرة 4 من المادة 3).

عند تقديم الذكاء الاصطناعي عالي التأثير أو المنتجات أو الخدمات التي تستخدمه، قد تخضع لالتزامات مختلفة، مثل الالتزام بتقديم إشعار مسبق والالتزام بتنفيذ تدابير السلامة والموثوقية، وعلاوة على ذلك، فإن توفير الذكاء الاصطناعي عالي التأثير للمؤسسات العامة قد يفرض في الواقع التزاما بإجراء تقييم للأثر وقد يفرض أيضا التزاما بالرد على طلبات المستخدمين للحصول على تفسيرات للنتائج التي يولدها الذكاء الاصطناعي، إذا كانت الشركة تقدم ذكاء اصطناعيا عالي التأثير أو منتجا أو خدمة تستخدمه، فقد تخضع لأنظمة مختلفة مثل تلك المذكورة أعلاه، لذا من الضروري مراجعتها بعناية مسبقا.

يفرض مشروع القانون الأساسي للذكاء الاصطناعي التزامات مختلفة على مشغلي الأعمال المتعلقة بالذكاء الاصطناعي الذين يعتزمون تقديم المنتجات أو الخدمات باستخدام الذكاء الاصطناعي التوليدي.، بحيث تم التعريف بالذكاء الاصطناعي التوليدي (الفقرة 6 من المادة 2)، ثم قدم الالتزامات المتمثلة في واجب الإخطار المسبق (الفقرة 1 من المادة 31) في حالة المخالفة، سيتم فرض غرامة تصل إلى 30 مليون وون (البند 1 من الفقرة 1 من المادة 43)، التزام الإشارة (الفقرة 2 من المادة 31)، والتزييف العميق (الفقرة 4 من المادة 31)

عند تقديم المنتجات أو الخدمات باستخدام الذكاء الاصطناعي التوليدي، قد تكون مسؤولا عن التزامات الإشعار المسبق والعرض، وبالنسبة لما يسمى بالتزييف العميق، فقد تكون مسؤولا عن

التزامات الإشعار أو العرض المنفصلة والمعززة، إذا كانت الشركة تستخدم الذكاء الاصطناعي التوليدي، فإنها تحتاج إلى مراجعته عن كثب مسبقا.

يتطلب مشروع قانون الذكاء الاصطناعي الأساسي من مشغلي أعمال الذكاء الاصطناعي مجموعة من الالتزامات (1) تحديد المخاطر وتقييمها والتخفيف منها طوال دورة حياة الذكاء الاصطناعي، (2) إنشاء نظام لإدارة المخاطر لمراقبة الحوادث المتعلقة بالذكاء الاصطناعي، والاستجابة لها، وتقديم نتائج هذا التنفيذ إلى وزير العلوم وتكنولوجيا المعلومات والاتصالات (المادة 32).

بناء على ما تقدم فإن الالتزامات التي المذكورة في الفقرة السابقة مماثلة لتلك المنصوص عليها في قانون الذكاء الاصطناعي للاتحاد الأوروبي، الذي دخل حيز التنفيذ في أغسطس/آب الماضي، وقانون الابتكار الآمن والمضمون لنماذج الذكاء الاصطناعي الرائدة، والذي صدر في كاليفورنيا لكن لم يتم إقراره أبدا بسبب حق النقض الذي يتمتع به الحاكم.

بناء على ذلك، من المتوقع أن يكون نطاق تطبيق هذا النظام محدودا، ولكن بما أنه قد يفرض التزامات قوية في الحالات التي يطبق فيها، فمن الضروري انتظار صدور مرسوم رئاسي مستقبلي يحدد نطاق التطبيق، كما ينص مشروع قانون الإطار بشأن الذكاء الاصطناعي على سلطة وزير العلوم وتكنولوجيا المعلومات والاتصالات.

من المتوقع أن يكون مشروع القانون الأساسي للذكاء الاصطناعي بكوريا أول قانون ينظم بشكل مباشر صناعة الذكاء الاصطناعي ومنتجاته وخدماته باعتباره التشريع الأساسي لعصر الذكاء الاصطناعي، ومن المتوقع أن يكون له تأثير واسع النطاق على كل من مطوري ومستخدمي الذكاء الاصطناعي، لذلك، إذا كانت الشركة تدير خدمة مرتبطة بالذكاء الاصطناعي أو شركة تستخدم الذكاء الاصطناعي، فمن المعتقد أنه من الضروري الاهتمام بقانون الذكاء الاصطناعي الأساسي المقترح ومواصلة مراقبة جدول مداولات الجمعية الوطنية واتجاهات المناقشات حول مرسوم التنفيذ.[53]

---

[53] *لجنة العلوم والدفاع في الجمعية الوطنية تقر مشروع قانون الذكاء الاصطناعي الأساسي*، تاريخ النشر: 04 ديسمبر 2024، النشرة الإخبارية، باللغة الكورية على موقع KIM & CHANG: https://www.kimchang.com/ko/insights/detail.kc?sch_section=4&idx=30837، تاريخ الاضطلاع: 2025/06/30، على الساعة 00:41 مساء.

الفقرة الثالثة: الإطار القانوني لحالة التوحيد القياسي ضمن إمكانية الوصول وراحة المستخدم بكوريا الجنوبية

قامت المؤسسات الإدارية والعامة المحلية، بتطوير وتوزيع العديد من الأدلة في الماضي للتطبيق الفعال لمفاهيم إمكانية الوصول وراحة المستخدم (UI/UX)، ويتم بناء أنظمة المعلومات العامة لأسباب "المصلحة العامة"، بدءا بقانون الحكومة الإلكترونية على وجه الخصوص:

- المادة 59 (التوحيد القياسي من مرسوم إنفاذ القانون نفسه، إرشادات الامتثال لتوافق خدمات الحكومة الإلكترونية).
- بالإضافة إلى المعلوماتية الذكية، المادة 46 من القانون الأساسي (ضمان الوصول إلى خدمات المعلومات الذكية واستخدامها للأشخاص ذوي الإعاقة وكبار السن وغيرهم)، والمادة 49 من نفس القانون (سد الفجوة المعلوماتية).

تعقيبا على ما سبق، فمن خلال إضفاء الطابع المؤسسي على المعايير وحل فجوة المعلومات، تم توضيح أهمية إمكانية الوصول وراحة المستخدم (UI/UX) في جميع القنوات التي تقدم الخدمات العامة كالتزام قانوني ومع ذلك، بدلا من تحديد معايير فنية دقيقة، يتم تقديم الإشعارات التنظيمية الإيجابية والمبادئ التوجيهية أو الأدلة لتوفير إمكانية الوصول (الويب وكذلك الهاتف المحمول)، حيث تم بذل الجهود لتحسين راحة المستخدم (UI/UX).[54]

يوفر الدليل الإرشادي المعنون ب "إرشادات إدارة جودة مواقع الحكومة الإلكترونية" معلومات مفصلة عن طرق تشخيص مراقبة الجودة بناء على سبعة جوانب تتعلق بجودة موقع الويب، (توافق الويب/ إمكانية الوصول إلى الويب/ توفير الوقت/ انفتاح الويب/ توفير الراحة/ موثوقية الويب، كلها تمثل محتويات إدارة مراقبة جودة مواقع الحكومة الإلكترونية) حتى يتمكن الجميع من الاستمتاع بنفس التجربة والمزايا.

تعد الجمعية الكورية لتكنولوجيا الاتصالات (TTA)، المنظمة الوحيدة لتوحيد معايير تكنولوجيا المعلومات والاتصالات في كوريا، كما يقوم المعهد الوطني للتكنولوجيا والمعايير بوضع وتقديم المعايير المتعلقة بإمكانية الوصول، وهو منظمة وطنية للمعايير الصناعية.[55]

---

[54] سون سونغ هيون، مرجع سابق.

[55] بارك تاي-غيون، إرشادات التوزيع والاستخدام لواجهة المستخدم وتجربة المستخدم لمواقع الحكومة الإلكترونية، غرفة بيانات معايير وإرشادات المعلومات، تاريخ النشر: 21 مارس 2019، على الموقع الرسمي لوزارة الداخلية والأمن بكوريا الجنوبية:

المطلب الثاني: الإطار التشريعي لتقنية السحابة والمرونة والثقة الصفرية

أعلنت وزارة العلوم وتكنولوجيا المعلومات والاتصالات عن "الخطة الأساسية الثالثة للحوسبة السحابية (2022-2024) في 6 سبتمبر 2021، بناء على "قانون تعزيز الحوسبة السحابية وحماية المستخدمين (قانون تطوير السحابة/ قانون الحوسبة السحابية)" الصادر في عام 2015 (الفقرة الأولى).

في حين لإدارة ذكية مرنة تم استخدام Agile وهي طريقة لتطوير البرمجيات تهدف إلى تطوير برامج قابلة للتشغيل وتوفيرها بشكل مستمر من خلال التكرار السريع، ولكنها منظور يتجه إلى التعاون وسير العمل بدلا من مجموعة من اللوائح التي تحدد العمل المطلوب لتطوير البرمجيات، وهي عملية تنظيمية، أقرب إلى "نظام القيم الذي يوجه الاختيارات حول ما يجب صنعه وكيفية صنعه، في نفس سياق Agile تم تقديم DevOps[56] بوتيرة سريعة جدا مؤخرا، سرعة تطوير البرمجيات بالمقارنة مع الأساليب الحالية.

باعتبارها متعلقة بالبيانات قانونيا ونظاما أي كل من Agile وDevOps، فقد سنت الدولة ما مجموعه 9 قوانين تخضع لسلطة 6 وكالات، بما في ذلك قانون البيانات العامة كقوانين متعلقة بالبيانات، تم سنه وتنقيحه، بما في ذلك قانون البيانات العامة، وقانون إدارة البيانات والقانون الإطار بشأن المعلومات الذكية وقانون صناعة البيانات والقانون الرقمي الصناعي، إضافة إلى أن هناك قانون تعزيز التحويل، وقانون المعايير الوطنية، وقانون حماية المعلومات الشخصية، وقانون شبكة المعلومات والاتصالات، وقانون المعلومات الائتمانية، من بينها قانون صناعة البيانات، (صدر في 19 أكتوبر 2021) لعرض إنشاء أساس لتطوير صناعة البيانات، بما في ذلك خلق قيمة اقتصادية من البيانات (الفقرة الثانية).

ظهر نموذج Zero trust وهو نموذج جديد لشبكة الأمان المقترح ليكون آمنا من مثل هذه الهجمات السيبرانية، وتعتمد الثقة المعدومة على الفرضية الأساسية التي تقول "لا أحد موثوق به"، عند الوصول إلى منطقة خاصة داخلية من منطقة عامة خارجية، حتى المستخدمين المصرح لهم أو حركة

---

https://www.mois.go.kr/frt/bbs/type001/commonSelectBoardArticle.do?bbsId=BBSMSTR_00000000004
5&nttId=69451، تاريخ الاطلاع : 2025/06/07، على الساعة 02:41 صباحا.

[56] DevOps ، باللغة الكورية على موقع ويكيبيديا : https://ko.wikipedia.org/wiki/devops، تاريخ الاطلاع : 2025/06/07، على الساعة 02:41 صباحا.

مرور الشبكة لا يتم الثقة بهم بشكل غير مشروط، ويتم الموافقة عليهم من خلال التحقق الذي يضمن السلامة.

تكمن أهمية بنية الثقة المعدومة في الابتعاد عن النموذج الأمني الحالي القائم على المحيط، حيث يكون الوصول إلى الموارد أو البيانات داخل الحدود غير مؤكد، للانتقال إلى نموذج أمن تكنولوجيا المعلومات الذي "لا يثق في الحدود أو أي شيء خارج الحدود" (الفقرة الثالثة).

الفقرة الأولى: الإطار القانوني للسحابة الأصلية

سنعمد إلى التعرف على الإطار العام والقانوني للسحابة بالمغرب (أولا)، والسياسة الرئيسية للحوسبة السحابة (ثانيا)، وإطارها القانوني (ثالثا).

أولا: السحابة

من أجل تسريع التحول الرقمي وتعزيز نمو القطاع الرقمي الوطني، تم اعتماد عدد من المحفزات ووضعها في صلب الاستراتيجية الوطنية أبرزها استخدام الخدمات الرقمية السحابية وذلك عن طريق تشجيع الإدارات والمؤسسات العمومية والمقاولات الى اللجوء الى استخدام هذه التكنولوجيا في حال الاستعانة بمصادر خارجية لإدارة نظم المعلومات.[57]

أ- الإطار العام للسحابة

تجدر الإشارة إلى أنه على الرغم من وجود العديد من الفاعلين الذين يقترحون خدمات إيواء المعطيات بواسطة التكنولوجيا السحابية، يظل العرض الوطني في هذا المجال موجها أساسا لتلبية الاحتياجات الاعتيادية والمألوفة (خدمات إيواء المواقع والمعطيات، والبنية التحتية الأساسية، إلى جانب بعض التطبيقات الأكثر تداولا)، وذلك دون أن يشمل أنواعا أخرى من خدمات التطبيقات والخدمات ذات القيمة المضافة العالية (البرمجيات).

من جهة أخرى ثمة عوامل متعددة يمكنها أن تفسر هذه الوضعية، نذكر منها: سوق وطني محدود، نظرا لضعف ترسيخ ثقافة التكنولوجيا السحابية، تكاليف مرتفعة نسبيا للربط بالإنترنت، الخصاص في الموارد البشرية المؤهلة، والتأخر المسجل على مستوى تنزيل تصنيف المعطيات حسب مستوى

---

[57] نشر المرسوم رقم 2.24.921 المتعلق بلجوء الهيئات والبنيات التحتية ذات الأهمية الحيوية المتوفرة على نظم معلومات حساسة أو معطيات حساسة إلى مقدمي الخدمات الرقمية السحابية بالجريدة الرسمية، على الموقع التالي: https://www.dgssi.gov.ma/ar/actualites/nshr-almrswm-rqm-224921-almtlq-bljw-alhyyat-walbnyat-althtyt-dhat-alahmyt-alhywyt ، بتاريخ: 2025/06/29، على الساعة 22:16 مساء.

حساسيتها، كما ينص على ذلك القانون 05.20 المتعلق بالأمن السيبراني والمرسوم الصادر بتطبيقه، ويظل هذا التصنيف أساسيا لاختيار البنيات التحتية الأكثر ملاءمة لكل صنف حسب درجة حساسية هذه المعطيات.

ب- الإطار القانوني للسحابة بالمغرب

هناك تشريعات عامة تطبق على الحوسبة السحابية بالمغرب بما في ذلك قانون الأمن السيبراني رقم 20-05 الذي ينظم حماية المعطيات الحساسة والمرسوم الصادر بتطبيقه، بالإضافة إلى قوانين أخرى تركز على حماية البيانات الشخصية تتمثل في قانون حماية الأشخاص الذاتيين لمعالجة المعطيات ذات الطابع الشخصي08-09، ولا يوجد قانون خاص بالحوسبة السحابية بالمغرب.

ثانيا: السياسة الرئيسية حول الحوسبة السحابية بكوريا الجنوبية

يهدف قانون تعزيز الحوسبة السحابية وحماية المستخدمين (اختصارا: قانون الحوسبة السحابية) إلى تعزيز تطوير واستخدام الحوسبة السحابية وخلق بيئة يمكن فيها استخدام خدمات الحوسبة السحابية بأمان، مما يساهم في تحسين حياة الناس وتنمية الاقتصاد الوطني.

الحوسبة السحابية: وفقا لـ "قانون تعزيز الحوسبة السحابية وحماية المستخدمين"، فإنها تشير إلى نظام معالجة المعلومات الذي يسمح بالاستخدام المرن لموارد المعلومات والاتصالات مثل أجهزة المعلومات والاتصالات المتكاملة والمشتركة، ومرافق المعلومات والاتصالات، والبرمجيات من خلال شبكة المعلومات والاتصالات وفقا للتغيرات في احتياجات المستخدم أو مطالبه.

يتضمن القانون بين جنباته أحكاما من بينها تتعلق بتفعيل خدمات الحوسبة السحابية وشهادة الأمان لتكنولوجيا الحوسبة السحابية، وتتمثل المحتويات الرئيسية فيما يلي: تشجيع استخدام خدمات الحوسبة السحابية الخاصة من قبل الجهات الحكومية والحكومات المحلية والمؤسسات العامة (المادة 20 من قانون الحوسبة السحابية)، ويتم تحديد أساس شهادة أمن خدمات الحوسبة السحابية وإلغائها في القانون (المادتان 23-2 و23-3 من قانون الحوسبة السحابية) من ناحية أخرى تنص هاته الأحكام في القانون بشكل مباشر على المسائل المتعلقة بشهادة الأمن وإلغائها بهدف تعزيز إنشاء نظام تكنولوجيا الحوسبة السحابية والمسائل المتعلقة بأمن المعلومات.[58]

[58] قانون تعزيز الحوسبة السحابية وحماية المستخدمين (المختصر باسم قانون الحوسبة السحابية)، [دخل حيز التنفيذ في 31 يناير 2025] [القانون رقم 20732، 31 يناير 2025، المعدل جزئيا]، على موقع المركز الوطني للمعلومات القانونية بوزارة التشريع الحكومي، موقع رسمي للحكومة الإلكترونية لجمهورية كوريا الجنوبية:

في المقابل أعلنت وزارة العلوم وتكنولوجيا المعلومات والاتصالات عن "الخطة الأساسية الثالثة للحوسبة السحابية (2022-2024) في 6 سبتمبر 2021[59]، بناء على "قانون تعزيز الحوسبة السحابية وحماية المستخدمين (قانون تطوير السحابة/ قانون الحوسبة السحابية)" الصادر في عام 2015، وتهدف هذه الخطة إلى تعزيز القدرة التنافسية في الصناعة السحابية من خلال أولوية استخدام السحابة الخاصة في القطاع العام، والتحول السحابي في صناعة البرمجيات السحابية، والتحول الرقمي لجميع الصناعات، واقترحت تعزيز وإنشاء نظام بيئي سحابي يمكنه دعم البيانات والذكاء الاصطناعي.

من خلال "الاستراتيجية الرقمية لكوريا" التي تم الإعلان عنها في مؤتمر الطوارئ الثامن للاقتصاد وسبل العيش الذي ترأسه الرئيس جمهورية كوريا في 28 سبتمبر 2022، تعمل على تعزيز الاستخدام اليومي للسحابة في القطاعين العام والخاص، تسعى هذه الاستراتيجية إلى تعزيز تطوير تقنيات المصدر لتأمين تكنولوجيا الذكاء الاصطناعي ذات المستوى العالمي، وخلق بيئة لدمج البيانات العامة والخاصة، وتجميعها وتوزيعها واستخدامها.

لتحقيق هذه الغاية، تم القيام بترويج "مشروع مشاركة الموارد المستندة إلى الإنترنت" حيث يمكن ربط خدمات الذكاء الاصطناعي بشكل عضوي على أساس مركز بيانات سحابي عالي السرعة، ومنخفض الطاقة مبني على أشباه موصلات الذكاء الاصطناعي المحلية، وتوسيع النطاق بالكامل سوق البرمجيات مع التركيز على SaaS، حيث يتم التخطيط لإعادة تنظيم وتعزيز أكثر من 2000 شركة SaaS بحلول عام 2027.[60]

ثالثا: الإطار القانوني للسحابة بكوريا الجنوبية

لكي تتمكن المؤسسات العامة من بناء أنظمة المعلومات والاتصالات الخاصة بها، يجب أن تخضع للتحقق من الملاءمة الأمنية وفقا للمادة 4 من قانون جهاز المخابرات الوطنية، والمادة 56 من قانون الحكومة الإلكترونية وفقا لآراء خبرائهم بكوريا الجنوبية، من أجل تحسين مستوى أمان المعلومات الوطنية وشبكة الاتصالات.

---

https://www.law.go.kr/lsInfoP.do?lsId=012266&ancYnChk=0#0000، تاريخ الاطلاع: 2025/07/05، على الساعة 20:50 مساء.

[59] *الخطة الأساسية الثالثة للحوسبة السحابية (22~24)*، مرجع سابق.

[60] [مباشر] الرئيس يون سوك يول، الاجتماع الطارئ الثالث والعشرون للاقتصاد وسبل عيش الشعب، يدعوا إلى "تخفيف العبء، وزيادة الحيوية"، باللغة الكورية على يوتيوب: https://www.youtube.com/watch?v=tRUJSY2Qz4E، تاريخ الاطلاع: 2025/06/30، على الساعة 00:41 صباحا.

من أجل بناء نظام سحابي، يجب أن تقدم منتجات إدارة المحاكاة الافتراضية منتجات تم إصدار شهادة وظيفة أمان لها، كما يجب أن تخضع للتحقق من الملاءمة بعد التقديم، ومع ذلك، يجب تحقيق الأمان، ويمكن حذف التحقق الاصطناعي.

إضافة إلى ما سبق، يجب على المؤسسات العامة الحفاظ على مستوى حماية المعلومات وفقا للمادة 23-2 من قانون تعزيز الحوسبة السحابية وحماية المستخدمين، ومن أجل التحسين والضمان، يمكن استخدام الخدمات السحابية العامة الخاصة التي تلبي معايير شهادات الأمان.

بمعنى آخر، من أجل توفير الخدمات السحابية العامة والخاصة للمؤسسات العامة يجب استخدام الوكالة الكورية للإنترنت والأمن كهيئة اعتماد، إذ يجب الحصول على شهادة أمان الخدمة السحابية (CSAP)، تشمل الخدمات الخاضعة للشهادة Daas، وSaaS، وIaaS.

يتم تصنيف مستويات الأمان على أنها عالية ومتوسطة ومنخفضة، مع تعيين جهة التقييم/الاعتماد وفقا لقانون الحوسبة السحابية، جهة الاعتماد: وكالة الإنترنت والأمن الكورية كما ذكرنا سابقا، وجهة التقييم: جمعية تعزيز المعلومات والاتصالات الكورية، معهد تقييم تكنولوجيا المعلومات الكوري، شركة ضمان النظام الكورية المحدودة.[61]

إذا تمت مخالفة قانون الحوسبة السحابية بكوريا الجنوبية تقع الجزاءات التالية كما يلي: يعاقب بالسجن مدة لا تزيد على 5 سنوات أو بغرامة لا تتجاوز 50 مليون وون كل من استخدم معلومات المستخدم أو قدمها لطرف ثالث دون موافقته أو كل من تلقى معلومات المستخدم لأغراض الربح أو غير لائقة مع علمه بعدم موافقة المستخدم (المادة 35).

كما يعاقب بالحبس مدة لا تزيد على ثلاث سنوات أو بغرامة لا تتجاوز ثلاثين مليون وون كل من أفشى أسرارا علم بها أثناء قيامه بعمل موكل إليه (المادة 36).

وفقا للمادة 37 التي اقتصرت على الغرامات يعاقب بغرامة لا تزيد على 10 ملايين وون كل من ارتكب أيا من الجرائم التالية: الشخص الذي يعرض علامة شهادة أمنية أو علامة مماثلة، الشخص الذي يفشل في إخطار المستخدمين بحدوث خرق أمني أو تسرب معلومات المستخدم أو انقطاع الخدمة، الشخص الذي يفشل في الإبلاغ عن حدوث تسرب لمعلومات المستخدم إلى وزير العلوم

[61] شهادة أمان خدمة السحابة (CSAP)، على الموقع الرسمي لوكالة الإنترنت والأمن الكورية KISA: https://isms.kisa.or.kr/main/csap/intro/ ، تاريخ الاضطلاع: 2025/09/10، على الساعة 21:27 مساء.

وتكنولوجيا المعلومات والاتصالات، الشخص الذي لا يقوم بإعادة أو إتلاف معلومات المستخدم، الشخص الذي يفشل في الامتثال لأمر الإيقاف أو الأمر التصحيحي.

بالتالي يفرض وزير العلوم وتكنولوجيا المعلومات والاتصالات الرسوم الإضافية ويجمعها وفقا للقرار الرئاسي.[62]

الفقرة الثانية: الإدارة الذكية لموارد المعلومات في بيئة مرنة

بشكل مختصر سنتعرف على النظام المتكامل لإدارة البيانات للحصول على خدمات بيانات عالية الجودة وإطارها القانوني، فوفقا لأحكام المادة 27 من الدستور المغربي، والقانون 31.13 المتعلق بالحق في الوصول إلى المعلومات، يحدد كليهما نطاق الحق في الوصول إلى المعلومات التي تحتفظ بها الإدارات العامة والمؤسسات والهيئات المنتخبة التي تقدم الخدمة العامة، وكذلك شروط وإجراءات ممارسة هذا الحق، وبالتالي يمكن القول بأن المغرب أطر قانونيا لإدارة البيانات في الجانب المرتبط في الحصول عليها، أما في إطار الحماية القانونية للبيانات الشخصية فمؤطر بقانون رقم 08-09.

من أجل تحقيق خدمة *بياناتي* بكوريا الجنوبية، هناك حاجة إلى أساس قانوني يتطلب من صاحب المعلومات إرسال معلوماته بطلب منه، وبالتبع فكل من قانون معالجة الشكاوى المدنية وقانون الحكومة الإلكترونية، هما اللذان يحكمان المعلومات في القطاع العام، مع توفير أساس قانوني ينص على "الحق في الطلب".

تم تقديم "*بياناتي*" في القطاع العام لأول مرة من خلال "خطة تعزيز الابتكار في الحكومة الرقمية" في أكتوبر 2019، وتستهدف المؤسسات الإدارية والعامة المرتبطة بشبكة الحكومة الإلكترونية العامة *My Data*، ومعظم المعلومات التي يتم الكشف عنها هي معلومات عن شهادات مختلفة يمكن إصدارها عبر الانترنت، مما يجعل تعزيز عبء الأمن الإداري بسرعة ممكنا، والبيانات في حد ذاتها ليست معلومات مفيدة للاستفسار أو التحليل المتكامل، ولكنها مرتبطة بخدمات وتستخدم كمعلومات يجب إثباتها علنا.

من الناحية المتعلقة بمراجعة القوانين العامة لتعزيز "*بياناتي*" في كافة المجالات، فنظرا لأن الحق في نقل المعلومات الشخصية هو حق أساسي لصاحب المعلومات، فهو مرتبط بقانون حماية المعلومات الشخصية، وهو قانون عام يتعلق بالمعلومات الشخصية تم التوصل إلى توافق في الآراء بشأن ضرورة تنظيم المحتويات يناير 2021، ومن أجل ضمان الاتساق في الاتجاه القانوني

---

[62] قانون تعزيز الحوسبة السحابية وحماية المستخدمين بكوريا الجنوبية، مرجع سابق.

والمؤسسي، منصوص على حق نقل المعلومات الشخصية في قانون حماية المعلومات الشخصية، ويتم تنظيم التفاصيل التي تأخذ في الاعتبار خصائص كل مجال من خلال الإخطار من قبل الوزارات المختصة في كل صناعة.[63]

أدت حقبة عدم الاتصال التي سببتها جائحة فيروس كورونا في أوائل عام 2020، إلى زيادة استخدام تكنولوجيا المعلومات والاتصالات بشكل كبير، بالإضافة إلى زيادة استخدام أنظمة العمل عن بعد، ومؤتمرات الفيديو، والوثائق الإلكترونية، والذكاء الاصطناعي، ويؤدي الاستخدام المتزايد للتقنيات الرقمية الجديدة مثل السحابة إلى طرق جديدة لتطوير وتقديم البرامج، مثل: Agile[64]، كما أن DevOps[65] هي ثقافة تعمل على تحسين قدرة المؤسسة على تقديم التطبيقات والخدمات بوتيرة سريعة، كما تبتكر DevOps المنتجات بشكل أسرع من المؤسسات التي تستخدم عمليات تطوير البرامج وإدارة البنية التحتية التقليدية، وبالتالي سنتعرف على الإطار التشريعي لهاته التقنيات المختزلة في إدارة ذكية مرنة.

في الإطار القانوني بشأن تكنولوجيا المعلومات الذكية[66]، يتم تعريف تكنولوجيا المعلومات الذكية وفقا للمادة 2 على أنها "التكنولوجيا التي تنفذ التعلم والاستدلال والحكم من خلال الأساليب الإلكترونية"، أو تم تعريفه على أنه يشير إلى تقنية الجمع والاستخدام، وبناء على ذلك في هذا التقرير، تعتبر موارد المعلومات الذكية هي تكنولوجيا المعلومات الذكية، ونود تعريفها على أنها مصدر معلومات يتم استخدامه أو الاعتماد عليه، وكمفهوم لإدارة ذلك، قدمت مجلة أبحاث المعلومات نموذج عمل لإدارة موارد المعلومات الذكية.

---

[63] جاي دو لي، مرجع سابق.

[64] highsmith, J. Agile Project Mangement, Addison- Wesley, 2010, Retrieved from: https://www.researchgate.net/publication/234809670_Agile_Project_Management_Creating_Innovative_Products, accessed 06 june 2025 – 00 :44pm.

[65] DevOps, JFrog, URL: https://jfrog.com/devops-tools/what-is-devops/, (2025.06.30 – 00 :44pm 방문).

[66] القانون الأساسي بشأن المعلومات الذكية، [تاريخ النفاذ: 27 مارس 2025] [القانون رقم 20410، 26 مارس 2024، التعديل الجزئي]، على موقع المركز الوطني للمعلومات القانونية بوزارة التشريع الحكومي، موقع رسمي للحكومة الإلكترونية لجمهورية كوريا الجنوبية: https://www.law.go.kr/lsInfoP.do?lsId=000028&ancYnChk=0#0000 ، تاريخ الاطلاع: 2025/09/10، على الساعة 22:10 مساء.

تتطلب تقنية Agile فهما ونهجا على مستوى الإستراتيجية الوطنية للتحول الرقمي الفعال، مثل: سنغافورة، بدلا من اتباع نهج على مستوى منهجية برمجية أولية، ولذلك، من أجل إدارة موارد المعلومات الذكية القائمة على أساس مرن يلزم فهم سياق وعلاقات تقنيات العناصر الأساسية الشاملة (البيانات، الذكاء الاصطناعي، السحابة).

باعتبارها قانونا ونظاما متعلقة بالبيانات، فقد سنت الدولة ما مجموعه 9 قوانين تخضع لسلطة 6 وكالات، بما في ذلك قانون البيانات العامة كقوانين متعلقة بالبيانات، تم سنه وتنقيحه، بما في ذلك قانون البيانات العامة، وقانون إدارة البيانات والقانون الإطار بشأن المعلومات الذكية وقانون صناعة البيانات والقانون الرقمي الصناعي، إضافة إلى أن هناك قانون تعزيز التحويل، وقانون المعايير الوطنية، وقانون حماية المعلومات الشخصية، وقانون شبكة المعلومات والاتصالات، وقانون المعلومات الائتمانية، من بينها قانون صناعة البيانات، (صدر في 19 أكتوبر 2021) لعرض إنشاء أساس لتطوير صناعة البيانات، بما في ذلك خلق قيمة اقتصادية من البيانات.

في الوقت نفسه، أدخلت الحكومة وعززت هندسة تكنولوجيا المعلومات كسياسة موحدة لتعزيز المعلوماتية، في عام 2000 تم إنشاء معيار النموذج المفاهيمي للبنية التقنية ومعيار إطار عمل البنية المؤسسية للقطاع العام في عام 2003 لتوحيد المفاهيم والإطار الأساسي، بالإضافة إلى ذلك، هناك نموذج مرجعي يستخدم على مستوى الحكومة ولكنه معيار منفصل، ولا توجد حركة حتى الآن لتفعيله.[67]

بالنظر إلى الاتجاهات الحديثة لتكنولوجيا البيانات، فإن تكنولوجيا البيانات مدمجة مع تقنيات رقمية أخرى مثل الذكاء الاصطناعي في عصر المعلومات الذكي، وهناك اتجاهات مثل تعزيز التعقيد، والبيانات والامتثال للمعايير، والحاجة إلى ربط البيانات واستخدامها، والاهتمام بقيمة البيانات والمعاملات، ومع ذلك، نظرا لتشتت القوانين والمؤسسات المتعلقة بالبيانات، على الرغم من وجود الترتيبات المؤسسية، فإن عملية الحوكمة صعبة بسبب ملكية البيانات والأدوار والمسؤوليات، (R&R)في الربط الفعلي للبيانات ومشاركتها وتكاملها، هناك أيضا احتمال كبير بحدوث ذلك، ولذلك، هناك حاجة إلى فحص الكفاءة التشغيلية لنظام إدارة البيانات على المستوى الوطني.

كما أن هناك حاجة إلى المراجعة، بالإضافة إلى أن الحكومة ستضع وتعزز معايير وتدابير تنفيذ الموثوقية في تطوير واستخدام ونشر الذكاء الاصطناعي في 21 مايو، ذكاء اصطناعي جدير بالثقة،

[67] سون سونغ هيون، مرجع سابق.

للذكاء الاصطناعي الذي يركز على الإنسان لتحسين القبول العام للذكاء الاصطناعي، حيث تم إعداد استراتيجية التنفيذ (مسودة)، يشمل بحسب مراحل تطبيق منتجات وخدمات الذكاء الاصطناعي في القطاع الخاص (التطوير/ التحقق/ الاعتماد) الشركات، المطورين، إذ تم تقديم معايير ومنهجية لضمان الثقة التي يمكن للأطراف الثالثة الرجوع إليها لتحقيق الموثوقية.

في مرحلة "تطوير" هذه المنهجية، يتم إنتاج وتوزيع "دليل التطوير" الذي يمكنه التحقق من القوانين والأنظمة والأخلاقيات والمتطلبات الفنية المحلية والأجنبية المتعلقة بالموثوقية في وقت واحد، في مرحلة "التحقق"، يتم إعداد وتقديم "نظام التحقق" مثل إجراءات وعناصر وطرق التحقق لتأكيد وتقييم ما إذا كانت الموثوقية قد تم تأمينها وفقا لدليل التطوير ومستواه، في مرحلة "الاعتماد"، يتم الترويج لإصدار الشهادات والإفصاح الطوعي الخاص للمنتجات والخدمات التي تلبي المتطلبات الفنية والأخلاقية والتي اجتازت نظام التحقق، وبالنظر إلى الخطة الأساسية الثالثة للحوسبة السحابية، يعتقد أنه سيكون هناك مجال كبير للتحسين في خدمات النظام الأساسي المستقبلية.[68]

الفقرة الثالثة: الإطار العام والتشريعي لنموذج الثقة المعدومة جدير بالثقة

سنعمل على التعرف على نموذج الثقة المعدومة جدير بالثقة ويمكن الاعتماد عليه (أولا)، والتوجه التي تسير فيه كوريا الجنوبية وإطارها التشريعي (ثانيا).

أولا: الإطار العام للمنصة الرقمية للحكومة ذات الثقة المعدومة

حتى وقت قريب استمرت سرعة الإنترنت وتطور تكنولوجيا المعلومات في التغير والتطور بمعدل سريع ومذهل، مع هذا يتسارع التحول الرقمي إلى ما بعد الثورة الصناعية الرابعة، مع تطبيق التقنيات الجديدة للثورة الصناعية الرابعة (الذكاء الاصطناعي، والبيانات الضخمة، والتوأم الرقمي، والمحتوى الواقعي، والسحابة) في حياتنا تدريجيا، حيث أصبح العالم أكثر دراية بالوسائل الرقمية.

في الوقت نفسه هناك تهديدات مستمرة للفضاء السيبراني الرقمي، مثل: القرصنة، لذا فإنه ولتكون الشبكات آمنة من هذه التهديدات السيبرانية، هناك حاجة ملحة لتهيئة البيئة، يمكن أن تحدث الهجمات السيبرانية ليس فقط في تقنيات تكنولوجيا المعلومات الحالية، ولكن أيضا في الحالة غير المستقرة في بداية إدخال التكنولوجيا الجديدة، إنهم يهاجمون عندما يحين الوقت المناسب.

---

[68] بارك هي وون، دراسة حالة حول تطبيق إطار عمل Agile القائم على التعلم في مشاريع تكنولوجيا المعلومات واسعة النطاق، وقائع مؤتمر الكمبيوتر الكوري، 2016.

يتزايد الضرر الناجم عن الهجمات السيبرانية المختلفة بسرعة، على وجه الخصوص، مع انتشار استخدام الأجهزة المحمولة مثل إنترنت الأشياء والسحابة، فإن عدد التهديدات السيبرانية يتزايد تدريجيا، ويمكن أن تتسبب المعلومات التي يتم الحصول عليها عن طريق سرقة الحسابات الشخصية في فقدان البيانات من خلال الهجمات السيبرانية مثل تسرب المعلومات السرية الداخلية للشركات وللمؤسسات العامة وتدمير البيانات، وتحدث الأضرار الثانوية والثالثية مثل الخسارة والتسرب، وكذلك الخسارة المالية، بشكل متتابع، مما يؤدي إلى تجاوز حجم الضرر وشدته الخيال.

ظهر نموذج Zero trust وهو نموذج جديد لشبكة الأمان المقترح ليكون آمنا من مثل هذه الهجمات السيبرانية، وتعتمد الثقة المعدومة على الفرضية الأساسية التي تقول لا أحد" موثوق به"، عند الوصول إلى منطقة خاصة داخلية من منطقة عامة خارجية، حتى المستخدمين المصرح لهم أو حركة مرور الشبكة لا يتم الثقة بهم بشكل غير مشروط ويتم الموافقة عليهم من خلال التحقق الذي يضمن السلامة.[69]

نظرا لأن استخدام الأجهزة الذكية أصبح أكثر شيوعا، يمكن للبرامج الضارة مثل برامج الفدية أن تتسلل إلى الأجهزة المحمولة الفردية، كما أن حالات إساءة الاستخدام التي تؤدي إلى تسرب المعلومات تتزايد تدريجيا، وبشكل رئيسي يصيب التعليمات البرمجية الضارة لتسريب المعلومات الشخصية ومعلومات المطلعين/ مديري المؤسسة أو الشركة المستهدفة، ثم يسرق معلومات المصادقة للوصول إلى الأنظمة الداخلية الرئيسية، مما يتسبب في تدمير النظام وتسرب المعلومات وبرامج الفدية بسبب القرصنة، ثم يؤدي إلى أضرار مثل إساءة استخدام الأموال[70].

ثانيا: الإطار التشريعي بشأن نموذج الثقة المعدومة

في كوريا، تحققت الحاجة إلى استراتيجية أمنية جديدة في مجال الأمن السيبراني، وبدأت وزارة العلوم وتكنولوجيا المعلومات والاتصالات في عام 2022، Zero Trust هي مجموعة بحثية للتحول في نموذج الأمن السيبراني، تتألف من خبراء أمنيين من الحكومة والمؤسسات العامة والصناعة

---

[69] Kerman, A. Zero Trust Cybersecurity : Never Trust, Always Verify, 2020.08.28, NIST, Retrieved from: https://www.ncsc.gov.uk/collection/zero-trust-architecture, accessed 06 june 2025 - 00 :47pm.

[70] كيم سون-آي، هجوم سلسلة التوريد 1: أضرار جسيمة ناجمة عن هجمات سلسلة التوريد، تاريخ النشر: 2021/11/01، على موقع NetworkTIMS: https://www.datanet.co.kr/news/articleView.html?idxno=165985، تاريخ الاطلاع: 2025/09/13، على الساعة 14:47 مساء.

والأوساط الأكاديمية، وجرى إنشاء لجنة فرعية جديدة ولجنة فرعية لسلسلة توريد البرمجيات لإعداد التدابير اللازمة لوضع السياسات.

كما أن أمن تطوير البرمجيات العامة يقوم على تعزيز قدرات الوقاية من التهديدات السيبرانية المحتملة والاستجابة لها من خلال التشخيص المسبق والقضاء على نقاط ضعف أمن البرامج، والتي تعد السبب الرئيسي لانتهاكات الأمن، منذ مرحلة التطوير، وذلك من قبل وكالة الانترنت والأمن الكورية بتشخيص ثغرات أمن البرمجيات ودعم السياسات للمؤسسات الإدارية والعامة، ويرجع الأساس القانوني لذلك وفقا للمادتين 24 و45 من قانون الحكومة الإلكترونية، المبادئ التوجيهية لبناء وتشغيل أنظمة المعلومات الإدارية ونظم المعلومات للمؤسسات العامة.[71]

المبحث الثاني: الإطار القانوني والمؤسساتي للأمن السيبراني بين التحديات الأمنية والإشكالات التشريعية كوريا الجنوبية واليابان نموذجا

عرفت المادة 2 من قانون الأمن السيبراني المغربي رقم 20-05 الأمن السيبراني بأنه: "مجموعة من التدابير والإجراءات ومفاهيم الأمن وطرق إدارة المخاطر والأعمال والتكوينات وأفضل الممارسات والتكنولوجيات التي تسمح لنظام معلومات أن يقاوم أحداثا مرتبطة بالفضاء السيبراني، من شأنها أن تمس بتوفر وسلامة وسرية المعطيات المخزنة أو المعالجة أو المرسلة والخدمات ذات الصلة التي يقدمها هذا النظام أو تسمح بالولوج إليه".

وفقا للتقرير الجديد لسنة 2024 الذي أصدره مؤخرا الاتحاد الدولي للاتصالات (UIT)، فقد سجل المغرب تقدما على مستوى تحسين أمنه السيبراني، إذ أصبح مصنفا ضمن المجموعة الأولى (المستوى 1) إلى جانب 45 دولة أخرى، وتضم هذه المجموعة البلدان الرائدة التي أظهرت التزاما واضحا بقضايا الأمن السيبراني وفق المعايير الخمس.

يتكون قانون رقم 20-05 للأمن السيبراني بالمغرب من 53 مادة موزعة على ستة فصول وهي: الفصل الأول: أحكام عامة، الفصل الثاني: إجراءات حماية نظم المعلومات، الفصل الثالث: حكامة

[71] حماية البنية التحتية الرقمية، على موقع وكالة الإنترنت والأمن الكورية KISA: https://www.kisa.or.kr/ ، تاريخ الاطلاع: 2025/09/13، على الساعة 14:53 مساء.

الأمن السيبراني، الفصل الرابع: التكوين والتحسيس والتعاون الفصل الخامس: معاينة العقوبات والمخالفات الفصل السادس: أحكام ختامية.

في الإطار ذاته ينص هذا القانون، على مجموعة من تدابير الأمان ذات الطبيعة التنظيمية والتقنية التي تهدف إلى تعزيز القدرات الوطنية في مجال الأمن السيبراني، وتنسيق جهود الوقاية والحماية من الهجمات والحوادث المتعلقة بالأمن السيبراني، ويحدد هذا القانون كما جاء في المادة 1: قواعد ومقتضيات الأمن المطبقة على نظم معلومات إدارات الدولة والجماعات الترابية والمؤسسات والمقاولات العمومية وكل شخص اعتباري آخر خاضع للقانون العام؛ قواعد ومقتضيات الأمن المطبقة على البنيات التحتية ذات الأهمية الحيوية؛ قواعد ومقتضيات الأمن المطبقة على مستغلي الشبكات العامة للمواصلات ومزودي خدمات الإنترنت ومقدمي خدمات الأمن السيبراني ومقدمي الخدمات الرقمية وناشري منصات الإنترنت؛ والإطار الوطني لحكامة الأمن السيبراني.

بالمقابل ينحصر الأمن السيبراني بكوريا الجنوبية في القيم الدستورية المتعلقة بالسلامة الوطنية وسلامة المواطنين، وضمان الحقوق الأساسية، وسيادة القانون، والسلم الدولي، ويمكن القول بأنه تجسيد لهذه القيم، إذ يجسد استراتيجية استجابة حديثة للأمن الوطني لحماية الدستور، نشر مكتب الأمن القومي التابع للبيت الأزرق "الاستراتيجية الوطنية للأمن السيبراني" في أبريل 2019.

تتكون "الاستراتيجية الوطنية للأمن السيبراني" من الأهداف والمبادئ الأساسية والمهام الاستراتيجية وخطط التنفيذ، في حالة كوريا الجنوبية، فإن الأمن السيبراني هو نظام مزدوج حيث ينظم المرسوم الرئاسي "لوائح إدارة الأمن السيبراني الوطنية" القطاع العام بشكل مباشر، ويتم تنظيم القطاع الخاص من خلال "قانون تعزيز استخدام شبكة المعلومات والاتصالات وحماية المعلومات".

نتيجة للانتشار الواسع للهجمات الإلكترونية بغض النظر عن القطاع العام أو الخاص، تحدث أضرار اقتصادية هائلة، ومن أجل صد الهجمات الإلكترونية التي تهدد الأمن القومي بسرعة وتقليل الأضرار، تم إنشاء اللجنة الوطنية للأمن السيبراني، وتم تكليف المنظمات المسؤولة بمسؤولية حماية الفضاء الإلكتروني ضمن اختصاص الوكالات الحكومية والحكومات المحلية والمؤسسات التي تمتلك أو تدير التقنيات ذات الأهمية الوطنية.

في نفس المسار تم اقتراح "قانون الأمن السيبراني الوطني" كتشريع حكومي في يناير 2017 لإنشاء مسائل متعلقة بتنظيم وتشغيل الأمن السيبراني بكوريا الجنوبية بشكل منهجي، مثل تبادل معلومات التهديد السيبراني، واكتشاف الهجمات السيبرانية والرد عليها، والإبلاغ عن الحوادث الناجمة عن الهجمات السيبرانية والتحقيق فيها، ومع ذلك، فإن التقدم التشريعي يمر حاليا بمرحلة

بطيئة، وتشمل أسباب ذلك، أولا: المشكلة المزمنة المتمثلة في تحويل الجمعية الوطنية لتشريعات الأمن السيبراني إلى نقاش سياسي، وثانيا: المخاوف بشأن انتهاكات الخصوصية، وثالثا: وجهات النظر المتضاربة حول دور جهاز الاستخبارات الوطني (المطلب الأول).

بالمقابل أعلنت نقابة المحامين اليابانية في عام 2003، عن مشروع قانون يتكون من سبعة فصول وأحكام تكميلية إلى جانب بيان رأي يطلب إصدار القانون الأساسي للأمن المعلوماتي،[72] وعلى الرغم من ذلك، لم تصدر اليابان قانونا أساسيا في مجال الأمن السيبراني لفترة طويلة، ولكنها أنشأت منظمات ذات صلة ونفذت سياسات وفقا للقانون الأساسي بشأن تشكيل مجتمع شبكات المعلومات والاتصالات المتقدمة الصادر في نوفمبر 2000، وهو القانون الأساسي في مجال المعلوماتية.[73]

جوهر هذا القانون هو إنشاء مجلس سياسة الأمن المعلوماتي ومركز الأمن المعلوماتي، وتعزيز السياسات ذات الصلة التي تركز على هذه المنظمات، بالإضافة إلى ذلك، تم اتخاذ التدابير اللازمة في مجال الأمن السيبراني، مثل معاقبة أولئك الذين ارتكبوا أعمالا غير قانونية بناء على قانون حظر الوصول غير المصرح به، إلخ.

مع تزايد الهجمات السيبرانية، اقترحت "استراتيجية الأمن القومي" التي أُعلن عنها في عام 2013 تعزيز الأمن السيبراني، واقترحت "مخطط خطة الدفاع" الذي أُعلن عنه في نفس الوقت الاستجابة في الفضاء الإلكتروني كأحد وسائل الردع والاستجابة الفعالة لمختلف المواقف، ومع ذلك، فقد تم تحليل أن دورة الألعاب الأولمبية والبارالمبية في طوكيو الذي تم عقدها في عام 2020 كانت بمثابة عامل مباشر في تسليط الضوء على الحاجة إلى سن قانون أساسي في مجال الأمن السيبراني.

مع الاعتراف بأن هذا النوع من تدابير الأمن السيبراني له حدود،[74] سنت اليابان "القانون الأساسي للأمن السيبراني" بتاريخ 12 نوفمبر/تشرين الثاني 2014، الذي ينص على مسؤوليات كل كيان فيما يتعلق بالأمن السيبراني، ويعد هذا القانون بمثابة قانون أساسي في مجال الأمن السيبراني ويعزز فعالية الأمن السيبراني.

تجدر الإشارة إلى التأثيرات الستة التالية للقانون الأساسي للأمن السيبراني في اليابان، أولا، لقد سنت اليابان قوانين أساسية في مجال الأمن السيبراني منذ فترة طويلة؛ ثانيا، فهو يقلل الاعتماد على القواعد غير الصارمة ويتوافق مع مبدأ سيادة القانون؛ ثالثا، لقد أسست قاعدة قانونية لتعزيز الأمن

---

[72] بارك سانغ دون، مرجع سابق، صفحة 148.

[73] كيم جاي كوانج، مرجع سابق، ص 43.

[74] بارك سانغ دون، مرجع سابق، صفحة 149.

السيبراني على مستوى البلاد بناء على أيديولوجية أساسية؛ رابعا، رفعت مكانة المنظمة العامة للأمن السيبراني وشرعت لها؛ خامسا، خلقت بيئة تسمح لعامة الجمهور بالمشاركة من خلال ضمان الشفافية في أنشطة تعزيز الأمن السيبراني؛ وسادسا، أعلنت مشاركتها الفعالة في تشكيل نظام دولي للأمن السيبراني.[75]

بالإضافة إلى الآثار الستة المذكورة أعلاه، هناك ثلاثة آثار إضافية تتعلق بالخلفية التشريعية، أولا، كانت نقابة المحامين، وهي منظمة تابعة للقطاع الخاص وليست الحكومة، هي التي طلبت سن القانون في عام 2003، وعادة ما تكون القوانين المتعلقة بالأمن السيبراني تشريعات تقودها الحكومة في الغالب، لكن تبقى حالة اليابان فريدة من نوعها حيث لم يكن هذا هو الحال الطبيعي والعادي لمصدر التشريع لقانون بالأهمية تلك، ثانيا، كانت الزيادة في الهجمات الإلكترونية متناسبة مع التشريع المتعلق بهذا الموضوع، ثالثا، تم حل المخاوف الأمنية المتعلقة بالأحداث الدولية واسعة النطاق (دورة الألعاب الأولمبية والبارالمبية في طوكيو 2020) من خلال التشريعات[76]، إلا أننا سنعمل على السياق العام لقانون الأمن السيبراني باليابان والمتغيرات التي طرأت عليه (المطلب الثاني).

المطلب الأول: الإطار التشريعي والمؤسساتي للأمن السيبراني بين التجربة المغربية المتقدمة والتجربة الكورية المعقدة

يعرف الأمن السيبراني على أنه عبارة عن مجموع الوسائل التقنية والإدارية التي يتم استخدامها لمنع الاستخدام غير المصرح به وسوء الاستغلال واستعادة المعلومات الالكترونية ونظم الاتصالات والمعلومات التي تحتويها بهدف توافر واستمرارية عمل نظم المعلومات وتأمين حماية وسرية وخصوصية البيانات الشخصية لحماية المواطنين.[77]

بالمقابل ينحصر الأمن السيبراني بكوريا الجنوبية في القيم الدستورية المتعلقة بالسلامة الوطنية وسلامة المواطنين، وضمان الحقوق الأساسية، وسيادة القانون، والسلم الدولي، ويمكن القول بأنه تجسيد لهذه القيم، أما كقانون لحد عام 2025 لازالت كوريا بدون قانون للأمن السيبراني على الرغم من أن هناك مشروع قانون لم يصادق عليه لاعتبارات سياسة وخصوصية، إلا أنها تتطلع لذلك في عام 2026، وصوب عينيها قانون الأمن السيبراني الياباني، بمعنى أنه من المتوقع أن يكون قانون

---

[75] بارك سانج دون، نفس المرجع، ص 161-165."

[76] كيم جاي كوانغ، مرجع سابق.

[77] عدنان مصطفى البار، أمن المعلومات والأمن السيبراني، ص: 8، مقال منشور بالموقع الإلكتروني: www.kau.edu.sa، بتاريخ: 2025/06/29، على الساعة 22:17 مساء.

الأمن السيبراني الأساسي في اليابان مرجعا مهما لإصدار قانون الأمن السيبراني الأساسي في كوريا الجنوبية[78] (الفقرة الثانية).

الفقرة الأولى: الإطار القانوني للأمن السيبراني

سنتعرف على الطبيعة الإدارية لقانون الأمن السيبراني والمشاكل التي تواجهها بكوريا الجنوبية (أولا)، ثم الإطار المؤسساتي لها بكل من المغرب وكوريا الجنوبية (ثانيا)، وكذا الإحاطة بمضامين قانون الأمن السيبراني بالمغرب، مع ذكر أسباب التشريع للوائح الأمن السيبراني بكوريا الجنوبية ومحتوياتها (ثالثا)، إضافة إلى فهم العلاقة المتبادلة بين الأمن السيبراني والخصوصية (رابعا).

أولا: الطبيعة الإدارية لقانون الأمن السيبراني والمشاكل التي يواجهها بكوريا الجنوبية

يمكن اعتبار الأنشطة الخاصة بالأمن السيبراني بما في ذلك الوقاية والكشف والاستجابة والاسترداد وجميع الأنشطة المصاحبة، التي تقوم بها المنظمات ذات الصلة، لمنع انتهاكه من خلال التهديدات من الوسائط الإلكترونية أو التهديدات الناتجة عن استخدام الأساليب الإلكترونية، بمثابة إجراءات إدارية، والقوانين التي تشكل الأساس لهذه الأنشطة هي ذات طبيعة إدارية أكثر من القانون الجنائي، لا يمكن القول بأن قانون التنظيم الإداري الحالي في النظام القانوني للأمن السيبراني كاف، وعلى وجه الخصوص، يمكن اعتبار قانون الإجراءات الإدارية أكثر من سابقه في عدم كفايته.

بما أن القوانين المتعلقة بالأمن السيبراني لم يتم تطويرها بشكل كاف، فإن السلطة المعيارية لضمان تنفيذ السياسات لم يتم تشكيلها بشكل كاف، وعلى وجه الخصوص، كانت فعالية سياسات الأمن السيبراني على الجمهور محدودة، وقد تم بالفعل الكشف عن مشاكل هذه القضايا وقضايا مماثلة فيما يتصل بحماية البنية التحتية للمعلومات والاتصالات.

قبل سن قانون شبكة المعلومات والاتصالات، قامت المنظمات ذات الصلة بأعمال حماية البنية التحتية للمعلومات والاتصالات بناء على أحكام قانون تنظيم الحكومة، وقانون جهاز المخابرات الوطني، ولوائح العمل الأمني، وتم فرض العقوبة على المخالفات وفقا لقانون العقوبات، وقانون شبكة المعلومات والاتصالات، وأحكام أخرى، ومع ذلك، بسبب عدم وجود نظام لأنشطة الحماية العملية مثل تقييم نقاط الضعف، وإنشاء تدابير الحماية وخطط الحماية، والاستجابة لاختراقات الأمن، لم يكن

[78] كيم جاي كوانج، مرجع سابق، ص 145-177.

النظام فعالا في تأمين سلامة البنية التحتية للمعلومات والاتصالات، وهو الهدف النهائي من أعمال حماية البنية التحتية للمعلومات والاتصالات.[79]

تظهر هذه التجارب السابقة أنه من الصعب إرساء الحوكمة في أي مجال باستخدام قوانين التشغيل الإداري وقوانين التنظيم الإداري للمجالات المماثلة فقط بدلا من قوانين التشغيل الإداري للمجال المعني،[80] يمكن القول أن مجال الأمن السيبراني، الذي يتميز بخصائص تختلف عن حماية المعلومات العامة بسبب علاقته الوثيقة بالأمن القومي، في وضع مماثل للوضع الذي تم فيه وضع حماية البنية التحتية للمعلومات والاتصالات قبل سن قانون حماية البنية التحتية للمعلومات والاتصالات بكوريا الجنوبية.

أشار البعض إلى أن النظام القانوني الحالي فيما يتعلق بالأمن القومي يعتمد بشكل أساسي على فرضية الأمن القومي من خلال القوة المادية التقليدية، وأن هناك نقصا كبيرا في الأنظمة القانونية لحماية المواطنين الأفراد والمجتمع والنظام الوطني من التهديدات السيبرانية.[81]

تتمثل المشاكل المحددة التي تم تحديدها في هذا النقد فيما يلي:

أولا: لا يوجد نظام لتنظيم التحليل والتقييم الشامل للمعلومات على المستوى الوطني - كوريا الجنوبية.

ثانيا: لا يوجد نظام قادر على خلق تأثيرات التآزر الوطني من خلال تبادل المعلومات بين الإدارات فحسب، بل إن الوكالة المسؤولة عن الأمن القومي لم تمنح حق الوصول إلى الإخطارات والبيانات الخام.

ثالثا: هناك نقص في الأساس القانوني لاتخاذ تدابير فعالة للتعامل مع التهديدات السيبرانية، إذ لا يوجد قانون فعال لمنع مختلف أشكال الهجمات السيبرانية أو الاستجابة للمخاطر الفعلية.[82]

إذا أخذنا في الاعتبار أن الحاجة إلى أنشطة الأمن السيبراني ليست صغيرة، وخاصة في القطاع الخاص اليوم، فمن الممكن أن نرى أن هناك حاجة كبيرة إلى قانون للإجراءات الإدارية يشمل الأمور

---

[79] *البحث الأساسي حول سن قانون حماية شبكة المعلومات والاتصالات* (أبحاث السياسات 00-12) (معهد أبحاث سياسات المعلومات والاتصالات، 2000)، ص 49 وما يليها.

[80] بارك سانج دون، "دراسة في القانون العام حول تحسين حوكمة الأمن السيبراني"، مجلة القانون العام، المجلد 17، العدد 4 (الجمعية الكورية للقانون العام المقارن، 2016)، ص 359.

[81] جونغ جون هيون، "مراجعة لقانون الأمن السيبراني الوطني في مجتمع المعلومات المتقدمة"، مجلة دراسات القانون، المجلد 37، العدد 2 (معهد أبحاث القانون بجامعة دانكوك، 2013)، ص 462.

[82] جونغ جون هيون، نفس المرجع، ص 466-467.

المتعلقة بأنشطة الكيانات الخاصة، اليوم، لم يعد الفضاء الإلكتروني مجرد فضاء افتراضي؛ لقد تحولت إلى مساحة حيث تتحقق الحياة الحقيقية.

بما أن الإنترنت يعمل كشبكة عصبية، فإن التهديدات التي يتعرض لها القطاع الخاص في الفضاء الإلكتروني يمكن أن تنتقل إلى القطاع العام، والعكس صحيح، وفي بعض الحالات، قد يؤثر الضرر على كامل أراضي الدولة،[83] وبعبارة أخرى، فإن الأمن السيبراني هو قضية يجب معالجتها ليس فقط في القطاع العام ولكن أيضا في القطاع الخاص.

وفقا لمفهوم الدولة الضامنة، تضمن الدولة حل المهام الوطنية، ولكن هذا الضمان لا يتحقق بالضرورة من خلال قيام الدولة بتنفيذ المهام بمفردها، ولكن يمكن تنفيذه من خلال حلول طوعية من قبل كيانات خاصة، بحيث في دولة الضمان، تمنح القواعد القانونية الكيانات الخاصة سلطة تفويض تنفيذ المهام أو التنظيم الذاتي، مع تقديم الأهداف والمعايير اللازمة لتنفيذ المهام والتنظيم الذاتي، لذلك، فإن نقل تنفيذ المهام إلى القطاع الخاص وتعزيز الدور الاستراتيجي للدولة يصبحان عنصرين أساسيين في دولة الضمان.

بمعنى آخر، يمكن نقل أداء المهام إلى القطاع الخاص، ولكن الدولة لا تترك كل شيء للقطاع الخاص وتتراجع، بل تتخذ التدابير اللازمة لتنظيم الأنشطة الخاصة وتنظيمها بشكل صحيح، لذلك، ليس من الضروري أن تقوم الدولة بتنفيذ المهام الوطنية بشكل مباشر، وقد يكون هناك أشخاص غير الدولة مسؤولون عن أداء المهام، وقد يكون مديرو المهام هؤلاء شركات أو مؤسسات عامة خاضعة لسيطرة الدولة، أو أشخاصا اعتباريين أو أشخاصا ذاتيين خاضعين للقانون الخاص، ومن ناحية أخرى، فإن تنفيذ المهام العامة، وهي مفهوم يشمل المهام الاجتماعية بالإضافة إلى المهام الوطنية، لا يشترط إشراف الدولة، وهناك حالات لا يمكن تنفيذها إلا في غياب إشراف الدولة.[84]

رغم أنه لا يمكن القول على وجه اليقين بأن مفهوم الدولة الأمنية أصبح منتشرا على نطاق واسع اليوم، فإنه لا يمكن إنكار وجود عناصر مهمة للدولة الأمنية، وهناك أيضا أنشطة يمكن للقطاع

---

[83] بارك سانج دون، "دراسة حول المسؤولية الوطنية عن البنية التحتية للمعلومات والاتصالات"، أطروحة دكتوراه، جامعة سونغ كيون كوان، 2016، ص 181 وما يليها.

[84] هونغ سوك هان، "دراسة حول التنظيم الذاتي المنظم وفقا لتغيرات دور الدولة - مع التركيز على مجال حماية المعلومات الشخصية-"، أطروحة دكتوراه، جامعة سونغ كيون كوان، 2008، ص 74، على موقع مكتبة الجمعية الوطنية الكورية: https://docviewer.nanet.go.kr/reader/viewer ، تاريخ الاطلاع: 2025/09/13، على الساعة 16:10 مساء.

الخاص القيام بها للحفاظ على الأمن الوطني من خلال حماية المعلومات والاتصالات، على سبيل المثال: يشمل ذلك أنشطة اكتشاف التهديدات التي تقوم بها شركات مراقبة الأمن.[85]

لذلك، فإن حماية المعلومات والاتصالات هي قضية يجب على جميع أعضاء المجتمع الاجتماعي الانتباه إليها،[86] وفي السياق نفسه، يتطلب الأمن السيبراني أيضا مشاركة واهتمام جميع أعضاء المجتمع الاجتماعي، وحتى إذا كان موضوع أو صاحب المصلحة في النشاط ذي الصلة ينتمي إلى القطاع الخاص، فلا يمكن للدولة استبعاد الإجراء الإداري المتمثل في تنظيمه وبشكل مناسب، ومن ثم هناك حاجة في كوريا الجنوبية إلى قانون للإجراءات الإدارية ينظم بشكل كاف الإجراءات الإدارية المتعلقة بالأمن السيبراني، بيد أنها تحتاج أيضا إلى قانون للتنظيم الإداري ينسجم مع مثل هذا القانون للإجراءات الإدارية.

ثانيا: الإطار المؤسساتي في قانون الأمن السيبراني

سوف نتناول التنظيم الإداري للأمن السيبراني بالمعنى الواسع، وبناء على ذلك، حتى لو لم تكن تتعامل بشكل مباشر مع الأمن القومي، فإننا نود أن نطرح دورها كمنظمة إدارية للأمن السيبراني إذا لم نتمكن من استبعاد إمكانية أهميتها، بكوريا الجنوبية وقبلها المغرب.

أ- الإطار المؤسساتي وهيئات حكامة الأمن السيبراني بالمغرب

1. اللجنة الاستراتيجية للأمن السيبراني: تم إحداث اللجنة الاستراتيجية للأمن السيبراني (المسماة سابقا باللجنة الإستراتيجية لأمن نظم المعلومات (DGSSI)) بموجب القانون رقم 20 -05، وهي السلطة المسؤولة بالأساس عن إعداد التوجهات الاستراتيجية للدولة في مجال الأمن السيبراني والسهر على ضمان صمود نظم معلومات الهيئات والبنى التحتية ذات الأهمية الحيوية والمتعهدين.

---

[85] هونغ سيونغ مان، "استكشاف مجتمع المخاطر والعلنية: التركيز على حالات تسرب الماء والإشعاعات"، مجلة دراسات السياسة الكورية، المجلد 13، العدد 2 (جمعية الإدارة العامة في كيونغين، 2013)، ص 122، على موقع (GIAPA): https://giapa.or.kr/journal_article/%EC%9C%84%ED%97%98%EC%82%AC%ED%9A%8C%EC%9/9%80-%EA%B3%B5%EA%B3%B5%EC%84%B1-%ED%83%90%EC%83%89/، تاريخ الاطلاع: 2025/09/13، على الساعة 16:19 مساء.

[86] كيم جاي كوانغ، مرجع سابق.

2. لجنة إدارة الأزمات والأحداث السيبرانية الجسيمة: تم إحداث هذه اللجنة لدى اللجنة الاستراتيجية للأمن السيبراني، وهي مكلفة بضمان تدخل منسق في مجال الوقاية وتدبير الأزمات على إثر وقوع حادث أو حوادث أمن سيبرانية.[87]
3. الوكالة الوطنية الوكالة الوطنية لتقنين المواصلات (ANRT): مؤسسة عمومية مكلفة بتنظيم وتقنين قطاع المواصلات، أحدثت الوكالة طبقا للقانون رقم 96-24 المتعلق بالبريد والمواصلات، كما تم تغييره وتتميمه بمقتضى القانون رقم 55-01، الذي رسم الخطوط العامة لإعادة تنظيم القطاع، من خلال سلطتها المتعلقة بالتنظيم القانوني، تتولى تحقيق الدعم اللازم لدينامية السوق التنافسية، كما تتولى الوكالة سلطة التنظيم التقني للقطاع حيث تقوم بإعداد المعايير، إضافة إلى أنها تمتلك سلطة التنظيم الاقتصادي لقطاع المواصلات، بحيث تتبع تطور السوق ولها حق التدخل في حالة ملاحظة أي خلل أو مساس بالمقتضيات الجاري بها العمل.[88]
4. المركز المغربي للأبحاث متعددة التقنيات والابتكار (CMRPI): هو عبارة عن جمعية علمية مغربية، تعمل في مجال البحث والتطوير والابتكار وهي غير ربحية، تأسست في يونيو 2012، ومهمتها تتمثل في جمع الأفراد والكيانات القانونية المعنية بالعلم والتكنولوجيا في العديد من مجالات الصناعة والبحث العلمي، وتسهيل مشاركة الباحثين المغاربة، من داخل البلاد وخارجها، في المساهمة في تنمية المغرب، وتشجيع التواصل المتكرر مع الأعضاء الآخرين، في تخصصاتهم أو خارج تخصصاتهم، وخاصة بالنسبة للأعضاء الأصغر سنا، وتمثيل جميع أعضائها أمام الجمعيات العلمية والتقنية الأخرى المغربية أو الأجنبية، ...، كما يرتبط نشاط المركز المغربي للبحث والابتكار ارتباطا وثيقا بالبحث التطبيقي في مجال التقنيات المتقدمة، كما يتواصل المركز بشكل وثيق مع الإدارات والهيئات الحكومية.[89]
5. المقر الاستراتيجي للأمن السيبراني: وهو المركز الوطني للابتكار في الأمن السيبراني (CIC)، يقع مقره داخل المدرسة الوطنية العليا للمعلوميات وتحليل النظم (ENSIAS) التابعة لجامعة محمد الخامس بالرباط، والذي يهدف المركز إلى تعزيز البحث والتطوير والتدريب في مجال

---

[87] حميد بحكاك، حميد بحكاك يكتب: المغرب والأمن السيبراني الإطار التشريعي والمؤسساتي والاستراتيجي، تاريخ النشر: 17 أكتوبر 2024 - 0:00، موقع حزب العدالة والتنمية: https://h1.nu/10hs-، تاريخ الاطلاع: 2025/06/29، على الساعة 22:18 مساء.

[88] الوكالة الوطنية الوكالة الوطنية لتقنين المواصلات (ANRT)، على موقعها الرسمي: https://www.anrt.ma/ar/a-propos/presentation?csrt=17500348124919813617 ، تاريخ الاطلاع: 2025/09/15، على الساعة 18:36 مساء.

[89] Le Centre Marocain de Recherches Polytechniques et d'Innovation (CMRPI) : https://www.cmrpi.ma/cmrpi-v2/presentation-du-cmrpi/ , Date de consultation: 15/09/2025, 18 :54am.

الأمن السيبراني، ويسعى إلى بناء شراكات مع المؤسسات الأكاديمية والصناعية على المستويين الوطني والدولي.[90]

6. فرق التقنية للشرطة الوطنية: يتم تدريب فرق من المتخصصين في تحليل وتتبع الجرائم الرقمية ضمن وحدات الشرطة القضائية لمكافحة الجرائم الإلكترونية.[91]
7. مصلحة المركزية لمكافحة الجرائم المرتبطة بالتكنولوجيا الحديثة: تعمل هذه المصلحة كنقطة اتصال على مدار الساعة لاتفاقية بودابست الدولية، مما يعزز التعاون الدولي في مجال الجرائم الإلكترونية.[92]

ب- التنظيم الإداري في ظل قانون الأمن السيبراني بكوريا الجنوبية

1- إنشاء اللجنة الوطنية للأمن السيبراني

تعتبر اللجنة الوطنية للأمن السيبراني أعلى هيئة تداولية لسياسة الأمن السيبراني الوطنية، ويترأس اللجنة مدير الأمن الوطني، ويفسر أن هذا الأمر منصوص عليه في القانون ليعكس دور مدير الأمن الوطني، الذي يعمل حاليا بمثابة برج مراقبة للأمن السيبراني الوطني.

2- السلطات المسؤولة والوكالات الداعمة

الوكالات الحكومية والحكومات المحلية والمنظمات التي تمتلك وتدير التقنيات ذات الأهمية الوطنية وتتحمل الوكالات وغيرها مسؤولية حماية الفضاء الإلكتروني بشكل آمن تحت ولايتها القضائية باعتبارها وكالات مسؤولة، ويجوز لمدير جهاز الاستخبارات الوطني تعيين الوكالات أو المنظمات ذات القدرات الفنية لدعم الوكالات المسؤولة كوكالات داعمة (المادتان 6 و7).[93]

---

[90] عماد السعيدي، المغرب يطلق مركزا وطنيا للابتكار في الأمن السيبراني لتعزيز البحث والتطوير الرقمي، تاريخ النشر: 04 يونيو 2025، على موقع DETA FOUR العربية:
https://detafour.com/%D8%A7%D9%84%D9%85%D8%BA%D8%B1%D8%A8-%D9%8A%D8%B7%D9%84%D9%82-%D9%85%D8%B1%D9%83%D8%B2%D8%A7-%D9%88%D8%B7%D9%86%D9%8A%D8%A7-%D9%84%D9%84%D8%A7%D8%A8%D8%AA%D9%83%D8%A7%D8%B1-%D9%81%D9%8A/ ، تاريخ الاطلاع: 2025/09/15، على الساعة 17:48 مساء.

[91] دور السلطات المغربية في مكافحة الابتزاز الإلكتروني في المغرب، على موقع مكتب محاماة تهوم والصغير في الدار البيضاء:
https://ar.thoumetsghair.com/%D8%A7%D9%84%D8%A7%D8%A8%D8%AA%D8%B2%D8%A7%D8%B2-%D8%A7%D9%84%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A/ ، تاريخ الاطلاع: 2025/09/15، على الساعة 18:26 مساء.

[92] أنفاس بريس، هذه هي استراتيجية المديرية العامة للأمن الوطني في محاربة الجرائم الإلكترونية، تاريخ النشر: 10 نوفمبر 2019، على موقع أنفاس بريس: https://2cm.es/1a6fu ، تاريخ الاطلاع: 2025/09/15، على الساعة 18:16 مساء.

[93] تقرير مراجعة لجنة الاستخبارات في الجمعية الوطنية، صفحة 28، على الموقع الرسمي لافتتاح الجمعية الوطنية بكوريا الجنوبية:
https://watch.peoplepower21.org/index.php?mid=Committee&sangim=%EC%A0%95%EB%B3%B4#watch ، تاريخ الاطلاع: 2025/09/13، على الساعة 16:49 مساء.

3- معهد أبحاث الأمن السيبراني

يجوز لمدير جهاز المخابرات الوطني إنشاء معهد أبحاث للأمن السيبراني لبحث وتطوير السياسات والتقنيات اللازمة للأمن السيبراني، أو تعيين مؤسسة أو معهد تابع للمؤسسة المنشأة بموجب قوانين أخرى كمعهد أبحاث للأمن السيبراني بعد التشاور مع رؤساء الأجهزة الإدارية المركزية ذات الصلة (الفقرة 1 من المادة 9 من مشروع القانون)، يسمح مشروع القانون الحكومي لجهاز الاستخبارات الوطني بإنشاء أو تعيين "معهد أبحاث الأمن السيبراني"، والذي يبدو أنه يهدف إلى الاستعداد للحالات التي ينشأ فيها الطلب على الأبحاث على مستوى من المستحيل تلبيته من خلال تعيين معاهد بحثية أو التعاقد على الأبحاث مع معاهد بحثية خاصة في المستقبل.

4- مركز تبادل معلومات التهديدات السيبرانية

من أجل تبادل معلومات التهديدات السيبرانية، تم إنشاء مركز لتبادل معلومات التهديدات السيبرانية تحت إشراف مدير جهاز الاستخبارات الوطني، وتم تنظيم وتشغيل مجلس لتبادل معلومات التهديدات السيبرانية يتألف من المنظمات المسؤولة وخبراء القطاع الخاص (الفقرتان 1 و5 من المادة 12 من مشروع القانون)، مع تزايد تعقيد التهديدات السيبرانية، هناك دعوات لإنشاء نظام أكثر تحديدا لتبادل المعلومات المتعلقة بالتهديدات السيبرانية بين المؤسسات العامة والشركات الخاصة.

5- مركز التحكم الأمني للجهة المسؤولة

يجب على مدير جهاز الاستخبارات الوطني، من أجل الاستجابة السريعة والفعالة للهجمات الإلكترونية على الفضاء الإلكتروني الوطني، إنشاء وتشغيل نظام وطني للكشف عن الهجمات الإلكترونية والاستجابة لها بالتشاور مع رؤساء الوكالات الإدارية المركزية ذات الصلة، يجب على رؤساء الهيئات المسؤولة، وفقا للمرسوم الرئاسي، إنشاء وتشغيل منظمة (يشار إليها فيما يلي باسم "مركز التحكم الأمني") قادرة على اكتشاف وتحليل الهجمات الإلكترونية على الفضاء الإلكتروني الخاضع لولايتهم واتخاذ تدابير الاستجابة الفورية، أو اتخاذ تدابير مثل تكليف العمل بمركز التحكم الأمني الذي أنشأه ويديره رئيس هيئة مسؤولة أخرى (المادة 14 من مشروع القانون).

6- فريق التحقيق المشترك

نص مدير جهاز المخابرات الوطني على أنه عند إجراء تحقيق في حادث يستهدف وكالة مسؤولة في القطاع الخاص، فإنه/إنها يجب أن يقوم/تقوم بتشغيل فريق تحقيق مشترك يتألف من الوكالات الإدارية المركزية ذات الصلة، ووكالات التحقيق، ووكالات الدعم وفقا لأحكام المرسوم الرئاسي (الفقرة 4 من المادة 15 من مشروع القانون)، إذا أجرى فريق التحقيق المشترك تحقيقا إداريا وتحقيقا

جنائيا في نفس الوقت، فيجب تطبيق القوانين المعمول بها في كل منهما بشكل مختلف، ولكن من الممكن تجنب اللوائح الصارمة لقانون الإجراءات الجنائية من خلال طريق ملتو يسمى التحقيق الإداري تحت ذريعة التحقيق المشترك.

7- مقر الاستجابة للأزمات السيبرانية

إذا قرر رئيس وكالة مسؤولة عليا أن أيا مما يلي ينطبق على الفضاء الإلكتروني الخاضع لولايته القضائية، 1. إذا تم إصدار تحذير بمستوى أعلى من المستوى المنصوص عليه في المرسوم الرئاسي أو تحذير خاص بالقطاع؛ 2. إذا تم اعتبار الضرر الناجم عن هجوم إلكتروني خطيرا)، فيجوز له إنشاء وتشغيل مقر استجابة للأزمات الإلكترونية (يشار إليه فيما يلي باسم "مقر الاستجابة") حيث تشارك الوكالة المسؤولة ووكالة الدعم ووكالة التحقيق لاتخاذ تدابير على الفور مثل تحليل السبب والتحقيق في الحوادث والاستجابة للطوارئ واسترداد الأضرار الناجمة عن الهجمات الإلكترونية.

الفقرة الثانية: مضامين قانون الأمن السيبراني

عمد المشرع المغربي في إطار قانون 05.20 إلى تعريف الأمن السيبراني، يتضح إذا أن المشرع حاول قدر المستطاع أن يوسع في مفهوم الأمن السيبراني من خلال تسليط الضوء على كافة المعاني التي يمكن أن يستوعبها وذلك من شأنه أن يحد من التداخل الذي يمكن أن يحصل مع مجموعة من المفاهيم المتشابهة، وبهذا الصدد فإن المغرب لديه قانون للأمن السيبراني.

على عكس كوريا الجنوبية التي يعتمد قطاعها العام على لائحة إدارة الأمن السيبراني الوطنية، وهي توجيهات رئاسية، ويستثنى من نطاق التطبيق القطاعات الخاصة الأخرى غير الهيئات الإدارية والمؤسسات التشريعية والقضائية، وبالإضافة إلى ذلك، يواجه القطاع الخاص قيودا في الكشف عن علامات الهجمات الإلكترونية والاستجابة لها، ولذلك، ينبغي للحكومة والقطاع الخاص التعاون لإنشاء نظام استجابة منهجي وموحد على المستوى الوطني بكوريا، مما سيمكن من الكشف المبكر عن الهجمات السيبرانية والحجب المبكر لاحتمالية وقوع أزمة سيبرانية، وتعبئة القدرات الوطنية لكوريا في حال وقوع أزمة.[94]

أ- مضامين قانون الأمن السيبراني بالمغرب

1. نطاق الحماية التي يوفرها قانون الأمن السيبراني رقم 20-05

[94] كيم جاي كوانج، مرجع سابق، ص 145-177.

يختص القانون رقم 20-05 بتوفير الحماية في الفضاء السيبراني من كل الحوادث أو الجرائم التي قد يقصد بها أصحابها المساس بأنظمة المعلومات أو تغييرها أو التشويش على سيرها، وقد حدد المشرع الجهات المعنية بهذه الحماية التي يوفرها هذا القانون في الأنظمة المعلوماتية الخاصة بالفئات المشار إليها في المادة الأولى من القانون أعلاه، وتتحدد هذه الفئات في إدارات الدولة والجماعات الترابية والمؤسسات والمقاولات العمومية وكل شخص اعتباري أخر خاضع للقانون العام، والتي يشار إليهم في القانون ب "الهيئة".

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

تبعا لما سبق، فإن هذا القانون يهدف إلى توفير الحماية لبنية المعلوماتية الخاصة بالمؤسسات العامة للدولة، أي بالمصالح الإستراتيجية للدولة، خاصة وأن المرحلة الحالية يغلب عليها لامادية المعطيات والبيانات، وبالتالي فالمساس بهذه المعطيات يعتبر مساسا بأسرار الدولة ومؤسساتها.

على مختلف البنيات والخدمات الحيوية للبلاد التي ستحدد بنص تنظيمي من قبل الجهات المختصة، كما تشمل أيضا القطاع الخاص المتمثلين في الشركات العاملة في مجال استغلال الشبكات العامة للاتصال ومقدمي خدمات الأمن السيبراني وبصفة عامة كل الجهات التي تدخل حسب قانون 05.20 ضمن ما يسمى بالمتعهدين.

2. إجراءات الحماية في قانون الأمن السيبراني المغربي

نظم المشرع المغربي في إطار القانون رقم 05.20 مجموعة من إجراءات الحماية المرتبطة بالأمن السيبراني، والكفيلة بتحقيق حماية فعالة من كل التهديدات التي قد تطال النظم المعلوماتية الخاصة بالفئات المشار إليها في المادة الأولى من القانون أعلاه، وقد أوكل في هذا الإطار مهمة تتبع ومراقبة سير تنفيذ هذه إجراءات إلى جهاز إداري يدعى بالسلطة الوطنية.[95]

ب- تقييم لوائح الأمن السيبراني بكوريا الجنوبية – سبب الاقتراح والمحتويات الرئيسية

لن أدخل في مشروع قانون الأمن السيبراني الوطني الذي اقترحه النائب لي تشيول وو، خاصة وأنه قديم بعض الشيء، وسأعمد إلى الإحاطة بسبب التشريع والمحتويات الرئيسية لمشروع قانون

[95] محمد القاسمي، قراءة في قانون 05.20 المتعلق بالأمن السيبراني، منشورات موقع الباحث القانوني، موقع مجلة الباحث للدراسات والأبحاث: https://www.allbahit.com/2021/05/0520.html، بتاريخ: 2025/06/29، على الساعة 22:19 مساء.

الأمن السيبراني بكوريا الجنوبية لعام 2022، ثم سبب المراجعة للتشريع الجزئي لمشروع قانون الأمن السيبراني لعام 2024 بتاريخ تنفيذه 5 مارس عام 2025، ومحتوياته الرئيسية التي تم إضافتها، كما يلي:

1. سبب التشريع

إن الأمن القومي والمصالح الوطنية تتعرض لتقويض خطير بسبب الهجمات الإلكترونية المتزامنة والواسعة النطاق التي تشنها منظمات القرصنة الدولية والمدعومة من قبل الدول، ومع ذلك، فإن أنشطة الاستجابة الوطنية لدى كوريا الجنوبية منفصلة ويتم الاستجابة لها بشكل مستقل وفقا للقوانين واللوائح الفردية لكل وزارة، وبالتالي هناك حدود للاستجابات الشاملة على مستوى الحكومة عندما يحدث تهديد للأمن السيبراني الوطني.

علاوة على ذلك، وعلى الرغم من توسع نطاق الأمن القومي إلى الفضاء الإلكتروني بسبب تطور التكنولوجيا السيبرانية، بما في ذلك الثورة الصناعية الرابعة، فلا يوجد حتى قانون أساسي لإنشاء وتنفيذ اتجاهات السياسة والتدابير المضادة لضمان الأمن السيبراني، مما يؤدي إلى عدم الكفاءة مثل الارتباك في أدوار كل وزارة وتداخل مجالات العمل.

بناء على ذلك، تخطط الحكومة لإنشاء نظام وطني للأمن السيبراني يتمحور حول مكتب الرئيس من خلال تشكيل لجنة وطنية للأمن السيبراني تضم خبراء مدنيين لتعزيز سياسات ومشاريع الأمن السيبراني الوطنية بكفاءة، وإنشاء وتشغيل منظمة استجابة متكاملة بشكل منفصل لإجراء تحقيقات سريعة في الحوادث، ومشاركة معلومات التهديد، وما إلى ذلك من خلال جمع القدرات الوطنية في أوقات الأزمات، بالإضافة إلى ذلك، تهدف إلى تعزيز أنشطة الوقاية والاستجابة من خلال توضيح المسؤولية عن حماية مجال اختصاص كل وزارة وتعزيز التعاون على مستوى الحكومة للاستجابة بشكل فعال لتهديدات الأمن السيبراني الوطني.

2. المحتويات الرئيسية

الغرض (المادة 1 من مشروع القانون)، يهدف هذا المشروع إلى تعزيز القدرات الوطنية، وتحديد أنظمة الاستجابة الوطنية للأمن السيبراني، والأنشطة، وأدوار المؤسسات في معالجة تهديدات الأمن السيبراني، والمساهمة في الأمن الوطني وحماية المصالح الوطنية.

أ- إنشاء اللجنة الوطنية للأمن السيبراني (المادة 6 من مشروع القانون)

من أجل مناقشة الأمور المتعلقة بوضع السياسات والاستراتيجيات الوطنية المتعلقة بالأمن السيبراني، يتم إنشاء لجنة وطنية للأمن السيبراني تحت إشراف الرئيس، وتتكون اللجنة من عدد لا يزيد على عشرين عضوا بما في ذلك الرئيس، ويتولى مدير مكتب الأمن الوطني رئاسة اللجنة، وتتكون اللجنة من رؤساء الأجهزة الإدارية المركزية، مثل مدير جهاز المخابرات الوطني ورئيس لجنة حماية المعلومات الشخصية، الذين يرشحهم الرئيس، والأشخاص الذين توصي بهم لجنة الاستخبارات في الجمعية الوطنية، والأشخاص الذين يعينهم الرئيس من بين الخبراء المدنيين.

ب- أنشطة الوقاية والاستجابة (المادة 7 من مشروع القانون)

1. (تقوم الأجهزة الإدارية المركزية وغيرها بتنفيذ الأنشطة الوقائية والاستجابة مثل عمليات التفتيش الأمنية والتدريب وإدخال واستخدام أجهزة المعلومات والاتصالات الآمنة وإنشاء وتشغيل أنظمة تبادل المعلومات والإبلاغ عن التهديدات وتأمين وتدريب الموظفين المتخصصين داخل مناطقهم المعنية.

2. (تتخذ الأجهزة الإدارية المركزية وغيرها التدابير اللازمة للرد على التهديدات مثل استغلال منظمات القرصنة لأجهزة المعلومات والاتصالات، وإعداد التدابير اللازمة لتعزيز التعاون الدولي واتخاذ التدابير الهجومية المضادة.

ت- تبادل المعلومات (المادة 8)، تدير الحكومة نظاما لتبادل وإدارة التهديدات الأمنية السيبرانية وتشارك المعلومات وفقا للقوانين واللوائح.

ث- تشغيل منظمة الاستجابة المتكاملة (المادة 9 من الخطة)، من أجل الاستعداد للتهديدات السيبرانية، ستقوم الحكومة بإنشاء وتشغيل نظام استجابة موحد يشمل الإخطار والتحقيق، ولتحقيق ذلك، ستقوم بإنشاء وتشغيل منظمة استجابة متكاملة تحت إشراف جهاز الاستخبارات الوطني تحت سيطرة اللجنة.

ج- الرقابة على الجمعية الوطنية (المادة 12 من مشروع القانون)، يسمح بإنشاء لجنة فرعية دائمة ضمن لجنة الاستخبارات في الجمعية الوطنية للتحقيق والإشراف على عمليات الأمن السيبراني.

ح- معالجة المعلومات الشخصية، وما إلى ذلك (المادة 16 من مشروع القانون)، لضمان الأمن السيبراني، نتخذ التدابير اللازمة لتقليل كمية المعلومات الشخصية التي تتم معالجتها ولضمان الإدارة الآمنة والمعالجة المناسبة.[96]

3. سبب المراجعة الجزئية الأخيرة لعام 2024

من أجل أداء عمل الأمن السيبراني بكفاءة ومنهجية، تمت إضافة معلومات الأمن السيبراني وأعمال التخطيط والتنسيق المتعلقة بالأمن إلى عمل الأمن السيبراني؛ من أجل منع التهديدات الأمنية السيبرانية بسرعة وتقليل الأضرار، يمكن لمدير جهاز الاستخبارات الوطني اتخاذ تدابير لتحييد أنشطة منظمات القرصنة الدولية والتابعة للدولة بشكل استباقي؛ ومن أجل تعزيز الأمن السيبراني، يمكن لمدير جهاز الاستخبارات الوطني إنشاء والتحقق من التدابير الأمنية لاستخدام خدمات الحوسبة السحابية من قبل الوكالات الإدارية المركزية وغيرها، وبالتالي تحسين واستكمال بعض أوجه القصور في تشغيل النظام الحالي.

4. المحتويات الرئيسية للمراجعة الجزئية الأخيرة لعام 2024

أ- إضافة أعمال التخطيط والتنسيق إلى نطاق عمل الأمن السيبراني (المادة 3، الفقرة 1، الفقرتان الفرعيتان 1 و2، المادة 3-2 المنشأة حديثا)

1) يقوم مدير جهاز الاستخبارات الوطني بأعمال التخطيط مثل وضع السياسات بشأن عمل معلومات الأمن السيبراني وعمل الأمن السيبراني، ويجب عليه وضع وتنفيذ المبادئ التوجيهية الأساسية لأداء هذا العمل بكفاءة ومنهجية.

2) في الحالات التي يكون فيها تنسيق عمل معلومات الأمن السيبراني وعمل الأمن السيبراني ضروريا، يتولى مدير جهاز الاستخبارات الوطني التنسيق المباشر للمسائل العاجلة التي لها تأثير كبير على الأمن الوطني، وينسق المسائل الأخرى وفقا للمبادئ التوجيهية الأساسية بشأن عمل معلومات الأمن السيبراني وعمل الأمن السيبراني.

---

[96] إشعار تشريعي بشأن مشروع القانون الأساسي للأمن السيبراني الوطني، إشعار جهاز المخابرات الوطني رقم 2022-5، بتاريخ : 8 نوفمبر 2022، على موقع وزارة التشريع الحكومي: https://www.moleg.go.kr/lawinfo/makingInfo.mo?lawSeq=70698&lawCd=0&&lawType=TYPE5&mid=a10104010000، تاريخ الاطلاع: 2025/09/13، على الساعة 21:09 مساء.

ب- الرد الاستباقي والمنهجي على تهديدات الأمن السيبراني (المادة 6-2 المضافة حديثا)

1) يجوز لمدير جهاز المخابرات الوطني إجراء اختبارات وتحليلات فنية على أجهزة المعلومات والاتصالات والبرمجيات التي تستخدم أو يحتمل استخدامها بشكل كبير في أنشطة تتعارض مع الأمن والمصالح الوطنية من أجل التأكد من سلامتها، ويجوز له أن يطلب من الوكالات الحكومية وغيرها اتخاذ التدابير اللازمة لتقليل المخاطر بناء على النتائج.

2) يجوز لمدير جهاز الاستخبارات الوطني اتخاذ التدابير اللازمة، مثل تعقب وتحييد القواعد الخارجية والكورية الشمالية، لتحديد وردع وحظر أنشطة منظمات القرصنة الدولية والتابعة للدولة والتي تتعارض مع الأمن والمصالح الوطنية.

3) يجوز لمدير جهاز المخابرات الوطني إنشاء وتشغيل نظام استجابة متكامل مشترك بين القطاعين العام والخاص لإدارة حالات الأزمات بالتشاور مع مدير مكتب الأمن الوطني كإجراء استجابة لحماية سلامة الشعب من الأنشطة التي تتعارض مع الأمن الوطني أو المصالح الوطنية.

ت- تعزيز احتياطات الأمن السيبراني (المادة 9)

1) يجوز لمدير جهاز المخابرات الوطني وضع تدابير أمنية بشأن استخدام خدمات الحوسبة السحابية من قبل الوكالات الإدارية المركزية وغيرها، والتحقق مما إذا كانت خدمات الحوسبة السحابية التي تستخدمها الوكالات الإدارية المركزية وغيرها مناسبة للتدابير الأمنية.

2) لمدير جهاز المخابرات الوطني أن يتمكن من قياس مستوى إدارة الأمن بهدف اكتشاف وتحسين نقاط الضعف في أجهزة المعلومات والاتصالات، وشبكات المعلومات والاتصالات، أو أنظمة المعلومات المرتبطة بها في الأجهزة الإدارية المركزية وغيرها، وعند قياس مستوى إدارة الأمن، عليه أن يخطر رؤساء الأجهزة الإدارية المركزية ذات الصلة وغيرها مسبقاً بالبنود والإجراءات وتوقيتها.

ث- تحسين نظام تقييم حالة الأمن السيبراني (المادة 13)

1) يكون مدير جهاز الاستخبارات الوطني قادرا على تقييم حالة الأمن السيبراني للوكالات الإدارية المركزية، وما إلى ذلك، من خلال إجراء التشخيص الذاتي والتفتيش على المنظمة والموظفين والميزانية والتدريب الوظيفي والأمن السيبراني لأداء أعمال الأمن السيبراني.

2) يجب على رئيس الجهاز الإداري المركزي المختص، الذي تم إخطاره بنتائج تقييم حالة الأمن السيبراني، إذا تم اكتشاف أي مشاكل نتيجة للتقييم، إعداد تدابير التحسين في غضون ثلاثة أشهر من

تاريخ إخطار النتائج وإخطار مدير جهاز المخابرات الوطني بذلك، ويستطيع مدير جهاز المخابرات الوطني بعد ذلك التحقق من مدى تنفيذ تدابير التحسين.

3) يجوز لمدير جهاز المخابرات الوطني الكشف عن نتائج تقييم حالة الأمن السيبراني بالقدر الذي لا يمس الأمن الوطني.[97]

رابعا: الأمن السيبراني والخصوصية

في كوريا الجنوبية، تتم مناقشة مشاريع القوانين المتعلقة بالأمن السيبراني دائما من حيث حماية الحقوق الأساسية، وكان هناك وعي كبير بأن تعزيز الأمن السيبراني له تأثير سلبي على الحق في حماية المجال الخاص للأفراد، مثل حرية الإقامة المنصوص عليها في المادة 16 من الدستور، وسرية وحرية الحياة الخاصة المنصوص عليها في المادة 17 من الدستور، وسرية الاتصالات المنصوص عليها في المادة 18 من الدستور.[98]

عند الترويج لسياسات الأمن السيبراني، يجب مراعاة تجنب الانتهاكات المحتملة لحماية المعلومات الشخصية أو حقوق الإنسان، إن الخصوصية والأمن السيبراني مرتبطان ارتباطا وثيقا، ولكنهما في حالة توتر مع بعضهما البعض، من أجل تأمين الأمن السيبراني، فإن معالجة المعلومات الشخصية أمر لا مفر منه، ولكن يمكن أيضا تأمين الأمن السيبراني من خلال حماية المعلومات الشخصية، وعندما يتم تأمين الأمن السيبراني، يمكن أيضا تحقيق حماية المعلومات الشخصية، وبالتالي فهما مرتبطان ارتباطا وثيقا،[99] في ضوء ذلك، يجب أن تكون حماية المعلومات الشخصية والخصوصية من الاعتبارات الأساسية في سياسة الأمن السيبراني الوطنية والتشريعات التي يتم الترويج لها محليا،[100] وذلك لأن التهديدات للخصوصية تصبح أكبر بما يتناسب مع التقدم التكنولوجي.

لا يستثني قانون الأمن السيبراني الوطني تطبيق قوانين وأنظمة حماية المعلومات الشخصية في مختلف الإجراءات الإدارية في مجال الأمن السيبراني، يسمح قانون الأمن السيبراني الوطني لمركز

---

[97] لوائح عمل الأمن السيبراني [تاريخ التنفيذ: 1 يناير 2025] [المرسوم الرئاسي رقم 34287، 5 مارس 2024، منقح جزئيا]، على موقع المركز الوطني للمعلومات القانونية بوزارة التشريع الحكومي، موقع رسمي للحكومة الإلكترونية لجمهورية كوريا الجنوبية: https://www.law.go.kr/LSW//lsInfoP.do?lsiSeq=261003&efYd=&ancYnChk=undefined#0000، تاريخ الاطلاع: 2025/09/13، على الساعة 21:17 مساء.

[98] بارك سانغ دون، مرجع سابق، ص 266.

[99] تشوي كيونج جين، مرجع سابق، ص177.

[100] كيم هيون سو، مرجع سابق، ص 172.

التحكم الأمني بجمع واستخدام المعلومات الشخصية بالقدر اللازم للكشف عن الهجمات السيبرانية والرد عليها، ويحدد أساس ونطاق جمع واستخدام المعلومات الشخصية.

بالإضافة إلى ذلك، تعتبر المعلومات الشخصية التي تتم معالجتها لأغراض الأمن السيبراني بمثابة معلومات شخصية وفقا للفقرة 1 من المادة 58 من قانون حماية المعلومات الشخصية، وفي الوقت نفسه، هناك حاجة إلى معايير معالجة المعلومات الشخصية والتدابير اللازمة وفقا للفقرة 4 من المادة 58 من قانون حماية المعلومات الشخصية، ويتم تنفيذ الرقابة الأمنية، ويوضح أيضا كيفية التعامل مع المعلومات الشخصية عبر جميع أنشطة الأمن السيبراني.

إن حقيقة أن أحكام قانون حماية المعلومات الشخصية المتعلقة بمعالجة المعلومات الشخصية والإدارة الآمنة للمعلومات الشخصية وضمان حقوق أصحاب البيانات ولجنة الوساطة في نزاعات المعلومات الشخصية والدعاوى الجماعية المتعلقة بالمعلومات الشخصية لا تنطبق على معالجة المعلومات الشخصية لأغراض الأمن السيبراني بموجب قانون الأمن السيبراني الوطني لا يرجع إلى أن قانون الأمن السيبراني الوطني يسن أحكاما مختلفة تماما عن قانون حماية المعلومات الشخصية وبالتالي يستبعد بشكل أساسي تطبيق قانون حماية المعلومات الشخصية، ولكنها نتيجة لتطبيق الفقرة 1 من المادة 58 من قانون حماية المعلومات الشخصية.

إن النص الوارد في قانون الأمن السيبراني الوطني الذي يطبق الفقرة 1 من المادة 58 من قانون حماية المعلومات الشخصية على معالجة المعلومات الشخصية لأغراض الأمن السيبراني يهدف فقط إلى منع الجدل حول ما إذا كانت معالجة المعلومات الشخصية لأغراض الأمن السيبراني بموجب قانون الأمن السيبراني الوطني تتوافق مع معالجة المعلومات الشخصية لغرض تحليل المعلومات المتعلقة بالأمن القومي كما هو محدد في الفقرة 1 من المادة 58 من قانون حماية المعلومات الشخصية من خلال تحديد هذا المحتوى، ويجب النظر إليه على أنه لا يهدف إلى استبعاد نظام قانون حماية المعلومات الشخصية، حتى لو كان لديهم مظهر أنشطة الأمن السيبراني كما هو منصوص عليه في قانون الأمن السيبراني الوطني، فإن أولئك الذين يقومون فعليا بمعالجة المعلومات الشخصية لأغراض لا علاقة لها بالأمن السيبراني، مثل ما يسمى بالمراقبة غير القانونية، لا يستوفون المتطلبات اللازمة للخضوع للفقرة 1 من المادة 58 من قانون حماية المعلومات الشخصية وسيتم معاقبتهم وفقا لعقوبة انتهاك حظر استخدام المعلومات الشخصية لأغراض أخرى غير الغرض المقصود منها.

بالإضافة إلى ذلك، حتى عند معالجة المعلومات الشخصية لأغراض الأمن السيبراني، يتم تطبيق الأحكام العامة لقانون حماية المعلومات الشخصية، مثل مبادئ حماية المعلومات الشخصية، وحقوق أصحاب البيانات، ومسؤوليات الدولة، بالإضافة إلى الأحكام المتعلقة بنظام تعزيز إنشاء سياسة حماية

المعلومات الشخصية المتمركز حول لجنة حماية المعلومات الشخصية، والعقوبات المختلفة، دون استثناء.[101]

في نهاية المطاف، يفترض قانون الأمن السيبراني بكوريا الجنوبية تطبيق نظام قانون حماية المعلومات الشخصية، ونظام قانون الأمن السيبراني ونظام قانون حماية المعلومات الشخصية هما في علاقة متقاطعة متبادلة، لذلك، من أجل معالجة المعلومات الشخصية بشكل صحيح في مختلف الإجراءات الإدارية للأمن السيبراني، يمكن ملاحظة أنه لا يجب على قوانين وأنظمة الأمن السيبراني أن تنص بشكل صحيح على محتويات حماية المعلومات الشخصية فحسب، بل يجب أيضا تحديد محتويات قوانين وأنظمة حماية المعلومات الشخصية بشكل صحيح.

إن وجود نظام قانوني للأمن السيبراني لا يستبعد تطبيق قوانين حماية المعلومات الشخصية في المسائل المتعلقة بالأمن السيبراني، كما يعمل القانون الأساسي لحماية المعلومات الشخصية كقانون أساسي لحماية المعلومات الشخصية التي يتم التعامل معها في الإجراءات الإدارية للأمن السيبراني، وفي مثل هذه الحالة، إذا لم يتم إعداد محتوى نظام قانون حماية المعلومات الشخصية بشكل صحيح، فهناك قلق من أن حماية المعلومات الشخصية قد لا يتم تنفيذها بشكل صحيح عند تطبيق نظام قانون حماية المعلومات الشخصية على قضايا الأمن السيبراني، على الرغم من عدم وجود مشكلة في نظام قانون الأمن السيبراني.[102]

بالإضافة إلى ذلك، تجدر الإشارة إلى أنه كما تمت مناقشته أعلاه، فإن تطبيق قانون حماية المعلومات الشخصية بالكامل لا يستبعد على المعلومات الشخصية وفقا للفقرة 1 من المادة 58 من قانون حماية المعلومات الشخصية، لذلك، فإن عبارة "لا ينطبق نفس القانون وفقا للفقرة 1 من المادة 58 من قانون حماية البيانات الشخصية" الواردة في المادة 21 من قانون الأمن السيبراني الوطني غير دقيقة وتحتاج إلى مراجعة لأنها يمكن أن تخلق سوء فهم لا داعي له.

يمكن تقييم إنشاء "الاستراتيجية الوطنية للأمن السيبراني" على أنه ذو أهمية كبيرة بحيث يمكن اعتباره رمزا للمسؤولية الوطنية عن الأمن السيبراني، ويمكن أيضا تقييم التشريع الحكومي، قانون الأمن السيبراني الوطني، من حيث التأكيد على التعاون بين الوزارات وبين القطاعين العام والخاص فيما يتعلق بتصميم المنظمات الإدارية للأمن السيبراني والعمليات الإدارية، وعند إنشاء منظمة إدارية للأمن السيبراني، يمكن ملاحظة وجود اتجاه عام في الدول الأجنبية المتقدمة للتأكيد على التعاون بين

---

[101] تشوي كيونج جين، مرجع سابق، ص 216-219.

[102] بارك سانج دون، مرجع سابق، ص 85-86.

الوزارات وبين القطاعين العام والخاص، ومن الضروري تقسيم الأدوار المتعلقة بالأمن السيبراني بشكل مناسب بين كل وزارة، بحيث تتمحور حول مكتب الأمن الوطني.

مع ذلك، هناك حاجة إلى ضمان الدور العملي الإيجابي لجهاز المخابرات الوطني، الذي كان مسؤولا عن الأمن السيبراني في القطاع العام، وفي حالة الولايات المتحدة، على نحو مقارن، تم توزيع سياسة الحكومة الفيدرالية لحماية الشبكات على وكالات مختلفة وفقا لمهامها أو وظائفها، ومع ذلك، يعمل البيت الأبيض ووزارة الأمن الداخلي على تعزيز وظائف الإدارة والتنسيق من منظور سياسي واستراتيجي، فضلا عن إدارة الحوادث والتنسيق من منظور عملي، ومن الضروري أيضا أن نلاحظ أن الجهود تبذل باستمرار لوضع أساس قانوني لذلك.[103]

خامسا: مشاكل في قوانين كوريا الجنوبية المتعلقة بالأمن السيبراني

من أبرز المشاكل التي تواجهها كوريا الجنوبية في القوانين واللوائح المتعلقة بالأمن السيبراني القيود المفروضة على التدابير الأمنية لمواجهة الهجمات الإلكترونية، غياب قوانين الأمن السيبراني العامة ومشاكل اتساق القوانين الفردية.

أ- أنواع جديدة من الهجمات الإلكترونية والقيود المفروضة على التدابير الأمنية

المشكلة الأكبر هي أنه لا توجد طريقة مطلقة لمنع الهجمات الإلكترونية، بحيث أن الفضاء الإلكتروني يختلف عن الفضاء المادي، إذ لا حدود له أو أقاليم، لذلك فمن غير الممكن وضع قواعد وضوابط لجميع الأفعال التي تتم في هذا الفضاء، علاوة على ذلك أصبحت الهجمات السيبرانية وأساليب التهديد غير قابلة للتنبؤ وبشكل متزايد، حتى مع تطوير تدابير أمنية للرد عليها، تبقى التدابير المتبعة لا تواكب مستوى التهديد، بحيث أن سرعة تطور تكنولوجيا المعلومات والاتصالات والوسائل والتقنيات للأعمال الخبيثة (الفيروسات المختلفة وأدوات القرصنة) التي تستخدمها تتطور بسرعة.

مع ذلك فإن التكلفة والاستثمار في الوقت المطلوب للتدابير المضادة والتكنولوجيا والقوى العاملة للدفاع ضدها هائلة، وفي نفس السياق من الضروري مراقبة الوضع الذي أصبح فيه مجال الأمن أقل أمنا بسبب رحيل خبراء الأمن، مما يجعل كوريا الجنوبية أكثر عرضة للهجمات الإلكترونية، وعلى وجه الخصوص، يتعين عليهم أن يسعوا إلى إيجاد تدابير استجابة للجوانب التي تحدث فيها الهجمات

---

[103] كيم جاي كوانغ، مرجع سابق.

الإلكترونية بالفضاء الإلكتروني، أعتقد أن هناك حاجة إلى مراجعة أكثر تعمقا من منظور السياسة القانونية والتشريعية وفي العالم الأكاديمي.

ب- غياب قوانين الأمن السيبراني العامة ومشاكل اتساق القوانين الفردية

تشمل المشاكل المتعلقة بالتشريعات الحالية المتعلقة بالأمن السيبراني، أولا، عدم وجود قانون عام للأمن السيبراني، وثانيا، عدم الاتساق في أنظمة القوانين الفردية، وثالثا، عدم وجود نظام قانوني للأمن المتقارب للتحضير لعصر إنترنت الأشياء.

(1) عدم وجود قوانين عامة للأمن السيبراني

في الوقت الحاضر، توجد في كوريا الجنوبية مشكلة خطيرة وجوهرية تتعلق بالأمن السيبراني، ألا وهي عدم وجود قانون عام للأمن السيبراني، وتعتبر هذه المشكلة مشكلة رئيسية فيما يتعلق بإدارة سيادة القانون، إن إدارة سيادة القانون تعني أن السلطة الإدارية يجب أن تمارس أيضا وفقا للقانون، وإذا انتهكت السلطة الإدارية حقوق الشعب، فيجب ضمان نظام للانتصاف (إنشاء نظام للرقابة الإدارية أو نظام للإغاثة الإدارية).

تتضمن مبادئ إدارة سيادة القانون القوة الإبداعية للقانون، ومبدأ سيادة القانون، ومبدأ تحفظ القانون، ومن بين هذه المبادئ مبدأ التحفظ القانوني الذي يعني أن ممارسة السلطة الإدارية يجب أن يكون لها أساس قانوني (وبشكل أدق، يجب أن يكون هناك أساس قانوني مباشر أو أساس في أمر صادر بناء على تفويض قانوني)، وإذا لم يكن هناك أساس قانوني، لا يمكن ممارسة السلطة الإدارية حتى لو كانت هناك حاجة للتدخل الإداري، فإن مبدأ التحفظ القانوني له أهمية كبيرة في حماية حقوق الإنسان وتحقيق الإدارة الديمقراطية.[104]

يعتبر الأمن السيبراني قضية أمن قومي جديدة ظهرت من السياسة، وهذا أيضا مجال من المرجح أن ينطوي على تقييد القطاع الخاص، لذلك، فيما يتعلق بلوائح الأمن السيبراني، من الأفضل تنظيمها كقوانين يتم سنها من خلال تشريعات من قبل الجمعية الوطنية، حيث أن إساءة استخدام القواعد الناعمة يمكن أن تنتهك مبدأ سيادة القانون.

---

[104] بارك جيون سيونج وكيم جاي جوانج، قانون إدارة الشرطة (الطبعة الثالثة)، (بارك يونغ سا، 2016)، ص 10، متوفر باللغة الكورية على مكتبة المحكمة: https://e-book.scourt.go.kr/contents/category?type=FOREIGN&lcate=001&mcate=003 ، تاريخ الاطلاع: 2025/09/13، على الساعة 21:40 مساء.

كما أن القوانين الحالية المتعلقة بالأمن السيبراني في كوريا متفرقة في نطاقها ونظام الاستجابة حسب القطاع، وتفتقر إلى اكتمال النظام، وعلى وجه الخصوص، في حالة القطاع العام، فإن المشكلة الخطيرة تكمن في أن لوائح الأمن السيبراني بكوريا الجنوبية أنشئت في شكل مرسوم رئاسي عام 2005، واستمرت في تنظيمها حتى يومنا هذا، إن حقيقة أن أعلى معيار فعلي للأمن السيبراني في القطاع العام هو مرسوم رئاسي وليس قانونا يعني وجود قيود متأصلة في نطاق المعيار ذي الصلة، وفي نهاية المطاف لا يتوافق مع مبدأ سيادة القانون، لذلك، من الضروري في نهاية المطاف حل هذه القضية من خلال التشريع.[105]

(2) مشكلة اتساق القوانين الفردية

تتضمن القوانين واللوائح الوطنية الحالية المتعلقة بالأمن السيبراني أحكاما فردية ومتفرقة بشأن الأمن السيبراني حسب القطاع أو الهدف، بدءا من قانون شبكة المعلومات والاتصالات، على سبيل المثال، حتى لو نظرنا فقط إلى الخطط الإدارية المتعلقة بالأمن السيبراني، فإن الخطط التمثيلية تشمل 1. خطة حماية البنية التحتية للمعلومات والاتصالات (قانون حماية البنية التحتية للمعلومات والاتصالات)، 2. خطة الحكومة الإلكترونية الأساسية (قانون الحكومة الإلكترونية)، 3. خطة المعلوماتية الوطنية الأساسية (القانون الأساسي للمعلوماتية الوطنية)، 4. سياسة تعزيز استخدام شبكة المعلومات والاتصالات وحماية المعلومات (قانون شبكة المعلومات والاتصالات)، 5. خطة تعزيز صناعة حماية المعلومات (قانون تطوير صناعة حماية المعلومات)، وأخيرا 6. الخطة الأساسية لتعزيز وتنشيط التقارب في مجال المعلومات والاتصالات (قانون تقارب المعلومات والاتصالات).

الخطة الإدارية هي خطة تحدد فيها جهة إدارية أو هيئة تابعة لها هدفا معينا للقيام بأنشطة إدارية معينة، وتختار الوسائل اللازمة لتحقيق هذا الهدف، وتضع هذه الوسائل وتلخصها، بحيث أن العناصر الأساسية للخطة الإدارية هي تحديد الأهداف وتنسيق وتجميع الوسائل، وعلى وجه الخصوص، تعد مسألة التوافق بين الخطط الإدارية المختلفة ذات أهمية كبيرة في مجال الأمن السيبراني، لا ينبغي أن يكون هناك تكرار أو تعارض بين الخطط الإدارية.[106]

---

[105] لي تشانج بوم، دور الأمن السيبراني في نجاح الحكومة 3.0، مجلة قانون وسياسة الأمن السيبراني، المجلة الكورية لقانون الأمن السيبراني، العدد 2، 2016، ص13، على الرابط التالي: http://www.kcsa2012.or.kr/wp-content/uploads/2019/01/2nd.pdf?ckattempt=1 ، تاريخ الاطلاع: 2025/09/13، على الساعة 21:51 مساء.

[106] بارك جيون سونغ وكيم جاي جوانج، مرجع سابق، ص 219.

تشمل هذه القوانين المتعلقة بحماية شبكات المعلومات والاتصالات وأنظمة المعلومات (القانون الجنائي، وقانون شبكة المعلومات والاتصالات، وقانون حماية البنية التحتية للمعلومات والاتصالات، وقانون الحكومة الإلكترونية، ولوائح إدارة الأمن السيبراني الوطنية)، والقوانين المتعلقة بحماية المعلومات الشخصية والخصوصية (قانون حماية المعلومات الشخصية، وقانون شبكة المعلومات والاتصالات، وقانون معلومات الموقع، وقانون حماية المعلومات المالية، وقانون معلومات الائتمان، وقانون حماية أسرار الاتصالات)، والقوانين المتعلقة بتعزيز القوى العاملة والصناعات في مجال الأمن السيبراني (قانون تعزيز صناعة المعلومات والاتصالات، وقانون شبكة المعلومات والاتصالات، وقانون الإطار الوطني للمعلوماتية، وقانون حماية التكنولوجيا الصناعية، ولوائح إدارة الأمن السيبراني الوطنية (المرسوم الرئاسي).

نظرا لوجود قوانين حسب القطاع أو الهدف، فمن الضروري إعادة تنظيم القوانين ذات الصلة من حيث اتساق النظام القانوني، بمعنى السعي إلى تحقيق اتساق منهجي في الأشكال المختلفة للقوانين واللوائح المتعلقة بالأمن السيبراني.[107]

(3) تشريعات أمن التقارب للتحضير للهجمات الإلكترونية عبر إنترنت الأشياء

هناك مشكلة تتمثل في عدم وجود قوانين أمنية متكاملة للتحضير للهجمات الإلكترونية عبر إنترنت الأشياء، في عصر إنترنت الأشياء، سيتغير العصر من عصر يستخدم فيه الناس الأشياء إلى عصر تعمل فيه الأشياء بنشاط لصالح الناس، كما ستنتشر الهجمات الإلكترونية مثل القرصنة والهجمات الإلكترونية ذات النية الخبيثة على نطاق واسع، إذ من خلال ما نراه من هجمات إلكترونية حاليا تقول بأننا في خضم ذلك، وبما أن كل شيء تقريبا في العالم متصل بالإنترنت، فمن المؤكد أن إنترنت الأشياء سيكون عرضة للهجمات، ومن المتوقع أن يكون الضرر الناجم عن هذه الهجمات هائلا إلى درجة لا يمكن السيطرة عليها، وسوف يكون من الصعب للغاية الاستجابة بشكل شامل للهجمات الإلكترونية التي تهدد الأمن القومي بسبب انفتاح إنترنت الأشياء.

من أجل الاستعداد لذلك، يتعين تحسين الواقع الحالي المتمثل في عدم كفاية السياسات والأنظمة الأمنية المترابطة والمتقاربة، يشير أمن التقارب إلى المنتجات والخدمات الأمنية التي تم إنشاؤها من خلال التقارب بين أمن المعلومات والأمن المادي، أو التقارب بين تقنيات الأمن مع التقنيات

---

[107] كيم جاي كوانج، "الاستراتيجية التشريعية استجابة للتغيرات في البيئة التشريعية للأمن السيبراني"، مجلة قانون وسياسة الأمن السيبراني، المجلة الكورية لقانون الأمن السيبراني، العدد 2، 2016، على الرابط التالي: http://www.kcsa2012.or.kr/wp-content/uploads/2019/01/2nd.pdf ، تاريخ الاطلاع: 2025/09/13، على الساعة 22:07 مساء.

والصناعات غير المتعلقة بتكنولوجيا المعلومات، ومن الضروري إنشاء نظام قانوني مناسب لأمن التقارب، وفي عصر إنترنت الأشياء، خاصة مع تزايد عمليات انتهاك الحياة الشخصية بسرعة، لذا يجب تعزيز حماية المعلومات الشخصية، ومن أجل الاستجابة لتهديدات الأمن السيبراني في عصر إنترنت الأشياء، هناك حاجة إلى "التعاون المفرط" بين القطاعين العام والخاص وأصحاب المصلحة المختلفين.[108]

سادسا: أنواع الجرائم الإلكترونية والقوانين المعمول بها بكوريا الجنوبية

تصنف الجرائم الالكترونية إلى جريمة الإرهاب الإلكتروني من قرصنة وتوزيع الفيروسات، وهي أعمال غير قانونية تستهدف شبكة المعلومات والاتصالات نفسها، والجرائم الإلكترونية العامة تشمل الأفعال غير القانونية الشائعة باستخدام الفضاء الإلكتروني مثل تسريب المعلومات الشخصية، وسأقتصر على هذا النموذج واحد من الجرائم الإلكترونية العامة، الذي سبق أن ذكرته كمثال، مع بيان القوانين واللوائح ذات الصلة حسب نوع الجريمة الإلكترونية.

أ- القرصنة

1. قانون حماية شبكة المعلومات والاتصالات

المادة 28 (العقوبات)

①يعاقب بالسجن لمدة لا تزيد على 10 سنوات أو بغرامة لا تتجاوز 100 مليون وون كل من يخالف أحكام المادة 12 ويقوم بتعطيل أو شلل أو تدمير البنية التحتية الرئيسية للمعلومات والاتصالات.

②يعاقب على الشروع في ارتكاب جريمة بموجب الفقرة 1.

2. قانون تعزيز استخدام شبكات المعلومات والاتصالات وحماية المعلومات.

المادة 71 (العقوبات)

①يعاقب بالسجن لمدة لا تزيد على 5 سنوات أو بغرامة لا تتجاوز 50 مليون وون كل من وقع تحت أي من الفقرات الفرعية التالية.

المادة 12 (حظر الأعمال التي تمس البنية التحتية الرئيسية للمعلومات والاتصالات وغيرها)

---

[108] لي سانغ هو وجو يون يونغ، مرجع سابق، ص 16-26.

لا يجوز لأي شخص ارتكاب أي من الأفعال التالية: 1. يقوم شخص لا يملك حقوق الوصول بالوصول إلى المعلومات الأساسية والبنية التحتية للاتصالات، أو يقوم شخص يتمتع بحقوق الوصول بالتلاعب بالبيانات المخزنة أو تدميرها أو إخفائها أو سرقتها عن طريق تجاوز حقوقه، وكل من دخل على شبكة المعلومات والاتصالات بالمخالفة للمادة 48 فقرة 1.[109]

ب- الفايروسات

1. قانون حماية البنية التحتية للمعلومات والاتصالات

المادة 28 (العقوبات)

①يعاقب بالسجن لمدة لا تزيد على 10 سنوات أو بغرامة لا تتجاوز 100 مليون وون كل من يخالف أحكام المادة 12 ويقوم بتعطيل أو شلل أو تدمير البنية التحتية الرئيسية للمعلومات والاتصالات.

②يعاقب على الشروع في ارتكاب جريمة بموجب الفقرة 1. المادة 12 (حظر الأعمال التي تمس البنية التحتية الرئيسية للمعلومات والاتصالات)

لا يجوز لأي شخص ارتكاب أي من الأفعال التالية: 2. إدخال برامج مثل فيروسات الكمبيوتر أو القنابل المنطقية بغرض تدمير البيانات أو التدخل في تشغيل البنية التحتية الرئيسية للمعلومات والاتصالات.[110]

ت- انتهاك الخصوصية

1. قانون حماية المعلومات الشخصية

المادة 71 (العقوبات) يعاقب بالسجن مدة لا تزيد على خمس سنوات أو بغرامة لا تتجاوز خمسين مليون وون كل من ارتكب أيا من الأفعال الآتية:

---

[109] قانون حماية البنية التحتية للمعلومات والاتصالات [تاريخ النفاذ: 24 يناير 2025] [القانون رقم 20068، 23 يناير 2024، تعديل جزئي]، على موقع المركز الوطني للمعلومات القانونية بوزارة التشريع الحكومي، موقع رسمي للحكومة الإلكترونية لجمهورية كوريا الجنوبية:
https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%A0%95%EB%B3%B4%ED%86%B5%EC%8B%A0%EA%B8%B0%EB%B0%98%EB%B3%B4%ED%98%B8%EB%B2%95، تاريخ الاطلاع: 2025/09/13، على الساعة 22:10 مساء.

[110] قانون تعزيز استخدام شبكات المعلومات والاتصالات وحماية المعلومات، مرجع سابق.

4 من 5. الشخص الذي يجمع معلومات شخصية دون موافقة المستخدم في انتهاك للمادة 39-3، الفقرة 1 (بما في ذلك الحالات المطبقة وفقا للمادة 39-14) (المادة 39-3 استثناءات خاصة للموافقة على جمع/استخدام المعلومات الشخصية) ① على الرغم من الفقرة 1 من المادة 15عندما يقوم مزود خدمات المعلومات والاتصالات بجمع معلومات شخصية عن مستخدم للاستخدام، يجب عليه إخطار المستخدم بجميع الأمور التالية والحصول على الموافقة، وينطبق الأمر نفسه أيضا إذا كنت ترغب في تغيير أي من العناصر التالية: الغرض من جمع المعلومات الشخصية واستخدامها، وعناصر المعلومات الشخصية التي تم جمعها، وفترة الاحتفاظ بالمعلومات الشخصية واستخدامها.[111]

2. القانون الجنائي

المادة 316 (الإخلال بالسرية) الفقرة ② كل من اكتشف محتويات رسالة أو وثيقة أو رسم أو سجل إلكتروني أو سجل إعلامي خاص آخر مختوم أو مخفي باستخدام الوسائل التقنية يعاقب بنفس العقوبة المنصوص عليها في الفقرة 1 (الحبس أو الاحتجاز لمدة لا تزيد على 3 سنوات أو غرامة لا تتجاوز 5 ملايين وون)، كما تنص المادة 318 (الدعوى) على أنه لا تجوز إقامة الدعوى إلا بناء على شكوى عن الجرائم المنصوص عليها في هذا الفصل، وكل من أفشى أو سرب محتويات اتصال أو محادثة تم الحصول عليها وفقا لأحكام المادة 1.[112]

3. قانون تسجيل المقيمين

المادة 37 (العقوبات)

②يعاقب بالسجن لمدة لا تزيد على 3 سنوات أو بغرامة لا تتجاوز 30 مليون وون كل من وقع تحت أي من الفقرات الفرعية التالية.

---

[111] قانون حماية المعلومات الشخصية، [تاريخ التنفيذ: 13 مارس 2025] [القانون رقم 19234، 14 مارس 2023، مراجع جزئيا]، على موقع المركز الوطني للمعلومات القانونية بوزارة التشريع الحكومي، موقع رسمي للحكومة الإلكترونية لجمهورية كوريا الجنوبية: https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EA%B0%9C%EC%9D%B8%EC%A0%95%EB%B3%B4%EB%B3%B4%ED%98%B8%EB%B2%95، تاريخ الاطلاع: 2025/09/13، على الساعة 22:13 مساء.

[112] القانون الجنائي [تاريخ التنفيذ: 8 أبريل 2025] [القانون رقم 20908، 8 أبريل 2025، معدل جزئيا]، على موقع المركز الوطني للمعلومات القانونية بوزارة التشريع الحكومي، موقع رسمي للحكومة الإلكترونية لجمهورية كوريا الجنوبية: https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%ED%98%95%EB%B2%95، تاريخ الاطلاع: 2025/09/13، على الساعة 22:16 مساء.

1 .كل من أنشأ رقم تسجيل إقامة مزورا باستخدام أسلوب تخصيص أرقام تسجيل الإقامة وفقا للمادة 7 فقرة 4 واستخدمه لمنفعته الشخصية أو لمنفعة شخص آخر أو لمنفعته المالية.

4 .الشخص الذي قام بنقل أو توزيع برنامج ينشئ رقم تسجيل مقيم زائفا لشخص آخر.

10 .الامتناع عن استعمال رقم تسجيل إقامة شخص آخر بطريقة غير مشروعة المادة 3 (حماية أسرار الاتصالات والمحادثات)

① لا يجوز لأي شخص مراقبة البريد أو التنصت على الاتصالات أو تقديم تأكيد لوقائع الاتصالات أو القيام بأعمال غير معلنة بين الآخرين إلا وفقا لأحكام هذا القانون أو قانون الإجراءات الجنائية أو قانون المحكمة العسكرية.[113]

المطلب الثاني: الأمن السيبراني للحكومة الإلكترونية بين التجربة المغربية وآفاق التجربة اليابانية على ضوء القوانين الرقمية

تم سن القانون الأساسي للأمن السيبراني في عام 2014 (هيسي 26) ودخل حيز التنفيذ في يناير 2015 (هيسي 27)، وينص هذا القانون على المبادئ الأساسية والمسؤوليات الوطنية واستراتيجيات الأمن السيبراني وغيرها من المسائل السياسية الأساسية من أجل تعزيز تدابير الأمن السيبراني بطريقة شاملة وفعالة.

مع ذلك، فإن هذه ليست سوى مجموعة من المبادئ الأساسية، وسيتم ترك الاستراتيجيات المحددة لأنشطة المركز الوطني للاستعداد للحوادث واستراتيجية الأمن السيبراني (NISC) والقوانين الأخرى، كما لا ننكر بأن التحديات الأمنية التي واجهتها اليابان كانت المحفز الأكبر لوضع تغييرات بالقانون (الفقرة الأولى)، بالتالي سنعمد إلى سرد القانون الأساسي للأمن السيبراني الحالي بالإمبراطورية اليابانية (الفقرة الثانية).

---

[113] قانون تسجيل المقيمين [تاريخ التنفيذ: 27 ديسمبر 2024] [القانون رقم 19841، 26 ديسمبر 2023، التعديل الجزئي]، على موقع المركز الوطني للمعلومات القانونية بوزارة التشريع الحكومي، موقع رسمي للحكومة الإلكترونية لجمهورية كوريا الجنوبية: https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%A3%BC%EB%AF%BC%EB%93%B1%EB%A1%9D%EB%B2%95، تاريخ الاطلاع: 2025/09/13، على الساعة 22:17 مساء.

الفقرة الأولى: قانون الأمن السيبراني باليابان

قبل أن تعرف على الخلفية التي أتى منها قانون الأمن السيبراني باليابان (ثانيا)، وكذا الهجمات السيبرانية التي كانت الدافع لوضع تعديلات بالقانون (ثالثا)، سأعمل على تصنيف الهجمات الإلكترونية مع الجزاءات حسب القوانين اليابانية (أولا).

أولا: تصنيف الهجمات الإلكترونية والقوانين المعمول بها باليابان

أ- قانون العقوبات- التسجيل الإلكتروني للتعليمات غير المصرح بها (ما يسمى بجرائم فيروسات الكمبيوتر).

صدر قانون تعديل قانون العقوبات، لمواكبة التطورات في مجال معالجة المعلومات، (القانون رقم 74 لسنة 2011) في 24 يونيو/حزيران 2011، وأضاف القانون المعدل جريمة جديدة هي "التسجيل الإلكتروني للتعليمات غير المصرح بها (ما يسمى بجرائم فيروسات الكمبيوتر)" إلى قانون العقوبات، ودخل حيز النفاذ في 14 يوليو/تموز من العام نفسه.

1. جريمة صنع وتوزيع الفيروسات

يشير هذا إلى فعل إنشاء وتوفير فيروس كمبيوتر أو برنامج فيروس كمبيوتر (كود المصدر) دون سبب مشروع، بقصد تشغيل الكمبيوتر تلقائيا وبغض النظر عن نوايا المستخدم.

تصل عقوبة هذه الجريمة إلى السجن لمدة تصل إلى ثلاث سنوات أو غرامة تصل إلى 500 ألف ين (الفقرة 1 من المادة 168-2 من قانون العقوبات).

2. جريمة توفير الفيروس

يشير هذا إلى فعل وضع فيروس الكمبيوتر في حالة يتم تنفيذها فيها تلقائيا وبشكل مستقل عن نوايا المستخدم دون سبب مشروع، أو فعل محاولة القيام بذلك.

تصل عقوبة هذه الجريمة إلى السجن لمدة تصل إلى ثلاث سنوات أو غرامة تصل إلى 500 ألف ين (الفقرة 1 من المادة 168-2 من قانون العقوبات).

3. جريمة الحصول على الفيروس وتخزينه

يشير هذا إلى عملية الحصول على فيروس كمبيوتر أو الكود المصدر لفيروس كمبيوتر وتخزينه دون سبب مشروع، بقصد تشغيله بحرية وبغض النظر عن نوايا المستخدم.

تصل عقوبة هذه الجريمة إلى السجن لمدة تصل إلى عامين أو غرامة تصل إلى 300 ألف ين (المادة 168 -3 من قانون العقوبات).[114]

ب- انتهاك قانون الوصول غير المصرح به إلى الكمبيوتر

إن الحصول على معرف وكلمة مرور بشكل غير قانوني والوصول إلى صفحة أو حساب يديره شخص آخر يعد انتهاكًا لقانون منع الوصول غير المصرح به، عقوبة الدخول غير المصرح به هي السجن لمدة تصل إلى ثلاث سنوات أو غرامة تصل إلى مليون ين.

تعاقب محاولات التصيد للحصول بشكل غير قانوني على هويات وكلمات مرور، أو محاولات تسهيل الوصول غير المصرح به، بالسجن لمدة تصل إلى عام واحد أو غرامة تصل إلى 500 ألف ين.

1. حظر الوصول غير المصرح به

المادة 3 لا يجوز لأي شخص ارتكاب أي فعل من أفعال الدخول غير المصرح به.

2. العقوبات

المادة 11 يعاقب بالحبس مدة لا تزيد على ثلاث سنوات أو بغرامة لا تزيد على مليون ين كل من يخالف أحكام المادة 3، (المادة 3 والمادة 11 من قانون حظر الدخول غير المصرح به إلى أجهزة الكمبيوتر)[115]

ت- قانون الأمن السيبراني الياباني

فرض عقوبات، مثل غرامة تصل إلى 2 مليون ين، على مشغلي البنية التحتية الأساسية الذين يفشلون في الإبلاغ عن الحوادث ولا يتخذون إجراء حتى بعد تلقي أمر تصحيحي.

---

[114] قانون تعديل قانون العقوبات وغيره للتعامل مع تقدم معالجة المعلومات، القانون رقم 74 (24 يونيو 2011) – القانون الياباني، على موقع مجلس النواب، اليابان: https://www.shugiin.go.jp/internet/itdb_housei.nsf/html/housei/17720110624074.htm، تاريخ الاطلاع: 2025/09/13، على الساعة 22:22 مساء.

[115] قانون حظر الوصول غير المصرح به إلى أجهزة الكمبيوتر، القانون رقم 128 لسنة 1999، الصادر في 17 يونيو 2022، على موقع e-GOV البحث القانوني: https://laws.e-gov.go.jp/law/411AC0000000128/20220617_504AC0000000068، تاريخ الاطلاع: 2025/09/13، على الساعة 22:25 مساء.

يتعلق قانون الأمن السيبراني بإدخال "الدفاع السيبراني النشط" لمنع الهجمات السيبرانية الخطيرة، سيتم فرض عقوبات على الأشخاص الذين يقومون بتسريب معلومات الاتصالات التي تم الحصول عليها ومشاركتها في عملية التعاون بين القطاعين العام والخاص لتحديد علامات الهجمات الإلكترونية، وسوف يؤدي هذا إلى إنشاء نظام يمكن للقطاعين العام والخاص من خلاله الحفاظ على السرية، وكجزء من الدفاع السيبراني النشط، تحصل الحكومة على معلومات الاتصالات المحلية والدولية حول الهجمات السيبرانية من الشركات من أجل الكشف عن مصدر الهجمات.[116]

وتجدر الإشارة إلى أن المقالة تلخص مشروع قانون الأمن السيبراني في حين أنه تمت المصادقة على مشروع قانون ودخل حيز التنفيذ، فيما بعد سأعمل على دراسة مضمون القانون وهيكلته، مع ذكر الخلفية التي على أساسها تمت عدة تعديلات عليه.

ث- المساس بسرية الاتصالات السلكية

يعاقب بالسجن مدة لا تزيد على خمس سنوات أو بغرامة لا تزيد على مليون ين كل من ألحق الضرر بمرافق الاتصالات السلكية أو أدخل جسما في اتصال معها أو أعاق بأي شكل آخر عمل مرافق الاتصالات السلكية وبالتالي عطل الاتصالات السلكية (المادة 13 من قانون من قانون الاتصالات السلكية)، ويعاقب على كل محاولة ارتكاب جريمة بموجب الفقرة السابقة.

يعاقب بالسجن مدة لا تزيد على سنتين أو بغرامة لا تزيد على خمسمائة ألف ين كل من ينتهك سرية الاتصالات السلكية بالمخالفة لأحكام المادة 9 (المادة 14 من نفس القانون).

إذا ارتكب أي شخص يعمل في مجال الاتصالات السلكية أيا من الأفعال المنصوص عليها في الفقرة السابقة، يعاقب بالسجن لمدة لا تزيد على ثلاث سنوات أو بغرامة لا تزيد على مليون ين.

يعاقب على أي محاولة ارتكاب جريمة بموجب الفقرتين السابقتين.

---

[116] *الدفاع السيبراني وعقوبات تسريب معلومات الاتصالات للمسؤولين الحكوميين والمواطنين*، 15 يناير 2025، nikkei: https://www.nikkei.com/article/DGXZQOUA15B8T0V10C25A1000000/، تاريخ الاطلاع: 2025/09/13، على الساعة 22:32 مساء.

تخضع الجرائم المنصوص عليها في الفقرات الثلاث السابقة لأحكام المادة 4-2 من قانون العقوبات (القانون رقم 45 لسنة 1907). [117]

ثانيا: مضمون القانون الأساسي للأمن السيبراني باليابان

سنعمد إلى ذكر المبادئ الرئيسية للقانون الأساسي للأمن السيبراني باليابان، ثم سرد خلفية سنه.

أ- المبادئ الأساسية

ينص القانون الأساسي للأمن السيبراني على مبادئه الأساسية في المادة 3 على النحو التالي:

1. بناء على مبدأ ضمان التدفق الحر للمعلومات، ينبغي للقطاعين العام والخاص العمل معا للاستجابة بشكل استباقي لهذه القضية.
2. يحتاج كل مواطن إلى تعميق وعيه بالأمن السيبراني، واتخاذ إجراءات تطوعية، وبناء نظام مرن.
3. بناء مجتمع اقتصادي نابض بالحياة من خلال تطوير شبكات المعلومات والاتصالات المتقدمة واستخدام تكنولوجيا المعلومات.
4. لعب دور قيادي في تشكيل النظام الدولي فيما يتعلق بالأمن السيبراني وتنفيذه وفقا للتعاون الدولي.
5. عدم التعدي على حقوق المواطنين بشكل غير مبرر، وسيتم تنفيذ التدابير على أساس هذه المبادئ.

ب- منظمة

في يناير 2015، تم إنشاء مقر استراتيجي للأمن السيبراني داخل مجلس الوزراء بناء على هذا القانون، يتألف المقر الرئيسي من رئيس مجلس الوزراء والوزراء المعنيين الآخرين والخبراء، الأمانة العامة هي الأمانة العامة لمجلس الوزراء للمركز الوطني للاستعداد للحوادث والاستراتيجية للأمن السيبراني(NISC) ، وهي منظمة جديدة تشكلت من المركز الوطني لأمن المعلومات (NISC) السابق (ملاحظة: الاختصار هو نفسه كما كان من قبل).

ت- خلفية سن القانون الأساسي للأمن السيبراني

---

[117] قانون الاتصالات السلكية، القانون رقم 96 لسنة 1950، ساري المفعول اعتبارا من 17 يونيو 2020 - القانون الياباني، على موقع e-GOV البحث القانوني: https://laws.e-gov.go.jp/law/328AC0000000096/20220617_504AC0000000068، تاريخ الاطلاع: 2025/09/13، على الساعة 22:43 مساء.

كان القانون الوحيد المتعلق بتكنولوجيا المعلومات حتى ذلك الحين هو القانون الأساسي بشأن تشكيل مجتمع شبكات المعلومات والاتصالات المتقدمة (المعروف باسم القانون الأساسي لتكنولوجيا المعلومات)، والذي دخل حيز التنفيذ في عام 2001 (Heisei 13) في عام 2005، بناء على قرار اتخذه مقر استراتيجية تكنولوجيا المعلومات التابع للحكومة، تم إنشاء مركز أمن المعلومات (NISC) داخل أمانة مجلس الوزراء.

ومع ذلك، استمر عدد التهديدات، مثل الإصابة بالفيروسات والهجمات المستهدفة على الوكالات الحكومية، في الارتفاع في الشركات الكبرى والوكالات الحكومية، وكانت هناك أيضا حالات تسرب معلومات شخصية لمنظمات مختلفة، وتتضمن أسباب تسرب المعلومات ليس فقط الهجمات الإلكترونية، بل أيضا الأخطاء البشرية مثل فقدان وسائط التخزين، وظل عدد الهجمات الإلكترونية يتزايد، وأصبحت أساليبها أكثر تنوعا وأوسع نطاقا، مما جعل من الضروري تعزيز استراتيجيات الأمن، وبعد ذلك تم سن قانون الأمن السيبراني الأساسي كقانون يتم استخدامه بالتزامن مع قانون تكنولوجيا المعلومات الأساسي.

ثالثا: خلفية تعديل القانون الأساسي للأمن السيبراني

حتى بعد دخول القانون الأساسي للأمن السيبراني حيز التنفيذ، كانت هناك سلسلة من حوادث تسريب المعلومات الشخصية، لذلك تم إجراء تعديلات في عام 2016 (هيسي 28) و2018 (هيسي 30)، وذلك بشكل أساسي بهدف تعزيز سلطة مركز الأمن السيبراني الوطني وتقليل عبء العمل الإداري.

أ- التعديلات في عام 2016

1- الخلفية

في عام 2015، وقعت حادثة تسرب بيانات في هيئة المعاشات التقاعدية اليابانية، تم تنفيذ هجوم مستهدف على شبكة المعلومات التابعة لدائرة المعاشات التقاعدية اليابانية، مما أدى إلى تسرب كمية كبيرة من المعلومات الشخصية الموجودة لدى الخدمة.

ومع ذلك، رغم أن مركز المعلومات الوطني كان قادرا في ذلك الوقت على الإبلاغ عن تسرب المعلومات إلى هيئة معاشات التقاعد اليابانية، فإنه لم يتمكن من إجراء تحقيق كاف أو اتخاذ التدابير اللازمة لأنه كان يقتصر على التحقيق في الوزارات والوكالات الحكومية المركزية ولم يشمل الوكالات الإدارية المستقلة مثل هيئة معاشات التقاعد اليابانية.

نتيجة لذلك، استمرت الهجمات المستهدفة، مما أدى إلى زيادة الأضرار الناجمة عن تسريبات المعلومات الشخصية، لقد كانت هذه الحادثة أحد العوامل المحفزة لتغير القانون.

2- التغييرات

تم توسيع نطاق مراقبة الحكومة للاتصالات غير القانونية والتحقيقات في أسبابها، وينطبق هذا التعديل أيضا على الشركات الخاصة والهيئات الإدارية المستقلة، وقد أدى توسيع نطاق التغطية أيضا إلى زيادة حجم أعمال المراقبة والتحقيق، ونتيجة لذلك، أصبح من الممكن الآن الاستعانة بمؤسسات إدارية مستقلة مثل وكالة تعزيز تكنولوجيا المعلومات (IPA) للقيام ببعض الأعمال الإدارية للمقر الاستراتيجي للأمن السيبراني.

كإجراء ملموس، تم إنشاء مؤهل وطني جديد، وهو "أخصائي أمن معالجة المعلومات"، والذي يؤهل الأفراد للحصول على مهارات عملية في تدابير أمن المعلومات، يتم إدارة هذه المؤهلات من قبل معهد الإدارة العامة (IPA) وتهدف إلى تطوير وتأمين الموارد البشرية لتعزيز تدابير الأمن السيبراني.

ب- التعديلات في عام 2018 (هيسي 30)

1- الخلفية

كان عام 2018 هو العام الذي أقيمت فيه دورة الألعاب الأولمبية الشتوية في بيونج تشانج، كوريا الجنوبية، وشهد هذا العام العديد من حوادث الإرهاب عبر الإنترنت، بما في ذلك خلال دورة الألعاب الأولمبية، وكانت هناك أيضا العديد من الهجمات الإلكترونية قبل دورة الألعاب الأولمبية في ريو دي جانيرو عام 2016 ولندن، وبحيث كانت هناك مخاوف آنذاك من أنه في حال وقوع هجوم إرهابي عبر الإنترنت في دورة الألعاب الأولمبية والبارالمبية، التي ستجمع بين كبار الرياضيين والمتفرجين من العديد من البلدان، فإن الأضرار ستكون هائلة، وعلى ضوء ذلك، تم تعديل القانون الأساسي للأمن السيبراني للسماح للقطاعين العام والخاص بالعمل معا لاتخاذ التدابير اللازمة وقتها لضمان الاستعداد الكامل لدورة الألعاب الأولمبية والبارالمبية في طوكيو عام 2020.

2- التغييرات

تم إنشاء مجلس الأمن السيبراني لتمكين مختلف الكيانات في القطاعين العام والخاص من العمل معا لتبادل المعلومات ومناقشة التدابير اللازمة وما إلى ذلك، تم إطلاقه في أبريل 2019 عندما دخل القانون المعدل حيز التنفيذ.

أنشأ المقر الاستراتيجي للأمن السيبراني إجراءات إدارية لتمكين التواصل السريع مع الأطراف ذات الصلة في اليابان والخارج، يمكن أيضا الاستعانة بمصادر خارجية لجزء من هذا العمل من خلال شركات محددة ملزمة بالتزامات السرية.

ث- تعزيز التدابير الأمنية

أصدر المقر الاستراتيجي للأمن السيبراني "استراتيجية الأمن" التي وافق عليها مجلس الوزراء في عام 2018، والتي تحدد الأهداف والمبادئ التوجيهية لتنفيذ التدابير المختلفة من عام 2018 إلى عام 2021، وتشير استراتيجية الأمن هذه، التي يجري تنفيذها حاليا في عام 2020، إلى أن المبادئ الخمسة المنصوص عليها في استراتيجية عام 2015 سوف تستمر في الالتزام بها: "ضمان التدفق الحر للمعلومات"، و"سيادة القانون"، و"الانفتاح"، و"الاستقلالية"، و"التعاون بين مختلف الجهات الفاعلة"، كما ينص بوضوح على تدابير محددة لتحقيق "تحسين الحيوية الاقتصادية والاجتماعية والتنمية المستدامة"، و"مجتمع يمكن للناس أن يعيشوا فيه بسلام وأمان"، و"السلام والأمن الدوليين، فضلا عن مساهمة اليابان في الأمن القومي".

كما ينص بوضوح على تدابير محددة لتحقيق "تحسين الحيوية الاقتصادية والاجتماعية والتنمية المستدامة"، و"مجتمع يمكن للناس أن يعيشوا فيه بسلام وأمان"، و"السلام والأمن الدوليين، فضلا عن مساهمة اليابان في الأمن القومي".

على وجه الخصوص، في عام 2020، يوصى بالاستخدام النشط للعمل عن بعد كإجراء ضد جائحة كوفيد-19، وفي حين أن العمل عن بعد يعد وسيلة فعالة للحد من المخاطر في الأماكن التي يتجمع فيها الكثير من الناس، مثل التنقل في ساعة الذروة وفي المكاتب، فإن إنشاء بيئة تضمن موثوقية البيانات الإلكترونية كان يشكل تحديا، ويشكل هذا عقبة كبيرة بشكل خاص أمام الشركات الصغيرة والمتوسطة الحجم التي لم تطبق بعد نظام العمل عن بعد.

يذكر مقر استراتيجية الأمن السيبراني أيضا العمل عن بعد في خطته السنوية لعام 2020، بالإضافة إلى ذلك، تم إعداد "إرشادات أمن العمل عن بعد (الطبعة الرابعة)"، والتي تتضمن معلومات وأمثلة على التدابير المتعلقة بدعم العمل عن بعد وضمان الأمن، كما قمنا أيضا بإنشاء مكتب مساعدة للتعامل مع الاستشارات المتخصصة فيما يتعلق بالتدابير الأمنية.

إن القانون الأساسي للأمن السيبراني هو قانون يركز على المبادئ الأساسية، ومن غير المرجح أن يكون بمثابة مرجع للشركات والأفراد لتنفيذ تدابير محددة، ومع ذلك، فإن المبادئ التوجيهية لا

تدعو الحكومات الوطنية والمحلية ومشغلي البنية التحتية فحسب، بل تدعو أيضا الشركات والأفراد إلى اتخاذ الاحتياطات اللازمة لضمان الأمن السيبراني وإعادة النظر في عملياتهم وأنماط حياتهم.[118]

الفقرة الثانية: القانون الأساسي للأمن السيبراني باليابان

من أجل تعزيز سياسات الأمن السيبراني بطريقة شاملة وفعالة، يحدد القانون الأساسي للأمن السيبراني المبادئ الأساسية، ويوضح مسؤوليات الأمة، وينص على صياغة استراتيجية للأمن السيبراني وغيرها من الأمور الأساسية لهذه السياسات.

يتضمن القانون الأساسي للأمن السيبراني الياباني من الفصل الأول الأحكام العامة (المواد من 1 إلى 11)، الفصل الثاني استراتيجية الأمن السيبراني (المادة 12)، الفصل الثالث: السياسات الأساسية (المواد من 13 إلى 24)، الفصل الرابع: المقر الاستراتيجي للأمن السيبراني (المواد من 25 إلى 37)، الفصل الخامس العقوبات (المادة 38)، الأحكام التكميلية، وسنسرد تاليا كل ما سبق كما يلي:

أولا: الأحكام العامة (الفصل الأول)

أ- *الغرض (المادة 1)* في ضوء الوضع الراهن الذي أصبح فيه ضمان الأمن السيبراني مع ضمان التدفق الحر للمعلومات مسألة ملحة نظرا لتفاقم التهديدات التي يتعرض لها الأمن السيبراني عالميا نتيجة لتطور الإنترنت وشبكات المعلومات والاتصالات المتقدمة الأخرى، والتقدم المحرز في استخدام تكنولوجيا المعلومات والاتصالات وفقا لما تنص عليه المادة 2 من القانون الأساسي لتشكيل المجتمع الرقمي (القانون رقم 35 لعام 2021).

بالإضافة إلى التغيرات الأخرى في الظروف المحلية والدولية، يهدف هذا القانون إلى إرساء مبادئ أساسية لتدابير الأمن السيبراني في اليابان، وتوضيح مسؤوليات الحكومات الوطنية والمحلية، وتحديد المسائل الأساسية لصياغة استراتيجية للأمن السيبراني وتدابير أخرى للأمن السيبراني، بالإضافة إلى إنشاء مقر استراتيجي للأمن السيبراني، وبالتالي تعزيز تدابير الأمن السيبراني بشكل شامل وفعال بالتزامن مع القانون نفسه، بهدف تعزيز حيوية الاقتصاد والمجتمع وتنميتهما المستدامة، وتحقيق مجتمع يمكن للناس فيه العيش بأمان وراحة بال، وكذلك المساهمة في لضمان السلام والأمن للمجتمع الدولي وأمن اليابان.

---

[118] *ما هو "القانون الأساسي للأمن السيبراني"؟ شرح واضح لخلفيته ومحتوياته*، تاريخ النشر: 2025/01/27، على موقع JBS: https://www.jbsvc.co.jp/useful/security/cyber-security-fundamental-law.html، تاريخ الاطلاع: 2025/09/13، على الساعة 22:46 مساء.

ب- *تعريف (المادة 2)* في هذا القانون، يعني "الأمن السيبراني" اتخاذ التدابير اللازمة لمنع تسرب أو فقدان أو إتلاف المعلومات المسجلة أو المرسلة أو المنقولة أو المستلمة بتنسيقات إلكترونية أو مغناطيسية أو غيرها من التنسيقات التي لا يمكن إدراكها بالإدراك البشري، وغيرها من التدابير اللازمة للإدارة الآمنة لهذه المعلومات، وكذلك التدابير اللازمة لضمان سلامة وموثوقية أنظمة المعلومات وشبكات المعلومات والاتصالات (بما في ذلك التدابير اللازمة لمنع الأضرار الناجمة عن الأنشطة غير المصرح بها ضد أجهزة الكمبيوتر من خلال شبكات المعلومات والاتصالات، أو وسائط التسجيل للسجلات المصنوعة بتنسيقات كهرومغناطيسية، والحفاظ على هذا الوضع وإدارته بشكل صحيح.

ت- الفلسفة الأساسية

نظرا لأن تطوير الإنترنت وشبكات المعلومات والاتصالات المتقدمة الأخرى، وضمان التدفق الحر للمعلومات من خلال استخدام تكنولوجيا المعلومات والاتصالات، أمران مهمان للتمتع بحرية التعبير، وخلق الابتكار، وتعزيز الحيوية الاقتصادية والاجتماعية، فإنه يجب تعزيز تدابير الأمن السيبراني بهدف الاستجابة بشكل استباقي للتهديدات التي تواجه الأمن السيبراني من خلال التعاون بين مجموعة متنوعة من الجهات الفاعلة، بما في ذلك الحكومة الوطنية والحكومات المحلية ومشغلي البنية التحتية الاجتماعية الحيوية (المادة 3) .

1. يجب أن يهدف تعزيز سياسات الأمن السيبراني إلى تعميق الوعي بالأمن السيبراني بين كل مواطن وتشجيعهم على اتخاذ تدابير طوعية، مع تعزيز الجهود بشكل استباقي لمنع الأضرار الناجمة عن تهديدات الأمن السيبراني وبناء نظام قوي يمكنه التعافي بسرعة من أي ضرر يحدث كلية.
2. ويجب أن يتم تعزيز سياسات الأمن السيبراني بهدف تعزيز الجهود الرامية إلى تطوير الإنترنت وغيرها من شبكات المعلومات والاتصالات المتقدمة، وبناء مجتمع اقتصادي نابض بالحياة من خلال استخدام تكنولوجيا المعلومات والاتصالات.
3. ونظرا لأن الاستجابة للتهديدات التي تواجه الأمن السيبراني تشكل تحديا مشتركا للمجتمع الدولي، وأن الاقتصاد والمجتمع الياباني يعملان في بيئة دولية مترابطة بشكل وثيق، فإن تعزيز سياسات الأمن السيبراني يجب أن يتم وفقا للتعاون الدولي، بهدف لعب دور قيادي في تشكيل وتطوير نظام دولي بشأن الأمن السيبراني.
4. إن تعزيز سياسات الأمن السيبراني يجب أن يأخذ في الاعتبار المبادئ الأساسية للقانون الأساسي بشأن تشكيل المجتمع الرقمي.

5. عند الترويج لسياسات الأمن السيبراني، لا بد من الحرص على تجنب المساس غير المبرر بحقوق المواطنين.

ث- *مسؤوليات الدولة (المادة 4)* تقع على عاتق الدولة مسؤولية صياغة وتنفيذ سياسات شاملة فيما يتعلق بالأمن السيبراني وفقا للمبادئ الأساسية المنصوص عليها في المادة السابقة.

ج- *مسؤوليات الحكومات المحلية (المادة 5)* وتقع على عاتق الحكومات المحلية مسؤولية صياغة وتنفيذ سياسات الأمن السيبراني الخاصة بها وفقا للمبادئ الأساسية مع مراعاة التقسيم المناسب للأدوار مع الحكومة الوطنية.

ح- *مسؤوليات مشغلي البنية التحتية الحيوية (المادة 6)* وفقا للمبادئ الأساسية، ومن أجل تقديم خدماتهم بطريقة مستقرة ومناسبة، يجب على مشغلي البنية التحتية الاجتماعية الحيوية تعميق اهتمامهم وفهمهم لأهمية الأمن السيبراني، والسعي إلى ضمان الأمن السيبراني بشكل مستقل واستباقي، والتعاون مع تدابير الأمن السيبراني التي تنفذها الحكومات الوطنية والمحلية.

خ- *مسؤوليات الشركات ذات الصلة بالإنترنت والشركات الأخرى (المادة 7)* يجب على الشركات المرتبطة بالإنترنت (أي تلك التي تعمل في تطوير الإنترنت وشبكات المعلومات والاتصالات المتقدمة الأخرى، واستخدام تكنولوجيا المعلومات والاتصالات، أو الشركات المتعلقة بالأمن السيبراني؛ وينطبق الأمر نفسه أدناه) والشركات الأخرى أن تسعى، وفقا للمبادئ الأساسية، إلى ضمان الأمن السيبراني بطريقة طوعية واستباقية فيما يتعلق بأنشطتها التجارية، وأن تسعى إلى التعاون مع تدابير الأمن السيبراني التي تنفذها الحكومات الوطنية أو المحلية.

د- *مسؤوليات المؤسسات التعليمية والبحثية (المادة 8)* وفقا للمبادئ الأساسية، يجب على الجامعات والمؤسسات التعليمية والبحثية الأخرى أن تسعى بشكل مستقل واستباقي إلى ضمان الأمن السيبراني، وتنمية الموارد البشرية المتعلقة بالأمن السيبراني، وإجراء البحوث حول الأمن السيبراني ونشر نتائج هذه البحوث، فضلا عن السعي إلى التعاون مع التدابير المتعلقة بالأمن السيبراني التي تنفذها الحكومات الوطنية أو المحلية.

ذ- *الجهود الوطنية (المادة 9)* وفقا للمبادئ الأساسية، يتعين على الجمهور أن يسعى إلى تعميق اهتمامه وفهمه لأهمية الأمن السيبراني واتخاذ الاحتياطات اللازمة لضمان الأمن السيبراني.

ر- *الاجراءات التشريعية وغيرها (المادة 10)* يتعين على الحكومة أن تتخذ التدابير التشريعية والمالية والضريبية وغيرها من التدابير اللازمة لتنفيذ سياسات الأمن السيبراني.

ز- *تطوير التنظيمات الإدارية وغيرها (المادة 11)* عند اتخاذ التدابير المتعلقة بالأمن السيبراني، يجب على الحكومة الوطنية أن تسعى جاهدة إلى تحسين التنظيمات والعمليات الإدارية.

ثانيا: استراتيجية الأمن السيبراني (الفصل الثاني)

من أجل تعزيز سياسات الأمن السيبراني بشكل شامل وفعال، يجب على الحكومة وضع خطة أساسية للأمن السيبراني "استراتيجية الأمن السيبراني".

كما يجب أن تحدد استراتيجية الأمن السيبراني الأمور التالية: السياسة الأساسية بشأن تدابير الأمن السيبراني؛ المسائل المتعلقة بضمان الأمن السيبراني في الهيئات الإدارية الوطنية؛ المسائل المتعلقة بتعزيز ضمان الأمن السيبراني بين مشغلي البنية التحتية الاجتماعية الحيوية والمنظمات التي ينظمونها، وكذلك الحكومات المحلية (المشار إليها فيما يلي باسم "مشغلي البنية التحتية الاجتماعية الحيوية، إلخ").

بالإضافة إلى الأمور المذكورة في الفقرات الثلاث السابقة، فإن الأمور الضرورية لتعزيز تدابير الأمن السيبراني بشكل شامل وفعال هي: يتعين على رئيس الوزراء أن يسعى للحصول على قرار من مجلس الوزراء بشأن استراتيجية الأمن السيبراني المقترحة؛ عندما تقوم الحكومة بصياغة استراتيجيتها للأمن السيبراني، يتعين عليها إبلاغها إلى البرلمان دون تأخير ونشرها عبر الإنترنت أو غير ذلك من الوسائل المناسبة، ويجب على الحكومة أن تسعى إلى اتخاذ التدابير اللازمة لتنفيذ استراتيجية الأمن السيبراني بسلاسة، مثل إدراج مثل هذه الأموال في الميزانية لكل سنة مالية، في حدود المالية الوطنية، من أجل تأمين الأموال اللازمة للنفقات المطلوبة لتنفيذها (المادة 12)

ثالثا: التدابير الأساسية (الفصل الثالث)

أ- ضمان الأمن السيبراني في الأجهزة الإدارية الوطنية، وغيرها

ب- تعزيز ضمان الأمن السيبراني بين مقدمي البنية التحتية الاجتماعية الحيوية

ت- تعزيز الجهود التطوعية من قبل الشركات الخاصة والمؤسسات التعليمية والبحثية

ث- التعاون بين مختلف الجهات

ج- مجلس الأمن السيبراني (المادة 17) يقوم المدير العام لمقر الاستراتيجية الأمنية السيبرانية ووزراء الدولة المكلفين من قبله بتنظيم مجلس الأمن السيبراني لعقد المشاورات اللازمة فيما يتعلق بتعزيز سياسات الأمن السيبراني.

ح- مكافحة الجريمة ومنع انتشار الأضرار.

خ- الاستجابة للحوادث التي قد يكون لها تأثير كبير على أمن اليابان.

د- تعزيز الصناعة وتعزيز القدرة التنافسية الدولية (المادة 20).

ذ- تعزيز البحث والتطوير (المادة 21).

ر- تأمين الموارد البشرية.

ز- تعزيز التعليم والتعلم والتوعية العامة.

س-تعزيز التعاون الدولي (المادة 24).

رابعا: المقر الاستراتيجي للأمن السيبراني (الفصل الرابع)

من أجل تعزيز سياسات الأمن السيبراني بشكل شامل وفعال، ستقوم الحكومة بإنشاء مقر استراتيجي للأمن السيبراني (المادة 25).

أ- الواجبات التابعة

تتولى الإدارة العامة المهام التالية: المسائل المتعلقة بإعداد مقترحات استراتيجية الأمن السيبراني وتعزيز تنفيذها؛ المسائل المتعلقة بوضع معايير لتدابير الأمن السيبراني في الوكالات الإدارية الوطنية والوكالات الإدارية المستقلة والشركات المعينة، فضلا عن تقييم (بما في ذلك التدقيق) السياسات القائمة على تلك المعايير وتعزيز تنفيذ سياسات أخرى قائمة على تلك المعايير؛ المسائل المتعلقة بتقييم التدابير المتخذة في حالة وقوع حوادث أمنية سيبرانية خطيرة في الهيئات الإدارية الوطنية أو الهيئات الإدارية المستقلة أو الشركات المعينة (بما في ذلك التحقيقات لتحديد الأسباب)؛ تنسيق الاتصال مع الأطراف ذات الصلة في اليابان والخارج في حالة وقوع حادث يتعلق بالأمن السيبراني.

بالإضافة إلى المسائل المذكورة في الفقرات السابقة، يكون هذا المكتب مسؤولا عن التحقيق والمناقشة بشأن تخطيط سياسات الأمن السيبراني المهمة، والخطط المشتركة بين الوزارات، وصياغة تقديرات التكلفة للوكالات الإدارية ذات الصلة والمبادئ التوجيهية لتنفيذ السياسات، وتقييم السياسات، وغيرها من المسائل المتعلقة بتعزيز وتنسيق تنفيذ هذه السياسات بشكل عام، وعندما تنوي أي قيادة صياغة استراتيجية للأمن السيبراني، يتعين عليها أولا طلب رأي مجلس الأمن القومي، وسوف يتعاون المقر الرئيسي بشكل وثيق مع مجلس الأمن القومي بشأن قضايا الأمن السيبراني المهمة المتعلقة بالأمن القومي لليابان (المادة 26).

ب- **منظمة:** يتألف المقر الرئيسي من المدير العام لمقر استراتيجية الأمن السيبراني، ونائب المدير العام لمقر استراتيجية الأمن السيبراني، وأعضاء مقر استراتيجية الأمن السيبراني (المادة 27).

ت- رئيس المقر الاستراتيجي للأمن السيبراني

يتولى رئاسة المقر المدير العام للمقر الاستراتيجي للأمن السيبراني، الذي يكون أمين عام مجلس الوزراء، ويكون لرئيس المقر السيطرة الكاملة على شؤون المقر ويوجه ويشرف على موظفي دائرته، ويجوز للمدير العام للمقر (المادة 28) .

ث- نائب رئيس مقر استراتيجية الأمن السيبراني (المادة 29).

ج- **أعضاء المقر الاستراتيجي للأمن السيبراني (المادة 30)** يجب أن يكون لدى المقر الرئيسي أعضاء المقر الاستراتيجي للأمن السيبراني، ويكون أعضاء المقر الرئيسي من الأشخاص التاليين (باستثناء من يقع ضمن البنود من 1 إلى 6 ويتم تعيينهم كنائبين للرئيس): رئيس اللجنة الوطنية للسلامة العامة، وزير الشؤون الرقمية، وزير الداخلية والاتصالات، وزير الخارجية، وزير الاقتصاد والتجارة والصناعة، وزير الدفاع، بالإضافة إلى المذكورين في الفقرات السابقة، أي وزير دولة آخر غير رئيس ونائب رئيس المقر يعينه رئيس الوزراء كشخص يعتبر ضروريا بشكل خاص لتنفيذ شؤون المقر، ويتم تعيين شخص من قبل رئيس الوزراء من بين الأفراد ذوي المعرفة والخبرة المتميزة في مجال الأمن السيبراني.

ح- **تكليف الأعمال (المادة 31)** يجوز للقيادة العامة أن تعهد ببعض الشؤون المذكورة أدناه إلى الأشخاص المحددين مقابلها حسب تصنيف الشؤون: المقتصرة على تلك المتعلقة بالتدقيق على أساس معايير تدابير الأمن السيبراني في الوكالات الإدارية المستقلة والشركات المعينة؛ المقتصرة على تلك المتعلقة بالتحقيقات لتوضيح أسباب الأحداث الخطيرة المتعلقة بالأمن السيبراني التي وقعت في الوكالات الإدارية المستقلة أو الشركات المعينة؛ وكالة تعزيز تكنولوجيا المعلومات واليابان والمنظمات الأخرى التي حددتها الحكومة بأنها تمتلك القدرات التقنية الكافية والمعرفة المتخصصة والخبرة في مكافحة الأمن السيبراني والقادرة على تنفيذ المهام المذكورة بشكل موثوق؛ وكذا شركة تم تعيينها بموجب مرسوم حكومي بأنها تمتلك القدرات التقنية الكافية والمعرفة والخبرة المتخصصة للاتصال والتنسيق مع الأطراف ذات الصلة في اليابان والخارج في حالة وقوع حادث يتعلق بالأمن السيبراني، وقادرة على تنفيذ هذه الواجبات بشكل موثوق.

2 المادة 16-3 لا يجوز لموظف أو مستخدم في شركة أوكلت إليه أعمال بموجب أحكام الفقرة السابقة، أو لمن شغل مثل هذا المنصب، أن يفشي أو يسيء استعمال أي سر اطلع عليه فيما يتصل بالأعمال الموكلة إليه دون مبرر مقبول.

3 ويعتبر أي موظف أو مسؤول في شركة أوكلت إليه أعمال بموجب أحكام الفقرة 1 ويشارك في الأعمال المتعلقة بهذه التكليف موظفا يعمل في الخدمة العامة وفقا للقوانين والأنظمة لغرض تطبيق قانون العقوبات (القانون رقم 45 لسنة 1907) وأحكام العقوبات الأخرى.

أ- **توفير المواد وغيرها (المادة 32)** يجب على رؤساء الهيئات الإدارية ذات الصلة، وفقا لما تحدده المقر الرئيسي، تزويد المقر الرئيسي بالمواد أو المعلومات المتعلقة بالأمن السيبراني والتي من شأنها أن تساهم في أداء المقر الرئيسي لواجباته في الوقت المناسب.

ب- **تقديم المواد والتعاون الآخر:** عندما يرى المقر الرئيسي أنه من الضروري لأداء واجباته، يجوز له أن يطلب من رؤساء الحكومات المحلية والهيئات الإدارية المستقلة، ورؤساء أو رؤساء هيئات الجامعات الوطنية، ومديري هيئات معاهد البحوث المشتركة بين الجامعات، ورئيس مركز الدعم القانوني الياباني، وممثلي الشركات العامة والشركات المعتمدة التي يعينها المقر الرئيسي، وممثلي المنظمات ذات الصلة التي تتصل وتنسق مع الأطراف المحلية والأجنبية في حالة وقوع حادث أمن سيبراني، تقديم المواد اللازمة، وإبداء الآراء، وتقديم التوضيحات، والتعاون بطريقة أخرى فيما يتعلق بالتدابير التي يجب اتخاذها بالتعاون مع الحكومة الوطنية لمنع انتشار الأضرار الناجمة عن تهديدات الأمن السيبراني وضمان التعافي السريع من هذه الأضرار، وغيرها من تدابير الأمن السيبراني، في هذه الحالة يجب على الشخص الذي يتلقى الطلب أن يمتثل للطلب ما لم يكن هناك سبب مبرر لعدم القيام بذلك (المادة 33).

خامسا: العقوبات (الفصل الخامس)

يعاقب بالحبس مدة لا تزيد على سنة أو بغرامة لا تزيد على خمسمائة ألف ين كل شخص أيا كان أو كان يعمل في شؤون مجلس الوزراء أن يفشي أو يسيء استخدام أي سر اطلع عليه بشأن الأمن السيبراني دون سبب مبرر (المادة 38) .

سادسا: الأحكام التكميلية.[119]

[119] القانون الأساسي للأمن السيبراني، القانون رقم 104 لسنة 2014، ساري المفعول اعتبارا من 17 يونيو 2022، على موقع e-GOV البحث القانوني: https://laws.e-gov.go.jp/law/426AC1000000104، تاريخ الاطلاع: 2025/09/13، على الساعة 22:52 مساء.

الفصل الثاني: التطبيقات الإلكترونية وسياسة الخصوصية على ضوء قانون حماية البيانات الشخصية كوريا الجنوبية نموذجا

بتاريخ 2024/06/03، التحقت بالوكالة الحضرية بتطوان بصفتي طالبة باحثة لقضاء فترة التدريب، ارتباطا بمجال بحثي الأكاديمي ألا وهو قانون الرقمنة والمعاملات الإلكترونية، وبالتالي اطلعت على سياسة الخصوصية للبوابة الإلكترونية للوكالة الحضرية بتطوان باعتبارها تطبيقا محليا، ثم على سياسة خصوصية لتطبيق وطني وهو تطبيق رخص.

من هنا سأعمل على التعرف على المهام التي تقوم بها الوكالة الحضرية والتطبيقات المحلية والوطنية التي تستعملها لتقديم خدماتها إلكترونيا، ومواردها البشرية في قسم تكنولوجيا المعلومات، ثم التوصيات التي قدمتها الموارد البشرية للقسم السابق ذكره، وبعدها سأعمل على الاجتهاد في ضبط بعض النواقص إن صح التعبير لسياسة خصوصية البوابة الإلكترونية للوكالة.

يستخدم المستخدمون تطبيقات إلكترونية من أجل الحصول على خدمات إلكترونية، على سبيل المثال: رخصة البناء، من هذا المنطلق سأعمل على التعريف بموقع إدارتي وموقع بياناتي الموازية لها، وكذا المنصة الحاضنة *حكومة 24* بكوريا الجنوبية، إلا أننا سنبتعد عن تطبيق الإجراءات الإلكترونية هنا لضيق المساحة، ونكتفي بالإحالة على الفيديوهات التعليمية التي تقدمها هاته المواقع في شكل واضح وسلس باللغتين العربية والفرنسية، وأخرى بالموقع الرسمي.

كما سأعمل على التعريف بتطبيق إدارة المباني بكوريا الجنوبية الذي يقوم بنفس الدور الذي يقوم به موقع رخص بالمغرب، وعلى غراره سأكتفي بالتعريف بالتطبيقات دون الإجراءات التي اشتغلت عليها لموقع إدارة المباني والتي ناهزت 100 صفحة لوحدها، إلا أنها نفس الإجراءات المقدمة من قبل موقع رخص المغربي باستثناء الاختلاف في التفاصيل، زائد عليها إجراء واحد مختلف مرتبط بالشهادة الخضراء.

توفر *حكومة24* خدمات حكومية متكاملة ومعلومات سياسية كانت تقدمها كل وكالة في السابق بشكل منفصل، بحيث يمكن استخدامها من نافذة واحدة، ويتكون من ثلاث قوائم: *الخدمات الحكومية، والشكاوى المدنية 24، ومعلومات السياسة*،[120] وتمثل كل من اللجنة الوطنية لحماية البيانات الشخصية بالمغرب، مؤسسة وسيط المملكة، موقع الرئاسة العامة للشكايات الالكترونية، البوابة

[120] *حكومة 24*: https://www.gov.kr/portal/main/nologin، تاريخ الاطلاع: 2025/09/13، على الساعة 22:55 مساء.

الوطنية للشكايات، والمديرية العامة للأمن الوطني لموقعها الالكترونية شكاية، مؤسسات يمكن تبليغها عن وقوع تسريب أو انتهاك للبيانات الشخصية بالمغرب (المبحث الأول).

تمثل سياسة الخصوصية للبوابات والتطبيقات الإلكترونية، الحصن الحصين لحقوق هاته المواقع، مع حفظ حقوق المواطنين والمواطنات، لذلك سنعمل التعرف على سياسة لخصوصية لموقع *حكومة 24* الكوري الذي يوازي *موقع إدارتي* من حيث الكينونة والطبيعة، ، على أن نجدد التذكير بأن موقع إدارتي بالمغرب ليس له سياسة خصوصية، كما تجدر الإشارة إلى أن سياسة الخصوصية لموقع *حكومة 24* ينطبق على موقع إدارة الوثائق المعمارية بكوريا الجنوبية وجميع المنصات والمواقع والبوابات الإلكترونية بكوريا الجنوبية بناء على قانون حماية البيانات الشخصية.

تقوم *الحكومة 24* (المشار إليها فيما يلي باسم "*Government24*")[121]، بمعالجة المعلومات الشخصية وإدارتها بشكل قانوني وآمن وفقا لقانون حماية المعلومات الشخصية والقوانين واللوائح ذات الصلة لحماية حرية وحقوق أصحاب المعلومات، وبناء على ذلك، ووفقا للمادة 30 من قانون حماية البيانات الشخصية، تم وضع سياسة معالجة البيانات الشخصية التالية والإفصاح عنها لإعلام أصحاب البيانات بإجراءات ومعايير معالجة البيانات الشخصية والتعامل مع الشكاوى المتعلقة بها بسرعة وسلاسة.

لقد عانت كوريا الجنوبية من عدة أحداث ووقائع تم فيها تسريب الخصوصية، في أيام معدودات، سنعرف فيما بعد تفاصيل الأحداث وأسباب هذا التسريب، وكذلك الردود التي سجلتها الحكومة آنذاك.

يمكن تبليغ هيئات حماية البيانات الشخصية بكوريا الجنوبية عن تسرب أو انتهاك لهاته الحقوق، في كل من لجنة حماية البيانات الشخصية بكوريا الجنوبية، نظام الوساطة في حل نزاعات المعلومات الشخصية، قسم التحقيق في الجرائم الإلكترونية التابع لمكتب المدعي العام الأعلى، مركز الاستجابة للإرهاب السيبراني التابع لوكالة الشرطة الوطنية، إلا أنه حينما يتعلق الأمر برفع دعوى قضائية فعلى الأغلب يتم رفع دعوى قضائية جماعية وفقا لقانون حماية البيانات الشخصية بكوريا الجنوبية، أما قانون 08-09 لازال لم يضم بين طياته هاته الجزئية وتتم الإحالة على قانون المسطرة المدنية (المبحث الثاني).

---

[121] سياسة معالجة المعلومات الشخصية لنظام إدارة البناء التابع لوزارة الأراضي والبنية التحتية والنقل، متوفر على موقع(*Seumteo*) : https://www.eais.go.kr/moct/awp/aha01/AWPAHA01V01، تاريخ الاطلاع: 2025/09/13، على الساعة 22:57 مساء.

المبحث الأول: التطبيقات الإلكترونية بالمغرب وكوريا الجنوبية

قدم فريق قسم تكنولوجيا المعلومات بالوكالة الحضرية بتطوان المهام والعمليات المنوطة بالوكالة، والعمليات التي يقوم بها هذا الفريق خاصة، واحتياجات المستخدم وتحليلا للنظام المعلوماتي للوكالة الحضرية، وعرض توصياته في تقرير داخلي يضم مجموعة من المراحل؛ عبر فيها عن الحلول التكنولوجية والرقمية المطلوبة لصالح الوكالة الحضرية بتطوان وحتى بفرعها في شفشاون.

إن كان التحول نحو الجهوية مبدئيا ومؤسساتيا، لكن تبقى على تجهيزاتها وكينونتها وحتى مهامها قائمة، وبالتبع ما تحمله من تطلعات نحو التحسين والتطوير للأفضل، لذلك سنبرز عصارة التقرير الداخلي للوكالة عن طريق التوصيات الهامة.

كل هذا برز خلال محنة كوفيد-19، منحة رقمية ولدت من رحم الوكالة الحضرية بتطوان، ألا وهي البوابة الإلكترونية للوكالة الحضرية تطوان، باعتبارها موقعا محليا يقدم مجموعة من الخدمات الإلكترونية للمواطنين حتى لا تقف عجلة مصالحهم وبالتالي مصالح الاقتصاد الوطني والتنمية (المطلب الأول).

للحكومة الإلكترونية عدة أوجه، تظهر في عدة أشكال هي البوابات، التطبيقات، والمنصات الإلكترونية طبعا، من هنا اختصارا *موقع إدارتي* الذي يشترك مع جميع التطبيقات الأخرى (المقصود هنا موقع رخص – البوابة الإلكترونية للوكالة الحضرية) سواء المحلية منها والوطنية في وثيقة رخصة البناء، ويمكن الجزم بشبيه *موقع إدارتي* في المغرب منصة *حكومة 24* في كوريا الجنوبية.

في إطار خدمات الحكومة الإلكترونية في جمهورية كوريا عام 2017، قامت وزارة الداخلية والأمن بدمج أنظمة الحكومة الإلكترونية مثل الشكاوى المدنية 24، وبوابة حكومة جمهورية كوريا، وAlladrim، والتي كانت متناثرة في السابق عبر عدة وزارات، في نظام واحد، وأسمته *"حكومة 24"*، وتوفر *حكومة24* خدمات حكومية متكاملة ومعلومات سياسية، كانت تقدم كل خدمة في السابق بشكل منفصل، بحيث يمكن استخدامها من نافذة واحدة، وتتكون من ثلاث قوائم: الخدمات الحكومية، والشكاوى المدنية 24، ومعلومات السياسة والذي يعد شبيها بموقع *إدارتي* المغربي (المطلب الثاني).

المطلب الأول: التحول الرقمي للوكالة الحضرية بتطوان وسياسة خصوصيتها

سنعمد للإطار العام والقانوني للوكالة الحضرية بتطوان، المؤسسة التي خضت بها تدريبي الميداني، للتعرف على مهامها المنوطة بها، ثم النظر في آلياتها ونتائج جودة الأداء بعام 2022،

إضافة إلى أهم ما يمكن التطرق له وهو تفعيل التدبير اللامادي والتحول الرقمي بمشروع تحديث للبوابة الإلكترونية لهاته الوكالة، على عدة مستويات العملياتية منها والتواصلية، وكذا الإعلاميات والإدارة الإلكترونية، وقبل التطرق لبعض الخدمات الإلكترونية للوكالة الحضرية بتطوان، مع الإشارة إلى مشروع قانون انتقال الوكالات الحضرية لوكالات جهوية للتعمير والإسكان.

كما يستخدم موظفو الوكالة الحضرية بتطوان على غرار موظفي الوكالات الحضرية بالمغرب مواقع وطنية مثل موقع رخص، كذلك بعض المؤسسات الأخرى مثل العمالات والجماعات الحضرية، ... في استخداماتهم الوظيفية، والأخرى الاستخدامات الشخصية كمواطنين وأجانب، من هذا المنطلق سأعمل على التعريف بموقع رخص وموقع نظام إدارة المباني بكوريا الجنوبية، لأن له ارتباط برخصة البناء الوثيقة التي تقدمها الوكالة الحضرية، والتعريف بموقع *إدارتي*، وحكومة *24* بكوريا الجنوبية، كل هذا في إطار المقاربة لا المقارنة، إلا أننا سنبتعد عن تطبيق الإجراءات الإلكترونية هنا لضيق المساحة ونكتفي بالإحالة على الفيديوهات التعليمية التي تقدمها هاته المواقع في شكل واضح وسلس باللغتين العربية والفرنسية (الفقرة الأولى).

ثم التعرف على الموارد البشرية في قسم تكنولوجيا المعلومات بالوكالة، الأدوار المنوطة بهم، ومؤهلاتهم، مع العمل على التحليل الكمي والنوعي لموظفي قسم تكنولوجيا المعلومات، ومن تم ضمان الجودة، المراقبة القانونية، طلب الشكاوى، انتقاء من التقرير الداخلي الذي أعده فريق تكنولوجيا المعلومات بالوكالة، الذي ضم بعد أن ترجمته من اللغة الفرنسية إلى اللغة العربية ما يعادل 170 صفحة، بالتالي كان من المستحيل إدراجه بكليته في هذا التقرير الذي بين أيدينا فآثرت أن أضحي بمعظمه مقابل القليل منه، مع الأخذ بتوصيات الفريق وإدراجها هنا (الفقرة الثانية).

الفقرة الأولى: الوكالة الحضرية بتطوان وبوابتها الإلكترونية كتطبيق محلي

سنتعرف على الوكالة الحضرية بتطوان المكان الذي قضيت مدة تدريبي بها، وارتباطا بموضوع التقرير سأعمل بالتعريف البوابة الإلكترونية للوكالة الحضرية تطوان باعتبارها تطبيقا محليا.

أولا: الوكالة الحضرية بتطوان

سأعمد إلى الوكالة الحضرية بتطوان، وإطارها العام والقانوني، وآليات تدخلها.

1. التعريف بالوكالة الحضرية بتطوان

الوكالة الحضرية لتطوان هي مؤسسة عمومية تتمتع بالشخصية المعنوية والاستقلال المالي، يشمل نطاق اختصاصها كلا من إقليم تطوان، إقليم شفشاون، عمالة المضيق الفنيدق، وتخضع لوصاية وزارة إعداد التراب الوطني والتعمير والإسكان وسياسة المدينة.

يتشكل الهيكل الإداري للوكالة الحضرية لتطوان على أساس المقر الرئيسي بمدينة تطوان والفرع في مدينة شفشاون، يعمل مع 55 بلدية بما في ذلك 6 بلديات حضرية و49 بلدية قروية، إذ يمتد نطاق عمله على مساحة إجمالية قدرها 7768 كيلومتر مربع.

تسهر مديرة[122] الوكالة الحضرية لتطوان على تدبير شؤون الوكالة.

2. الإطار القانوني للوكالة الحضرية لتطوان والمهام المنوطة بها

تم إنشاء الوكالة الحضرية لتطوان بموجب مرسوم رقم 361-97-2، بتاريخ 27 جمادى الثانية 1418 (30 أكتوبر 1997)[123]، تنفيذا للظهير الشريف بمثابة قانون رقم 51-93-1 بتاريخ 22 ربيع الأول 1414 (10 سبتمبر 1993 المحدث للوكالات الحضرية)[124].

وفقا لمضمون المادة 3 من الظهير الذي ينصب على قانون رقم 51-93-1، فإن الوكالات الحضرية هي المسؤولة في حدود اختصاصاتها لمجالها الترابي[125] على:

- إنجاز الدراسات اللازمة لبلورة مخططات توجيه التهيئة العمرانية ومتابعة تنفيذ التوجهات المحددة فيها.
- برمجة مشاريع التهيئة المتعلقة بتحقيق أهداف مخططات توجيه التهيئة العمرانية.
- إعداد مشاريع وثائق التعمير التنظيمية لاسيما تصاميم التنطيق، تصاميم التهيئة ومخططات النمو.
- إعطاء الموافقة خلال مدة أقصاها شهر واحد على جميع مشاريع التجزيئات، المجموعات السكنية، التقسيم والمباني والتي يجب أن تنقل إليها من قبل السلطات المختصة.
- مراقبة مطابقة التجزيئات والتقسيمات والمجموعات السكنية والمباني في طور الانجاز مع الأحكام التشريعية والتنظيمية الجاري بها العمل ومع رخص التجزئ والتقسيم وإنشاء مجموعات سكنية أو البناء.

---

[122] AGENCE URBAINE DE TÉTOUAN ,PRÉSENTATION, QUI SOMMES NOUS ?, [En ligne] : https://aute.gov.ma/presentation/01/, (consulté le 13 septembre 2024- 18 :30pm).

[123] مرسوم رقم 2.97.361 صادر في 27 من جمادى الآخرة 1418 (30 أكتوبر 1997) يتعلق بالوكالات الحضرية للعيون ومكناس وتطوان ووجدة وآسفي-الجديدة والقنيطرة – سيدي قاسم وسطات وتازة، على الرابط التالي: https://2u.pw/qHay0GJR، تم الاطلاع عليه بتاريخ: 2024/09/13، على الساعة 18:51 مساء.

[124] ظهير شريف رقم 51-93-1 صادر في 22 من ربيع الأول 1414 (10 سبتمبر 1993) معتبر بمثابة قانون يتعلق بإحداث الوكالات الحضرية، على الرابط التالي: https://2u.pw/d7D6Kr6j، بتاريخ: 2025/06/29، على الساعة 22:23 مساء.

[125] مهام الوكالات الحضرية، موقع الكتروني لفدرالية الوكالات الحضرية بالمغرب، على الرابط التالي: https://www.federation-majal.ma/ar/Missions ، تم الاطلاع عليه بتاريخ: 2024/09/13، على الساعة 10:20 ليلا.

- إنجاز الدراسات المتعلقة بمشاريع تهيئة القطاعات الخاصة وتنفيذ جميع مشاريع الصيانة أو التهيئة نيابة عن الدولة أو السلطات المحلية أو أي شخص عام أو خاص الذين يطلبون ذلك عندما يكون المشروع ذو منفعة عامة.
- تعزيز وتنفيذ عمليات التأهيل الحضري والتجديد العقاري وإعادة الهيكلة للأحياء التي تخلو من مرافق البنية التحتية، ولهذه الغاية إنجاز دراسات الحصول على الخصائص الضرورية لهذه العمليات.
- المساهمة مع المقاولات التي تتوافق أنشطتها مع الأهداف المسندة إلى الوكالة الحضرية.
- تعزيز بمساعدة الهيئات المنتخبة، إنشاء وتنمية مجموعة الملاكين ووضع رهن إشارتهم الأطر اللازمة لتسهيل تنفيذ وثائق التعمير، لاسيما خلق جمعيات الاتحاد بموجب التشريع الجاري به العمل في هذا المجال، ومتابعة العمليات المنجزة من طرف هذه الجمعيات بالتنسيق مع المجالس الجماعية المذكورة.
- تقديم المساعدة التنقية إلى السلطات المحلية في مجال التعمير والتهيئة والفاعلين بالقطاع العام والخاص الذين يطلبون ذلك في عملياتهم للتهيئة.
- جمع ونشر جميع المعلومات حول التنمية الحضرية في العمالات والمجالات داخل المجال الترابي للوكالة.

3- آليات تدخل الوكالة الحضرية لتطوان ونتائج جودة الأداء لسنة 2022[126]

تتجلى آليات تدخل الوكالة الحضرية لتطوان فيما يلي:

- إنجاز دراسات استشرافية لبلوة رؤية من أجل الرفع من جاذبية وتنافسية المجال من خلال إعداد المخطط التوجيهي للتهيئة العمرانية لتطوان الكبير.
- تقنين استعمال الأرض من خلال تعميم التغطية بجيل جديد من وثائق التعمير تتميز بالنجاعة والفعالية.
- معالجة الأحياء ناقصة التجهيز من خلال إعداد تصاميم إعادة الهيكلة.
- المحافظة على التراث المعماري والطبيعي عبر تفعيل مواثيق الهندسة المعمارية والمشهدية.

[126] تقرير المجلس الإداري للوكالة الحضرية لتطوان، الدورة التاسعة عشر-2023، الوكالة الحضرية لتطوان، وزارة إعداد التراب الوطني والتعمير والإسكان وسياسة المدينة، ص: 14-15، على الرابط التالي: https://aute.gov.ma/s/a/library/2023-09-15/60915818-942e-4541-ac80-aa36c6b3e5c6.pdf ، تم الاطلاع عليه بتاريخ: 2024/09/15، على الساعة 17:03 مساء.

ثانيا: تفعيل التدبير اللامادي والتحول الرقمي للوكالة الحضرية بتطوان

سنتعرف على الإدارة الإلكترونية للوكالة الحضرية بتطوان وكذا الإعلاميات داخلها، والتدبير اللامادي والتحول الرقمي للوكالة الحضرية بمشاريعها الرقمية، أهمها البوابة الإلكترونية للوكالة.

أ- الإعلاميات والإدارة الالكترونية

ترتكز الإدارة الالكترونية داخل الوكالة الحضرية لتطوان على نظام معلوماتي متكامل ومترابط يسمح بالتواصل ومشاركة البيانات التعميرية وغيرها عبر مجموعة من التطبيقات والنظم المعلوماتية، الشيء الذي يساهم بفعالية في تحسين الأداء وتحقيق الكفاءة المطلوبة فيما يخص التدبير الإداري والتقني، مما يساهم في تجويد الخدمات المقدمة، بالإضافة إلى ذلك، تعزز الخدمات الرقمية المتاحة عبر البوابة الالكترونية للوكالة من تقريب الإدارة ودعم التواصل الخارجي مع المرتفقين والفرقاء.[127]

[127] نفس المرجع، ص 91.

ب- التدبير اللامادي والتحول الرقمي

استكمالا لتنزيل مضامين مخططها التوجيهي لنظام المعلومات 2020-2024، قامت الوكالة الحضرية لتطوان بإطلاق مجموعة من المشاريع المعلوماتية المهمة خلال سنة 2022،[128] من بينها:

1. مشروع تحديث البوابة الالكترونية للوكالة الحضرية لتطوان

في إطار التزامها بتبسيط أكثر للمساطير الإدارية وتعزيز أكثر لقرب الإدارة من المرتفقين والفرقاء، أطلقت الوكالة الحضرية لتطوان خلال سنة 2022 مشروع تحديث بوابتها الإلكترونية بهدف تحسين الخدمات الرقمية المقدمة وتسهيل وصول المرتفقين إلى المعلومات التعميرية.

تم تفعيل الإدارة الرقمية والتدبير اللامادي بالوكالة الحضرية بتطوان عبر اتخاذ الإجراءات المعتمدة أسفله لضمان استمرارية خدماتها في ظل الأزمة الصحية الاستثنائية الناتجة عن وباء كورونا:

- ✓ على المستوى العملياتي

اعتمدت الوكالة الحضرية لتطوان تقنية الاشتغال عن بعد لدراسة والبث في ملفات طلبات رخص التعمير كما وفرت لشركائها إمكانية الاستفادة من العديد من الخدمات الالكترونية التي توفرها المنصة الرقمية للوكالة مثل:

- الاطلاع على وثائق التعمير المصادق عليها بفضل البوابة الجغرافية التي تتضمن مختلف المقتضيات المتعلقة بالتنطيقات ومحارم الطرق والتجهيزات وقواعد البناء بالمناط المشمولة بوثائق التعمير.
- التدبير اللامادي لمسطرة مذكرة المعلومات التعميرية لتمكين المرتفقين من تقديم طلب الحصول على المذكرة إلكترونيا.
- المعالجة الالكترونية للشكايات عبر إيداعها والتوصل بالجواب عنها عبر البريد الالكتروني.
- الدراسة القبلية للملفات: إمكانية إيداع الملفات عبر المنصة والتوصل بالملاحظات القبلية.

[128] نفس المرجع، ص 92-93.

كما يوفر الموقع الالكتروني للوكالة إمكانية تصفح المراجع القانونية في ميدان التعمير وكذلك الوثائق والمستجدات الصادرة عن الوكالة، وقد وضعت الوكالة رهن إشارة مرتفقيها رموز الاستجابة السريعة QR CODES قصد تسهيل الولوج لمختلف هذه الخدمات.[129]

✓ على المستوى التواصلي

ضمانا منها لاستمرارية الخدمات العمومية المقدمة للمرتفقين والشركاء وضعت الوكالة الحضرية لتطوان رهن إشارة العموم أرقاما هاتفية وبوابة إلكترونية من أجل مواكبة جميع المشاريع والمبادرات الاستثمارية.

2. وسائل التواصل والخدمات الالكترونية عن بعد الخاصة بالوكالة الحضرية لتطوان

تقدم الخدمات الالكترونية ويتم التواصل عن بعد عبر تطبيقات وبرامج محلية ووطنية بالوكالة الحضرية لتطوان، حيث تتمثل التطبيقات المحلية في الموقع الالكتروني للوكالة الحضرية لتطوان، وما تتوفر عليه من خدمات الكترونية من إيداع الشكايات، الدراسة القبلية للملفات، حجز المواعيد، الاطلاع على وثائق التعمير المصادق عليها، الاطلاع على النصوص القانونية، استمارة الرضى، ربط الاتصال، طلبات العروض، صفحة التواصل الاجتماعي، وتطبيقات وطنية كل من بوابة المعلومات التعميرية، والمنصة الرقمية رخص.

- التوقعات

يضم البرنامج التوقعي للوكالة الحضرية لتطوان حول التدبير اللامادي والتحول الرقمي خلال فترة 2024-2026 مجموعة من المشاريع في الجانب المرتبط بالتدبير اللامادي والتحول الرقمي، من مشروع نظام تدبير التخطيط الحضري، ومشروع دعم نظام الأمن السيبراني لحماية الأنظمة والشبكات والبرامج ضد الهجمات الرقمية، ومشروع نظام تدبير الاحصائيات والمؤشرات الحضرية.[130]

مشاريع التدبير اللامادي والتحول الرقمي 2024-2026

[129] بلاغ صحفي تفعيل الإدارة الرقمية والتدبير اللامادي من أهم الإجراءات المعتمدة من طرف الوكالة الحضرية لتطوان لضمان استمرارية خدماتها في ظل الأزمة الصحية الاستثنائية الناتجة عن وباء كورونا (كوفيد19)، متوفر على الرابط التالي: https://autetouan.ma/web/uploads/dossier/5e984c4fc8131.pdf ، تم الاطلاع عليه بتاريخ: 2024/09/15، على الساعة 21:16 مساء.

[130] تقرير المجلس الإداري للوكالة الحضرية لتطوان، مرجع سابق، ص 114.

2024	2025	2026
مشروع نظام تدبير التخطيط الحضري	مشروع دعم نظام الأمن السيبراني لحماية الأنظمة والشبكات والبرامج ضد الهجمات الرقمية	مشروع نظام تدبير الاحصائيات والمؤشرات الحضرية
يهدف هذا المشروع إلى تبسيط إدارة دراسات التخطيط الحضري خصوصا تتبع إعداد وثائق التعمير، حيث سيسهل إدارة مختلف مراحل وتواريخ الإنجاز مع الأخذ بالاعتبار فهرسة وأرشفة الآراء والملاحظات والاقتراحات والطلبات والتعديلات التي تهم كل دراسة.	يهدف هذا المشروع إلى حماية سلامة بيانات المؤسسة والمحافظة عليها وإتاحة الوصول الآمن إليها.	يهدف هذا المشروع إلى تسهيل إدارة البيانات والجداول الإحصائية للوكالة من خلال إحداث مؤشرات إحصائية ولوحات قيادة لدعم عملية أخذ القرار.

أ- مشروع قانون انتقال الوكالات الحضرية لوكالات جهوية للتعمير والإسكان

يتجه المغرب وفق مشروع قانون إلى إحداث 12 وكالة جهوية للتعمير والإسكان[131] بدلا عن 30 وكالة حضرية، وتحل الأولى محل الثانية في جميع حقوقها والتزاماتها، والنقل المجاني للممتلكات العقارية والمنقولة إليها، فضلا عن نقل الموظفين والمستخدمين، مع احتفاظهم بحقوقهم المكتسبة، فيما يتعلق بوضعهم القانوني ونظام التقاعد الذي ينتمون إليه، بمعنى أن الغاية الارتقاء بأدوار ومهن الوكالات الحضرية، وتعزيز آلية الحكامة وخلق قطب خاص بالعالم القروي، وكذا الارتقاء بالموارد المالية والبشرية.

تفعيلا للتوجيهات الملكية التي دعت إلى "الإسراع بإطلاق إصلاح عميق للقطاع العام، ومعالجة الاختلالات الهيكلية للمؤسسات والمقاولات العمومية، قصد تحقيق أكبر قدر من التكامل والانسجام في مهامها"، وتنزيلا لمخرجات جلسة العمل التي ترأسها الملك بتاريخ 17 أكتوبر 2023 والتي

[131] بلاغ للديوان الملكي، الثلاثاء 17 أكتوبر 2023، وزارة إعداد التراب الوطني والتعمير والإسكان وسياسة المدينة: https://2u.pw/fVumLpxy، تم الاطلاع بتاريخ 2024/09/14، على الساعة 18:34 مساء.

خصصت لقطاع التعمير والإسكان، وتفعيلا للتوصيات المنبثقة عن الحوار الوطني حول التعمير والإسكان، وعن المجلس الأعلى للحسابات بخصوص إعادة تموقع الوكالات الحضرية، كما جاء في ديباجة مشروع القانون.

صادق مجلس الحكومة يوم الأربعاء 26 يونيو 2025، على مشروع القانون رقم 64.23 المتعلق بإحداث الوكالات الجهوية للتعمير والإسكان، في خطوة تروم إعادة هيكلة قطاع التعمير وتفعيل الجهوية المتقدمة.[132]

نص مشروع القانون على إحداث مؤسسة عمومية تحت مسمى "الوكالة الجهوية للتعمير والإسكان" على صعيد كل جهة من جهات المملكة، تتمتع بالشخصية الاعتبارية والاستقلال المالي، مع إحداث تمثيليات للوكالة الجهوية على صعيد عمالة أو إقليم أو أكثر، كلما اقتضت الضرورة ذلك، ويهدف هذا المشروع قانون إلى:

- تعزيز اختصاصات ومهام الوكالات الجهوية، لاسيما في مجال التخطيط الترابي ودعم التنمية ومواكبة الاستثمار واليقظة الترابية، وتفعيل السياسة الوطنية لدعم الولوج إلى السكن، إضافة إلى ترشيد تشكيل مجالس إدارة الوكالات الجهوية بما يحقق الفعالية والنجاعة، وتعزيز مهامها.
- التنصيص على إحداث لدى مجلس إدارة الوكالة الجهوية مجلسا للتوجيه والتتبع يتولى دراسة وإبداء الرأي في استراتيجيات التنمية الترابية الجهوية، وفي كل القضايا المتعلقة بالسياسة العامة للدولة في ميادين إعداد التراب الوطني والتعمير والإسكان وسياسة المدينة المعروضة على مجلس إدارة الوكالة.

جاءت الأحكام الختامية والانتقالية لمشروع قانون بكيفية حلول الوكالات الجهوية محل الوكالات الحضرية والمصالح اللاممركزة لوزارة إعداد التراب الوطني والتعمير والإسكان وسياسة المدينة في جميع حقوقها والتزاماتها، والنقل المجاني للممتلكات العقارية والمنقولة إليها، فضلا عن نقل الموظفين والمستخدمين، مع احتفاظهم بحقوقهم المكتسبة، فيما يتعلق بوضعهم القانوني ونظام التقاعد الذي ينتمون إليه.

---

[132] *مجلس الحكومة يصادق على مشروع قانون إحداث الوكالات الجهوية للتعمير والإسكان*، تاريخ النشر: 2025/06/26، على موقع SNRTNEWS: https://snrtnews.com/article/129265 ، تاريخ الاطلاع: 2025/09/14 على الساعة 17:16 مساء.

يعهد إلى الوكالة الجهوية نفس المهام الموكلة للوكالات الحضرية، وتحصل الوكالة من أجل تكوين ممتلكاتها، وفق المشروع قانون على عقارات من الدولة ومن الجماعات الترابية، ويجوز لها أن تقتني العقارات المذكورة، من الجماعات الترابية أو السلالية أو من الخواص.[133]

ثالثا: التطبيقات الإلكترونية الأخرى المشتركة في رخصة البناء

يعتبر موقع إدارتي البوابة الوطنية للمساطر والإجراءات الإدارية بالمغرب، ومن بينها إجراءات المتعلقة بالبناء والسكن والعقار، على سبيل المثال: رخصة البناء، مع التعرف على الإطار القانوني للخدمات الإلكترونية لموقع إدارتي، كما سنعمد إلى النظر في بعض المنصات والتطبيقات للحكومة الإلكترونية بكوريا الجنوبية، فيما يتعلق بالخدمات العمومية المقدمة من قبل منصة إلكترونية بكوريا تدعى بـ*حكومة 24*، والتي سنعمل على تعريفها، والتعرف على الخدمات التي تقدمها دون الدخول في تفصيلة الإجراءات الإلكترونية، مع إبراز المميزات التي تزخر بها منصة *حكومة 24* بكوريا الجنوبية المرادفة *لموقع إدارتي* المغربي، كما سنعمل على التعريف بموقع رخص المغربي وشبيهه بموقع نظام إدارة المباني *-نظام سوميتيو-* بكوريا الجنوبية.

أ- *موقع إدارتي* تطبيق وطني

موقع إدارتي البوابة الوطنية للمساطر والإجراءات الإدارية بالمغرب، ومن بينها إجراءات المتعلقة بالبناء والسكن والعقار، على سبيل المثال: رخصة البناء، وملاحظة هامة متعلقة بهذا الموقع أنه لا يتوفر على خاصية سياسة الخصوصية، وعلى أي قريبا سيتم إطلاق نسخة جديدة من البوابة.

1- التعرف على *موقع إدارتي*

إدارتي هي الفضاء الالكتروني الرسمي الوحيد، للحصول على جميع المعلومات المتعلقة بالخدمات الإدارية ولإنجاز المعاملات الإدارية المتعلقة بها، تضم هذه البوابة حصريا المساطر والقرارات الإدارية التي صادقت عليها اللجنة الوطنية للمساطر والإجراءات الإدارية، وسيتم تحديثها وتجديد مضمونها بشكل تدريجي بكل القرارات المصادق عليها من نفس اللجنة، واستكمالا لمكونات

[133] مذكرة تقديمية لمشروع القانون رقم ... يتعلق بإحداث الوكالات الجهوية للتعمير والإسكان، المملكة المغربية وزارة إعداد التراب الوطني والتعمير والإسكان وسياسة المدينة الوزيرة، نسخة منشورة على صفحة الأستاذ كريم لملوج موثق في مراكش على موقع لينكدن: https://2u.pw/Cwas501Q ، تم الاطلاع عليه بتاريخ: 2024/09/14، على الساعة 18:47 مساء.

هذه البوابة، سيتم تفعيل خاصية التبادل البيني للمستندات والوثائق والبيانات، وكذا الفضاء المعاملاتي في وقت لاحق.[134]

2- الإطار القانوني للخدمات الالكترونية *بموقع إدارتي*

يهدف القانون رقم 20-43 المتعلق بخدمات الثقة بشأن المعاملات الإلكترونية إلى تحديد النظام المطبق على: خدمات الثقة بشأن المعاملات الإلكترونية؛ وسائل وخدمات التشفير وتحليل الشفرات؛ والعمليات المنجزة من قبل مقدمي خدمات الثقة والقواعد الواجب التقيد بها من لدن هؤلاء ومن لدن أصحاب الشهادات الإلكترونية، ويحدد كذلك هذا القانون اختصاصات السلطة الوطنية لخدمات الثقة بشأن المعاملات الإلكترونية،[135] وكذلك القانون رقم 08-09 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي.

ب- منصة *الحكومة 24* بكوريا الجنوبية

في إطار خدمات الحكومة الإلكترونية في جمهورية كوريا عام 2017، قامت وزارة الداخلية والأمن بدمج أنظمة الحكومة الإلكترونية مثل *الشكاوى المدنية 24*، وبوابة حكومة جمهورية كوريا، وAlladrim، والتي كانت متناثرة في السابق عبر عدة وزارات، في نظام واحد، وأسمته *"حكومة 24"*، وتقدم *حكومة 24* خدمات متكاملة مثل ربط الخدمات الإدارية للحكومة والحكومات المحلية والمؤسسات العامة وإصدار وثائق العرائض المدنية المختلفة[136].

حكومة 24 هي عبارة عن منصات الإدارة العامة، بمعنى منصة خدمات، مكونة من "نظام الاستخدام المشترك للمعلومات الإدارية" كمنصة توزيع البيانات، وهناك "منصة متكاملة لإدارة البيانات على مستوى الحكومة" لتحليل البيانات، بالإضافة إلى ذلك البيانات الوصفية والبيانات الرئيسية، وقد تم إنشاء نظام لكل وظيفة، كل هذا جزء من مجموع المنصات التي تشكل المنصة الرقمية للحكومة بكوريا الجنوبية، أما باقي المنصات الأخرى فهي منصات البيانات التي يمكن للقطاع الخاص الوصول إليها بحرية تشمل بوابات البيانات العامة، ومنصات البيانات الضخمة،

---

[134] *إدارتي*: https://idarati.ma/ ، تاريخ الاطلاع: 2025/06/29، على الساعة 22:23 مساء.

[135] القانون رقم 20-43 المتعلق بخدمات الثقة بشأن المعاملات الإلكترونية، موقع المديرية العامة لأمن نظم المعلومات إدارة الدفاع الوطني المملكة المغربية: https://www.dgssi.gov.ma/ar/alqanwn-rqm-20-43-almtlq-bkhdmat-althqt-bshan-almamlat-alalktrwnyt، تاريخ الاطلاع: 2025/06/29، على الساعة 22:23 مساء.

[136] *حكومة 24*، مرجع سابق.

ومراكز الذكاء الاصطناعي وهناك منصات كبيرة وصغيرة تم تشكيلها بشكل مستقل من قبل الحكومات المحلية وكل مؤسسة.[137]

تتميز حكومة *24* بعدة ميزات بشكل مختصر كما يلي: من الممكن إصدار المستندات المدنية بسهولة حتى من الخارج؛ لا توجد أي تكلفة؛ يمكن حفظ مستندات الشكوى المدنية الصادرة عبر الإنترنت كملفاتPDF ؛ ويمكن استخدامه في أي وقت وفي أي مكان، بغض النظر عما إذا كان على جهاز كمبيوتر أو جهاز محمول.[138]

ت- *موقع رخص* المغربي *ونظام الإدارة المعمارية* بكوريا الجنوبية

موقع رخص يعتبر الشباك الوطني الوحيد لرخص الإدارات الترابية، ويستخدمه آلاف المستعملين داخل المغرب وخارجه منصة رخص للحصول بسرعة وسهولة على التراخيص اللازمة لأنشطتهم الاقتصادية والعمرانية، بشكل رقمي 100%، مواكبة كاملة من بداية الإجراء إلى نهايته.

ث- الإطار القانوني لموقع رخص

القرار المشترك لوزارة الداخلية ووزارة إعداد التراب الوطني والتعمير والإسكان وسياسة المدينة ووزير الصناعة والتجارة والاقتصاد الأخضر الرقمي رقم 338.20 الصادر في 25 من جمادى الأولى 1441 (21 يناير 2020) يحدد كيفيات تفعيل مساطر التدبير اللامادي المتعلقة بإيداع ودراسة طلبات الرخص ورخص السكن وشواهد المطابقة وتسليمها .

ج- *موقع إدارة المباني* بكوريا الجنوبية

يشير *(Seumteo)* الذي يستخدمه موظفو الحكومة الالكترونية إلى جانب المواطنين والشركات في الخدمات الالكترونية ضمن مجال التعمير والإسكان داخل إطار الشراكة والتعاون، إلى نظام يسمح للأشخاص بتقديم الشكاوى المدنية المتعلقة بالهندسة المعمارية وإدارة الإسكان بسهولة، في أي وقت، وفي أي مكان عبر الإنترنت، والتي كانت مهمة معقدة وصعبة في الماضي، من خلال رقمنة جميع أعمال إدارة المبنى، حيث يوفر 114 نوعا مختلفا من خدمات الإدارة المعمارية، بما في ذلك

---

[137] يساهم إطلاق خدمة بياناتي العامة في ابتكار جديد في الحكومة الرقمية، بيان صحفي لوزارة الإدارة العامة والأمن -كوريا الجنوبية، العدد الصباحي 210225، قسم توزيع البيانات العامة، وزارة الإدارة العامة والأمن، 2021، على موقع KDI: https://eiec.kdi.re.kr/policy/materialView.do?num=210954&topic=&pp=20&datecount=&recommend=&pg=، تاريخ الاطلاع: 2025/09/13، على الساعة 11:07 مساء.

[138] حكومة *24*، مرجع سابق.

إصدار سجلات البناء (حوالي 700 ألف حالة سنويا)، وتراخيص البناء والسكن، والخدمات الإحصائية، وتقدم الخدمات (حوالي 64 مليون خدمة سنويا).

ووفقا لخطة تطوير المؤسسات العامة التي وضعتها الحكومة، تم إنشاء شركة كوريا للأراضي وشركة كوريا الوطنية للإسكان للمساهمة في تنمية الاقتصاد الوطني من خلال حل المهام المتداخلة مثل مشاريع تطوير مواقع الإسكان التي تنفذها شركة كوريا لاند والمؤسسة الوطنية للإسكان وتحسين كفاءة الإدارة.[139]

الفقرة الثانية: الموارد البشرية بالوكالة الحضرية بتطوان والتحديات _قسم المعلوماتية

سنتعرف في هاته الفقرة الموارد البشرية في قسم المعلوماتية بالوكالة الحضرية بتطوان، خاصة وأننا نتعامل مع تطبيقات إلكترونية كموضوع للتقرير (أولا)، ثم التحديات التي تواجهها الوكالة الحضرية بتطوان في مشروع دراسة نظام المعلومات والتخطيط لتطويره (ثانيا).

أولا: الموارد البشرية المعلوماتية للوكالة الحضرية لتطوان

ترتكز مهام قسم تكنولوجيا المعلومات، حول توفير وظيفة تكنولوجيا المعلومات داخل الوكالة الحضرية لتطوان (*AUTE*) من خلال خدمة تكنولوجيا المعلومات، ويرتبط قسم تكنولوجيا المعلومات بإدارة الوكالة، والسمات الرئيسية لنظام المعلومات (SI) بما يلي: تحديد الاستراتيجية والتوجه العام لـ SI وGIS للوكالة الحضرية؛ تطوير وتنفيذ برنامج عمل الخدمة؛ تنفيذ مشاريع التطوير على أساس احتياجات المستخدمين؛ التنسيق المستمر مع المدير ؛ الاهتمام بإدارة فريق القسم والتأكد من الإشراف الوظيفي عليهم؛ مراقبة التطورات التكنولوجية لتكنولوجيا المعلومات؛ إدارة نظام المعلومات؛ إدارة نظام المعلومات الجغرافية؛ المشاركة في الحصول على تكنولوجيا المعلومات والموارد التقنية؛ إدارة الموارد البشرية والمادية المتاحة للخدمة؛ الصيانة الوقائية والتصحيحية (البرمجيات والأجهزة)؛ وإدارة موقع *AUTE* والمساحة الخاصة.

يتكون قسم تكنولوجيا المعلومات بالوكالة الحضرية بتطوان، على النحو التالي: السيدة المديرة، رئيس قسم تكنولوجيا، فني تكنولوجيا المعلومات (وحدة نظم المعلومات: – فني لشبكة الكمبيوتر وجوانب الصيانة، ثلاثة فنيين مخصصين لوحدة نظم المعلومات الجغرافية، ولإدخال ورقمنة الملفات وPPs للوكالة الحضرية).

---

[139] رخص، على الموقع التالي: https://rokhas.ma/ ، تاريخ الاطلاع 2025/07/11، على الساعة 11:22 صباحا.

تدور الوظائف والخدمات المختلفة لقسم تكنولوجيا المعلومات حول: إدارة البوابة الجغرافية؛ إدارة الموقع؛ إدارة الخدمات الإلكترونية؛ تنفيذ مشاريع نظم المعلومات الجغرافية الخارجية؛ إدارة تطبيقات نظم المعلومات الجغرافية وBDG؛ نظام المعلومات؛ خدمة إعلامية؛ الإحصاء ورسم الخرائط؛ إدارة معدات تكنولوجيا المعلومات؛ مراقبة مشاريع؛ تكنولوجيا المعلومات؛ حفظ البيانات؛ أمن تكنولوجيا المعلومات؛ الصيانة التصحيحية والوقائية؛ توسعة وتجديد.

1- مسؤوليات رئيس قسم تكنولوجيا المعلومات

تنقسم مسؤوليات رئيس قسم تكنولوجيا المعلومات إلى قسمين مكون نظام المعلومات ومكون نظام المعلومات الجغرافية (GIS):

- مكون نظام المعلومات:

فيما يتعلق بإدارة نظام المعلومات، تكون مسؤوليات رئيس القسم، كما يلي:

- ✓ تحديد الأهداف وبرنامج العمل واتجاهات نظام المعلومات AUTE؛
- ✓ تقييم احتياجات المستخدم من حيث تطبيقات الكمبيوتر وتطوير CPS؛
- ✓ إدارة وإدارة نظام المعلومات AUTE وشبكة الكمبيوتر.
- ✓ ضمان الاتصال بين قسم تكنولوجيا المعلومات والإدارات الأخرى في الوكالة؛
- ✓ ضمان إدارة ورصد التدخلات التي تتم على معدات تكنولوجيا المعلومات؛
- ✓ ضمان إدارة ومراقبة الصيانة التصحيحية والوقائية لمعدات تكنولوجيا المعلومات؛
- ✓ تحديد وتنفيذ إجراءات حماية أصول تكنولوجيا المعلومات؛
- ✓ المشاركة في الحصول على تكنولوجيا المعلومات والموارد التقنية؛
- ✓ ضمان الإدارة التقنية للموقع الإلكتروني للوكالة الحضرية؛
- ✓ المساعدة والدعم الفني (الأجهزة والبرامج) للمستخدمين؛
- ✓ جدولة تركيب معدات الشبكة الجديدة والكابلات اللازمة؛
- ✓ رفع مستوى الوعي لدى كافة الموظفين بمخاطر الإنترنت.
- ✓ الحفاظ على سلامة وسرية معلومات AUTE.

- مكون نظام المعلومات الجغرافية (GIS).

يتمتع رئيس القسم أيضا بمسؤوليات وصلاحيات فيما يتعلق بنظم المعلومات الجغرافية:

- ✓ تحديد خطة عمل المعلومات الجغرافية وفقا لاحتياجات AUTE؛
- ✓ وضع البنود الفنية لاستراتيجية الشراكة لمشاريع نظم المعلومات الجغرافية المستقبلية؛

- ✓ المراقبة الفنية لمكاتب التصميم المسؤولة عن تطوير حلول نظم المعلومات الجغرافية؛
- ✓ تحديد احتياجات مشروع نظم المعلومات الجغرافية (البيانات والأساليب والمهارات والجدول الزمني...)؛
- ✓ تنفيذ وإدارة نظم المعلومات الجغرافية الخاصة بـ AUTE؛
- ✓ متابعة وحدة نظم المعلومات الجغرافية المسؤولة عن تزويد قاعدة البيانات الجغرافية التقاط ورقمنة وأرشفة الملفات الإلكترونية؛
- ✓ مراقبة المسح الضوئي وإضفاء الطابع المادي على وثائق تخطيط المدن والخطط والخرائط وما إلى ذلك، والانتقال إلى تنسيق نظم المعلومات الجغرافية.
- ✓ التحكم في جودة البيانات الجغرافية لـ BDG؛
- ✓ إنتاج الخرائط المواضيعية والمعالجة الجغرافية المكانية والإحصاءات المكانية.[140]

2- مسؤوليات فنيي خدمات تكنولوجيا المعلومات

تقني خدمات تكنولوجيا المعلومات مسؤولون بشكل أساسي عن مسح ملفات البناء (المشاريع الكبيرة، المشاريع الصغيرة) والأقسام الفرعية: المستندات، والخطط، والخرائط، وما إلى ذلك.

- ✓ مسؤوليات فنيي الشبكة

مسؤوليات تقني الشبكة هي كما يلي:

- المساعدة والدعم الفني للمستخدمين (عن بعد أو في الموقع) بهدف تحسين استخدام معدات تكنولوجيا المعلومات وتشغيل البنية التحتية للشبكة؛
- تركيب واستكشاف الأخطاء وإصلاحها وصيانة معدات تكنولوجيا المعلومات (المعدات والأجهزة والبرامج والأجهزة الطرفية، ...)؛
- تحديد الحوادث وإعادة صياغة طلبها وحل أعطال الكمبيوتر: إرسال التعليمات عبر الهاتف أو التحكم عن بعد أو السفر إذا لزم الأمر؛

[140] Bilan, diagnostic et plan d'amélioration de l'infrastructure systèmes, réseaux, SGBD et messagerie. Phase 1 : Analyse et évaluation de l'existant et identification des axes stratégiques. ETUDE D'ELABORATION DU SCHEMA DIRECTEUR DU SYSTEME D'INFORMATION 2020-2024 DE L'AGENCE URBAINE DE TETOUAN. AGENCE URBAINE DE TETOUAN. Ministère de l'Aménagement du Territoire National, de l'Urbanisme, de l'Habitat et de la Politique de la Ville. Royaume du Maroc. Etude d'élaboration du Schéma Directeur des Systèmes d'Information 2020-2024 pour Urbaine de Tétouan. IL Consultant. Réf. : AUTE-SDSI-P1-BDPA.p :11.

- مراقبة حسن سير العمل في الخوادم والوصول إلى الشبكة: تحديد التنبيهات ومراقبتها، ومراقبة التدفقات والتدخل في حالة حدوث مشكلة (الاقتحام، أو الخلل، ...)، والتحكم.
- في النسخ الاحتياطية؛
- إجراء نسخ احتياطية لمحطات العمل والخوادم؛
- تركيب معدات الشبكة الجديدة والكابلات اللازمة؛ تكوين معدات الشبكة (جهاز التوجيه، والمحول، ...)؛
- منع حالات الشذوذ والفشل في تشغيل الشبكة؛
- تحديث برامج مكافحة الفيروسات والحفاظ على أمن نظام المعلومات.

✓ واجبات فنيي إدخال البيانات

مسؤوليات فنيي نظم المعلومات الجغرافية هي كما يلي:

- الإمداد المستمر بنظام المعلومات الجغرافية AUTE وضمان تحديثه عن طريق إدخال جميع المعلومات الضرورية ورقمنتها؛
- توريد قاعدة البيانات الجغرافية؛
- إدخال البيانات ورقمنة ملفات البناء (GP، PP) والأقسام الفرعية؛
- فهرسة الملفات؛
- الأرشفة الإلكترونية لملفات البناء والتقسيم.
- المساهمة في أعمال ترحيل بيانات CAD إلى نظم المعلومات الجغرافية؛
- المساهمة في تطوير Future-Modules-GIS؛
- المشاركة في ورش عمل نظم المعلومات الجغرافية والجيوماتكس.[141]

3- التحليل الكمي والنوعي وتقييم موظفي خدمة تكنولوجيا المعلومات

ينقسم تحليل موظفي قسم تكنولوجيا المعلومات إلى مجالين هما؛ التحليل الكمي، مما يتيح تقييم أرقام الخدمة ومقارنتها بالأرقام الملحوظة بشكل عام في المؤسسات المشابهة لـ AUTE، والتحليل النوعي، مما يجعل من الممكن تقييم تدريب ومؤهلات وملاءمة الموظفين للمهام الموكلة إليهم.

✓ التحليل الكمي لموظفي قسم تكنولوجيا المعلومات:

يتيح التحليل الكمي لعدد موظفي قسم تكنولوجيا المعلومات صياغة التقييمات التالية:

---

[141] ibid.p :12.

- يتكون موظفو تكنولوجيا المعلومات في AUTE من مصدرين بالإضافة إلى سكرتير مسؤول عن مسح الملفات بالإضافة إلى وحدة نظم المعلومات الجغرافية المسؤولة عن رقمنة وإدخال الملفات المختلفة في نظام المعلومات الجغرافية نيابة عن قسم الإدارة الحضرية؛
- لا يمكن اعتبار موظفي وحدة نظم المعلومات الجغرافية كموظفي تكنولوجيا المعلومات، حيث تتعلق أنشطتهم بإدخال ملفات الأعمال نيابة عن قسم GU؛
- تقدر النسبة الفعالة لعلماء الكمبيوتر فيما يتعلق بإجمالي القوى العاملة في AUTE (77) بـ2.6% (77/2)، وهذا المعدل أقل من المعدل الوطني البالغ 3%[142] الذي لوحظ بين الإدارة العامة؛
- لا توجد وظيفة RSSI (توجيهات DNSSI)، ومع ذلك، يمكن دعم هذه الوظيفة من قبل المدير المسؤول عن الإشراف وإدارة النظام والشبكات.

✓ التحليل النوعي لموظفي DSI

يغطي هذا التحليل النوعي عدة أبعاد: التدريب الأولي، والمهارات والخبرات المتاحة لموظفي تكنولوجيا المعلومات الحاليين (انظر الملحق 3 للاطلاع على السير الذاتية المصغرة للموارد)، وتتجلى النقاط التالية:

- مستوى التدريب الأساسي لموظفي تكنولوجيا المعلومات في قسم تكنولوجيا المعلومات مرتفع نسبيا:
  - مورد (رئيس قسم تكنولوجيا المعلومات) مهندس دولة بمستوى Bac +5؛
  - أحد الموارد (المسؤول عن الشبكة) هو تقني متخصص في نظم المعلومات بمستوى Bac +2، ومع ذلك، يتم تعويض الدورة الأساسية بدبلوم الدورة المتقدمة.
- تتمتع موارد قسم تكنولوجيا المعلومات بخبرة 8 سنوات لرئيس القسم و13 عاما لمدير الشبكة، ولذلك فإن موظفي تكنولوجيا المعلومات لديهم خبرة كبيرة تمكنه من القيام بالمهام التي يتولى مسؤوليتها.

[142] راجع رسم خرائط استخدام تكنولوجيا المعلومات والاتصالات في القطاعات العامة www.mmsp.gov.ma، بتاريخ: 2025/06/29، على الساعة 22:24 مساء.

- رئيس القسم لديه 5 سنوات من الأقدمية داخل AUTE، وهذا يتيح لهم من ناحية التعرف على المهن ومن ناحية أخرى معرفة تاريخ وتطورات نظام المعلومات والحصول على رؤية مستقبلية ومتطورة لنتائجه.[143]

ثانيا: التحديات التي تواجهها الوكالة الحضرية بتطوان في مشروع دراسة نظام المعلومات والتخطيط لتطويره

تتوزع التحديات التي يواجهها مشروع دراسة نظام المعلومات والتخطيط لتطويره بالنسبة للوكالة من حيث:

- الإدارة:

يعد إنشاء نظام معلومات فعال يسمح للمديرين بفهم الحوادث وأعطال الخدمة في وقت قصير جدا أمرا حاسما سواء من وجهة نظر اتخاذ القرار أو من وجهة نظر التحسين والحفاظ على الأداء.

- الصورة:

تخضع الخدمات التي تقدمها الوكالة لتغييرات كبيرة، لا سيما فيما يتعلق بالفوائد والخدمات الناجمة عن الأهداف التي حددتها AUTE وهي تخضع للتحسينات من حيث الاستجابة وجودة الخدمة المقدمة، دراسة تفصيلية للوضع الحالي وتحديد الاحتياجات وتحديد التوجهات الاستراتيجية تحليل وتقرير تقييم للوضع الحالي والاحتياجات.[144]

- الإنتاجية:

فتح التطبيقات على وظائف دعم القرار، والإمكانيات التي توفرها تكنولوجيات المعلومات الجديدة (الخدمات عن بعد)، وزيادة أتمتة العمليات، وتحسين سرعة وسهولة استغلال البيئة، وما إلى ذلك، ينبغي أن تتيح تحسين إنتاجية موظفي الوكالة بشكل كبير.

- المكاسب المالية:

---

[143] Bilan, diagnostic et plan d'amélioration de l'infrastructure systèmes, réseaux, SGBD et messagerie. Phase 1 : Analyse et évaluation de l'existant et identification des axes stratégiques. Opicit, p :12-13.

[144] Rapport d'analyse et d'évaluation de l'existant et des besoins. Phase 1 : Analyse et évaluation de l'existant et identification des axes stratégiques, opicit, p :5.

على الرغم من أن البحث عن زيادة الربحية ليس هو السبب وراء هذه الدراسة، فمن المتوقع أن يتم التعبير عن الانعكاسات الإيجابية للنظام الجديد أيضا من حيث المكاسب المالية، لا سيما بسبب الاستخدام الأفضل للموارد البشرية التي يمكن أن تنجم عن زيادة أتمتة العمليات واستبدال البنى التحتية والأنظمة والمعدات القديمة والمكلفة بأخرى أحدث وأقل تكلفة.

- المصداقية:

تشكل الدعوة إلى تقنيات جديدة، وبنية تطبيقات معيارية ومتكاملة، عوامل ستضمن الوكالة من خلالها زيادة موثوقية الخدمة، المرتبطة أيضا بتحسين أداء النظام[145].

المطلب الثاني: الاحتياجات والتوصيات بالوكالة الحضرية تطوان

سنبرز احتياجات المستخدم في الجانب المرتبط بتكنولوجيا المعلومات التابعة للوكالة الحضرية بتطوان وفرع شفشاون، ثم المخاطر التي تنضوي على الخدمات المقدمة ورقيا والتحليل الشامل لنظام المعلومات، مع التحليل الشامل للنظام المعلوماتي الحالي بالوكالة الحضرية تطوان (الفقرة الأولى)، ثم التطرق إلى التوصيات بشأن الوكالة الحضرية بتطوان سياسة خصوصية بوابتها الإلكترونية وأمنها السيبراني (الفقرة الثانية).

الفقرة الأولى: الاحتياجات والتحديات الطبيعية والتحليل الشامل للنظام المعلوماتي بالوكالة الحضرية

سنبرز في الجدول أسفله احتياجات المستخدم في الجانب المرتبط بتكنولوجيا المعلومات التابعة للوكالة الحضرية بتطوان وفرع شفشاون، ثم المخاطر التي تنضوي على الخدمات المقدمة ورقيا والتحليل الشامل لنظام المعلومات، مع التحليل الشامل للنظام المعلوماتي الحالي بالوكالة الحضرية تطوان.

أولا: احتياجات المستخدم

عملية الأعمال	
	الاحتياجات
الإدارة الحضرية	• تطوير وتنفيذ تطبيق نظم المعلومات الجغرافية على شبكة الإنترنت لإدارة معالجة الملفات عن طريق إضافة المزيد من

[145] ibid, p :6.

	الضوابط المنطقية وخلفية رسم الخرائط التي تجمع جميع وثائق تخطيط المدن وصور الأقمار الصناعية وجميع المعلومات اللازمة لمعالجة الملفات. • الأرشفة: يستغرق البحث عن الملفات وقتا طويلا، ومن هنا تأتي الحاجة إلى رقمنة الأرشيف، حتى تلك التي كانت قبل عام 2014؛ • ويجب أيضا رقمنة تعليمات الملف وتحميلها في نظام المعلومات الجغرافية وإرفاقها بالملفات الخاصة بها؛ • تطوير وتنفيذ وحدة إدارة الطلب؛ • أعرب مديرو الأقسام عن الحاجة إلى وجود وحدة لتحميل تقارير المراقبة فيما يتعلق بنظام المعلومات الجغرافية، علاوة على ذلك، فإن تقارير المراقبة التي قامت بها السلطات المحلية لا تحتوي على إحداثيات تحديد موقع قطعة الأرض الخاضعة للمراقبة، تحديد الموقع الجغرافي لهذه المؤامرات يستغرق الكثير من الوقت. • الوصول المباشر إلى نظم المعلومات الجغرافية لتتمكن من استخدام البيانات المتعلقة بالمشاريع المخالفة ومتابعة تاريخها وتتبعها وتحديد قطع الأراضي...إلخ.
شؤون الأراضي القانونية	• توحيد أدوات تكنولوجيا المعلومات المستخدمة (Arc GIS وAutocad)؛ • تطوير وتنفيذ وحدة إدارة الملاحظات الاستخباراتية؛ • الحصول على معلومات بشأن الجرائم؛ • لديك محطات عمل عالية الأداء قادرة على فتح والسماح بالعمل على البطاقات التي تتطلب طاقة عالية • الحساب والمعالجة. • الحاجة إلى حل لإدارة تراث رسم الخرائط ومشاركته على مستوى الإدارات؛ • تطوير وتنفيذ وحدة إدارة الطلب.

الدراسات	• توحيد إصدارات الأدوات المستخدمة (الأوتوكاد)؛ • احصل على استشارة تفاعلية للوصول إلى قاعدة البيانات الخاصة بـالخرائط والصور والتعويضات؛ • الوصول إلى قاعدة بيانات نظم المعلومات الجغرافية (خاصة السجلات، التحقيق والضوابط والجرائم والطرود)؛ • لديك محطات عمل فعالة.[146]
الإدارية والمالية	• اقتناء وتنفيذ نظام معلومات الموارد البشرية (HRIS)، الذي يتعامل مع الإدارة الإدارية للموارد البشرية، وكشوف المرتبات، وإدارة الإجازات، ... • إنشاء مكتبة افتراضية تزود موظفي AUTE بالوثائق المتعلقة بأنشطتهم والمتاحة للوكالة. • احصل على تطبيق متكامل يسمح لك بإدارة المحاسبة العامة ومحاسبة الميزانية والأصول والمشتريات. • فيما يتعلق بتطبيق إدارة أسطول السيارات، قم بإعداد سير عمل للتحقق من أوامر المهمة وإدارتها مباشرة على التطبيق، مع إمكانية تتبع المركبات باستخدام نظام تحديد الموقع الجغرافي الذي يسمح، من بين أمور أخرى، بالإدارة والقراءات التلقائية لعدد الكيلومترات. المركبات.
فرع شفشاون	• الحصول على التراخيص اللازمة للبرنامج المراد استخدامه (Autocad وArcGis)؛ • لديك نسخة احتياطية للبريد وتتبع تطبيق "القادمون والمغادرون" مشترك مع المقر الرئيسي (سيتم تطويره بناء على تطبيق Access الذي يستخدمه الفرع بالفعل منذ عام 2015) • إعادة تصميم تطبيق الإدارة الحضرية المعتمد من قبل AUTE (Tadbir) بحيث:

[146] ibid, p :28.

	1- التأكد من مراقبة الدوائر التي تم نقل الملفات إليها داخل AUTE 2- لديهم واجهة قابلة للتخصيص وبديهية وممتعة للاستخدام. 3- توفر إمكانية التشاور واستغلال وتقييم البيانات في الوقت الحقيقي من قبل المستخدمين (مثل تطبيق Excel). 4-إمكانية إضافة أو تعديل أو حذف الحقول حسب الاحتياجات 5-توفر إمكانية استيراد وتصدير البيانات بتنسيقات أخرى • الحصول على تطبيق لمراقبة الخدمات المقدمة (مرتبط بتطبيق تدبير) • لديك تطبيق لرصد مكافحة الجرائم (مرتبط بتطبيق تدبير) • تحقيق اللامركزية في إدخال البيانات في تطبيق الإدارة الحضرية عن طريق نشر الإدخال وفقًا لسير عمل معالجة الملف: يقوم الجميع بمعالجة إدخال المعلومات المتعلقة بتدخلهم في سلسلة معالجة الملفات؛ • الحصول على جميع الخرائط والوثائق الموضوعية الموجودة للمنطقة؛ • لديك قاعدة بيانات تحتوي على قائمة شاملة مع محرك بحث للنصوص القانونية التي تغطي أو تؤثر في مجال نشاط AUTE. • قم بتزويد الفرع باتصال سريع بالإنترنت مما يسمح بالاتصال الخالي من الأخطاء بقاعدة بيانات AUTE. • رقمنة وحفظ أرشيف الهوائي (أرشيف مكتب التسجيل ومكتب المراقبة) لتسهيل تصديره.[147]

ثانيا: المخاطر التي تنضوي على الخدمات المقدمة ورقيا

أ- التغطية الوظيفية لنظام معلومات الأعمال لتجنب المخاطر

الأعمال المتاحة اليوم لـ AUTE تعتمد على تكنولوجيا وحلول ناضجة ومستدامة، ومع ذلك، يجب توفير التغطية الكاملة، وسوف تحتاج بعض الميزات إلى التطوير والتنفيذ، وينطبق هذا بشكل خاص على مذكرات المعلومات أو الطلبات أو مشاركة التراث الخرائطي، علاوة على ذلك، فإن الكثير من البيانات التي تنتجها أو تجمعها خدمات AUTE لا تزال في شكل ورقي، وهذا الوضع يضع الوكالة في خطر كبير يتمثل في فقدان المعلومات.

[147] ibid, p : 29-30.

ب- أنواع المخاطر التي تحيط بالمعلومات المضمنة في شكل ورقي

فضلا عن الاستخدام المحدود للبيانات الخاصة بالوكالة الحضرية، فإن الاحتفاظ بهذه المعلومات في شكل ورقي ينطوي على مخاطر كبيرة:

1. خطر فقدان المعلومات، يتم حفظ البيانات في الأرشيفات المادية، ولذلك، هناك خطر كبير لفقدان هذه المعلومات بسبب تدمير وسطها (الفيضانات/الرطوبة، الحرائق، التدهور بسبب الحشرات)؛
2. الاستخدام الناقص أو الاستخدام المحدود لهذه المعلومات، بسبب التأخير في البحث في الأرشيفات أو رفع السرية عن الملفات.
3. تتطلب الأرشفة الورقية أيضا مساحة تخزين كبيرة، وهي مشكلة تتزايد بمرور الوقت.
4. وستستفيد الوكالة من تحويل المعلومات المتوفرة لديها إلى نسخ إلكترونية، ولذلك ينبغي لنظام المعلومات المستقبلي أن يضمن ما يلي:

- جمع المعلومات اليوم حصريا على الورق (على سبيل المثال: تعليمات لملفات المشروع أو تقارير المراقبة الواردة من السلطات المحلية)؛
- إدارة معالجة البيانات التي لم تتم حوسبتها بعد (الضوابط)، والتي لا يزال يتم جمعها اليوم في شكل ورقي؛
- السماح بالاستحواذ التدريجي على المعلومات المتاحة للوكالة حاليا من خلال تحويلها إلى نسخة إلكترونية يمكن الوصول إليها عن طريق نظام المعلومات.

ثالثا: التحليل الشامل للنظام المعلوماتي الحالي

يكشف التحليل الذي أجري للنظام الحالي عن الملاحظات التالية:

أ- بذل قسم تكنولوجيا المعلومات الجهود لنشر التطبيقات ودعم المستخدمين، ومع ذلك، فإن بعض أنشطة قسم تكنولوجيا المعلومات تدخل ضمن المهنة (المسح الضوئي والدخول إلى تطبيق نظم المعلومات الجغرافية).

ب- لدى AUTE تطبيقات لدعم الأنشطة التجارية للمستخدمين (Urbaget وGeo Portal)، توفر هذه التطبيقات تغطية واسعة للأنشطة، كما أنها تمثل مصدرا مهما للمعلومات.

ت- ومع ذلك، لا يزال يتعين بذل الجهود لتوسيع نطاق التغطية الوظيفية للأعمال (الرقابة، والإعفاءات، ...).

ث- المعلومات التي ينتجها AUTE لا يدعمها النظام بشكل كامل (مثل التعليمات).

ج- تثير تغطية التطبيق لعمليات الدعم بعض الملاحظات: يتم تطوير هذه التطبيقات من قبل مقدمي الخدمة الذين لا يقدمون الضمانات الكافية فيما يتعلق باستدامتها واستمراريتها؛ لا يتم إصدار طلبات حلولها بالتنسيق مع قسم تكنولوجيا المعلومات، وذلك من أجل مراعاة القيود التقنية لتكنولوجيا المعلومات (توجهات نظم المعلومات، والتوجهات التكنولوجية، وتوافر المنصات، ...).

- النظام الحالي لا يسهل تبادل البيانات والمعلومات بين هياكل AUTE، عدة أقسام، ترغب الكيانات في الحصول على معلومات من جهات أخرى.
- سوف تحتاج إلى تعزيز أمن AUTE's Si، يمكن الوصول إلى شبكات LAN في تطوان وشفشاون مباشرة من جهاز توجيه الوصول إلى الإنترنت، دون أي جدار حماية لتأمينها.

1. ضمان الجودة

تتمثل أهداف خطة ضمان الجودة (PAQ) من ناحية، في ضمان جودة العمل المنجز بالإضافة إلى التحكم في تكاليف المشروع والمواعيد النهائية من خلال وضع المعايير والإجراءات، ومن ناحية أخرى وصف وتنظيم المشروع، وينطبق برنامج PAQ هذا على المشروع المحدد: دراسة لتطوير المخطط الرئيسي لنظم المعلومات للوكالة الحضرية لتطوان 2020-2024 (AUTE).[148]

2. المراقبة القانونية

الغرض من هذه اللبنة الوظيفية هو إدارة المراقبة القانونية المخصصة لجمع وتوفير أي نص قانوني يتعلق بمجال تخطيط المدن، أو أي نص قد يكون له تأثير ويجب الاهتمام به أثناء التعليمات أو الضوابط، الميزات الرئيسية للغرض:

- المراقبة القانونية: تعريف وتحديد معايير البحث عن النصوص القانونية؛ البحث وجمع النصوص القانونية والتنظيمية في مختلف مجالات تدخل AUTE؛ وتصنيف وفهرسة النصوص القانونية.

[148] Plan d'Assurance Qualité. Phase 1 : Analyse et évaluation de l'existant et identification des axes stratégiques. ETUDE D'ELABORATION DU SCHEMA DIRECTEUR DU SYSTEME D'INFORMATION 2020-2024 DE L'AGENCE URBAINE DE TETOUAN. AGENCE URBAINE DE TETOUAN. Ministère de l'Aménagement du Territoire National, de l'Urbanisme, de l'Habitat et de la Politique de la Ville. Royaume du Maroc.

- الانتشار: إرسال دوري آلي للنصوص الجديدة لتلك الفترة؛ توفير كافة النصوص القانونية على الإنترانت بمحرك بحث متعدد المعايير؛ والبحث السياقي (المنطقة، نوع العملية، إلخ) للنصوص القانونية من وحدات إدارة التعليمات والإعفاءات والضوابط.
- إنشاء التقارير والإحصاءات والتقارير ولوحات المعلومات.[149]

3. إمكانية التشغيل البيني

يهدف الموقع إلى تزويد موظفي AUTE وشركائها بأكبر نطاق ممكن من الموارد والمعلومات والبيانات، المبدأ هو إنشاء مساحة افتراضية يعرف فيها الزائر أنه سيجد كل ما يحتاج إليه أو على الأقل يمكنه استخدامه كبوابة لمصادر المعلومات الأخرى ذات الصلة، والميزات الرئيسية هي كما يلي:

- توفير معلومات مفيدة وذات صلة لموظفي AUTE والشركاء المختلفين حول أنشطة الوكالة؛
- تحسين صورة العلامة التجارية للوكالة وتكون بمثابة واجهة عرض لأنشطتها؛
- خلق مساحة للتبادل (المنتدى) مع البيئة الخارجية؛
- استخدام الويب كوسيلة للنشر والتوعية؛
- إنشاء العرض المؤسسي للوكالة: التاريخ، المهام، الصفات، التنظيم؛
- تزويد الجمهور بالمعلومات التجارية بطريقة شاملة للإجابة على أسئلة مستخدمي الإنترنت وتعميق معرفتهم وفقا لملفهم الشخصي أو وفقا للموضوع المختار:

✓ توفير محرك بحث يسمح بالبحث باستخدام الكلمات الرئيسية أو النص الكامل ويسهل الوصول إلى موارد المعلومات المنشورة على الإنترنت؛

✓ تسهيل النشر: مكتبة حيث سيتم تخزين جميع الوثائق المعروضة للتنزيل، حسب الفئة؛

✓ صندوق الاقتراحات: سيتمكن المواطنون من إرسال تعليقاتهم واقتراحاتهم والتحسينات المقترحة ودرجة رضاهم عن خدمات ومحتوى صندوق الموقع؛

✓ تقديم الأخبار المتعلقة بنشاط الوكالة: ملخصات وجدول أعمال وفعاليات ودراسات وتجارب؛

✓ توفير روابط مفيدة؛

---

[149] Plan d'urbanisation fonctionnel du futur Sl. Phase 2 : Elaboration des plans d'urbanisation du futur Sl et des scénarios de mise en œuvre. ETUDE D'ELABORATION DU SCHEMA DIRECTEUR DU SYSTEME D'INFORMATION 2020-2024 DE L'AGENCE URBAINE DE TETOUAN. AGENCE URBAINE DE TETOUAN. Ministère de l'Aménagement du Territoire National, de l'Urbanisme, de l'Habitat et de la Politique de la Ville. Royaume du Maroc, p :34.

- ✓ تقديم الخدمات الإلكترونية (دروس تعليمية حول الخدمات الالكترونية متوفرة الموقع الرسمي)[150]:
  - ملاحظات الاستخبارات: إدخال قطعة الأرض ومعلومات مقدم الطلب؛ الدفع الإلكتروني للرسوم؛ مراقبة معالجة مذكرة المعلومات؛ وقم بتنزيل مذكرة المعلومات.
  - الشكاوى الإلكترونية: إدخال معلومات المطالبة؛ مراقبة معالجة الشكوى؛ واستلام إشعار الرد على الشكوى (عن طريق البريد الإلكتروني والرسائل النصية القصيرة ومباشرة على الموقع).
  - طلبات التعليم أو الإعفاء: إدخال معلومات الطلب؛ تحديد موعد؛ مراقبة معالجة الطلب؛ واستلام إشعار الرد على الشكوى (عن طريق البريد الإلكتروني والرسائل النصية القصيرة ومباشرة على الموقع).
  - وثائق التخطيط العمراني: التشاور عبر الإنترنت لوثائق تخطيط المدن؛ البحث عن طريق الكلمات الرئيسية أو النص الكامل في وثائق تخطيط المدن.
  - بيع الوثائق: اختيار الوثائق (وثائق التخطيط الحضري التي نشرتهاAUTE ، والخرائط، ...)، والدفع الإلكتروني[151].

4. خدمة الشكاوى

تقدم الهيئة على موقعها الإلكتروني خدمة إلكترونية لإدخال ومراقبة حالة الشكاوى (المطالبة الإلكترونية)، ومع ذلك، بواسطة *"Chikaya"*، الذي تم توفيره بواسطة وزارة الصناعة والاستثمار والتجارة والاقتصاد الرقمي لصالح الوزارات والإدارات العامة، ويسمح حل الويب هذا بإدخال الطلبات من خلال ملفات تعريف الطالب المختلفة، في عدة فئات من الطلبات، يقوم النظام بإرسال الطلبات وتعيينها، وإدارة سير عمل التحقق من الاستجابة ووضعها على الإنترنت.

تم تطوير حل *"Chikaya" (chikaya.ma)* من قبل مزود خدمات معترف به (ATEXO Morocco) نيابة عن وزارة الصناعة والاستثمار والتجارة والاقتصاد الرقمي، مما يجعله متاحا لجميع الإدارات العمومية المغربية، ويتم استخدام هذه الأداة بالفعل من قبل العديد من الوزارات (وزارة التخطيط

---

[150] Videothèque, Tutoriels videos, AGENCE URBAINE DE TÉTOUAN : https://aute.gov.ma/videotheque/, Date de consultation: 14/05/2025, 02 :50pm.

[151] ibid, p : 36-37.

الإقليمي، التخطيط العمراني، الإسكان والسياسة الحضرية، وزارة الشباب والرياضة، إلخ) وكذلك من قبل العديد من المكاتب والوكالات.[152]

5. الرسائل الإلكترونية

تهدف هذه الكتلة الوظيفية إلى ضمان التواصل بين موظفي AUTE والعالم الخارجي عبر البريد الإلكتروني، احترافية ومنظم وآمن، الميزات الرئيسية لها هي كالتالي:

- احصل على رسائل احترافية وسرية ومنظمة وآمنة، تم تكوينها وفقا للمعايير المحددة داخليا من قبل الوكالة.
- أن يكون لديك صندوق بريد خاص بك لإرسال واستقبال الرسائل من داخل الوكالة ومن خارجها، وكذلك مع التطبيقات المستقبلية التي تتواصل عبر الرسائل الإلكترونية؛
- لديك دليل مشترك لجميع المستخدمين؛
- تنظيم الاجتماعات؛
- تحسين أوقات نقل البريد بين مختلف أصحاب المصلحة الداخليين والخارجيين؛
- تسهيل التواصل مع الأطراف الثالثة.[153]

الفقرة الثانية: التوصيات بشأن الوكالة الحضرية بتطوان سياسة خصوصية بوابتها الإلكترونية وأمنها السيبراني

سنعمل على جمع التوصيات التي قدمها فريق قسم تكنولوجيا المعلومات بالوكالة الحضرية تطوان وترجمتها (أولا)، ثم ترجمة سياسة الخصوصية للبوابة الإلكترونية للوكالة (ثانيا)، ثم التوصيات بشأن أمنها السيبراني (ثالثا).

---

[152] Scénarii de mise en œuvre. Phase 2 : Elaboration des plans d'urbanisation du futur Sl et des scénarios de mise en œuvre. ETUDE D'ELABORATION DU SCHEMA DIRECTEUR DU SYSTEME D'INFORMATION 2020-2024 DE L'AGENCE URBAINE DE TETOUAN. AGENCE URBAINE DE TETOUAN. Ministère de l'Aménagement du Territoire National, de l'Urbanisme, de l'Habitat et de la Politique de la Ville. Royaume du Maroc, p :49-50.

[153] ibid, p :38.

أولا: التوصيات المقدمة من طرف فريق قسم تكنولوجيا المعلومات بالوكالة الحضرية بتطوان

إن إثراء الحلول المتاحة بالفعل وتحسينها داخل AUTE يجب أن يتيح تحسين كفاءة خدمات الأعمال والتغلب على أوجه القصور الحالية، ومن المتوقع بذل الكثير من الجهود، مما يؤدي على وجه الخصوص إلى التوصيات الرئيسية التالية:

- الحفاظ على ومواصلة الجهود التي يبذلها قسم تكنولوجيا المعلومات لضمان المساعدة الفنية المستمرة لصالح المستخدمين، سواء وظيفيا (التدريب على الاستخدام) وفنيا (التطورات وحل الأعطال)؛
- استثمار المزيد من الجهد في إجراءات الدعم وإدارة التغيير حتى يتمكن المستخدمون من الأنظمة المتاحة (المعلومات والاتصالات حول المشاريع، والوعي باستخدام تكنولوجيات المعلومات، والتدريب والمساعدة في الأدوات المنفذة، وتوفير الوثائق)؛
- توسيع وإكمال التغطية الوظيفية للعمليات التجارية (ملاحظة المعلومات والضوابط، ...) وعمليات الدعم التي لم تتم تغطيتها بعد.
- الأتمتة واسعة النطاق لأنشطة عملية AUTE سوف تقلل من الاعتماد على الأدوات المكتبية والوسائط الورقية التي يتميز بها النظام الحالي والتي تشكل عائقا تشغيليا مما يحد من إنتاجية وأداء المستخدمين؛
- ضمان المزيد من تبادل ومشاركة المعلومات بين الخدمات المختلفة لAUTE من خلال SI موحد ومتكامل لإدارة أنشطتها التجارية، مفتوحة لجميع المستخدمين الذين لديهم حقوق الوصول والتراخيص؛
- اختيار الحلول القياسية لعمليات الدعم بدلا من التطوير المحدد؛
- ضمان تداول وإتاحة المعلومات بشكل أفضل في جميع نقاط نظام المعلومات؛
- تزويد المستخدمين بأنظمة الإدارة ودعم القرار التي تمكنهم من:

✓ وجود مؤشرات ووسائل لتحديد عناصر الإدارة وبالتالي اكتساب القدرة على الاستجابة في اتخاذ القرار؛ ✓ الحصول على تنبيهات متقدمة بشأن بعض جوانب الأعمال (التجزئة، وما إلى ذلك)؛

✓ مراقبة تطور أنشطة AUTE وتوقع الإنجازات؛

✓ استخدام التقنيات الحديثة والأدوات الفعالة لتخطيط وإدارة المشاريع والأنشطة (لوحة المعلومات، المؤشرات، ...)؛

1. *تطوير نظام لدعم تطوير المواقف والتقارير المنتظمة* وبالتالي تزويد جميع كيانات AUTE بالمعلومات الإدارية.[154]
2. *على مستوى الخادم:* لا يزال هناك خادمان جديدان (عمرهما أقل من 5 سنوات): الخادم المخصص لاستضافة البوابة الجغرافية والآخر للدليل النشط، الاثنان الآخران عفا عليهما الزمن.

تؤدي دراسة الخطة الرئيسية إلى العديد من مشاريع إعادة تصميم التطبيقات (مجال الأعمال) والحصول على تطبيقات جديدة (مجال الدعم والإدارة)، لم تعد الأنظمة الأساسية للأجهزة (الخوادم) الحالية قادرة على دعم هذه الاحتياجات المستقبلية.

إذا تم اعتماد سيناريو الاستيعاب، فيجب على AUTE بذل جهود إضافية لترقية منصاتها التقنية، وبالتالي يجب على AUTE اتباع الإرشادات التالية، فيما يتعلق بمنصة الخادم الحالية، الحصول على خوادم جديدة لتحل محل تلك القديمة حاليا، وأيضا:

- ✓ دعم الحلول الجديدة التي سيتم تنفيذها، يمكن أن تتوزع عمليات الاستحواذ هذه بمرور الوقت: تم الحصول على خادمين في عام 2020، ثم خادم واحد في عام 2021 وآخر في عام 2022؛
- ✓ اعتبارا من عام 2023، يجب على AUTE تنفيذ سياستها بدقة لاستبدال الخوادم بعد 5 سنوات؛
- ✓ يجب أن يفضل AUTE الحصول على خوادم مثبتة على حامل؛
- ✓ في نهاية المطاف، يجب على AUTE جعل خوادمها افتراضية لمزيد من الدمج والترشيد:
  - التحكم في تشغيل خوادم الكمبيوتر من خلال تحسين معدلات استخدامها؛
  - تجانس بنيات الأجهزة لتقليل تكاليف الصيانة والدعم؛
  - مساحة أكبر في مركز البيانات من خلال إزالة المعدات القديمة، وبالتالي تقليل فاتورة الطاقة.

إذا تم اعتماد سيناريو الاستعانة بمصادر خارجية، فيجب على AUTE تفضيل خيار استخدام خوادم المضيف، مما يسمح للوكالة بتعديل الخدمة المطلوبة وفقا للاحتياجات المتغيرة، ومع ذلك، يمكن نشر الخادم المخصص لـ Géo Portail على المضيف، وسيستمر استخدام الخوادم الحالية الأخرى بنفس الطريقة:

---

[154] ibid, p : 31-32.

- ✓ سيظل الخادم الذي يستضيف الإعلان نشطا؛
- ✓ سيظل الخادم الذي يستضيف تطبيق GIS نشطًا حتى تتم إعادة تصميم تطبيق GIS ونشره على النظام الأساسي للمضيف؛
- ✓ يمكن الآن إزالة الخادم الذي يستضيف تطبيق إدارة البريد، لأن تطبيق إدارة البريد لا يعمل. يجب تنفيذ تطبيق جديد، وسيتم نشره على خوادم المضيف.[155]

3. *على مستوى أنظمة التشغيل:* أصبحت أنظمة تشغيل الخوادم ومحطات العمل قديمة، وأنظمة تشغيل الخادم الحالية متباينة للغاية، بصرف النظر عن الخادم المخصص لاستضافة Geo Portal، فإن الخوادم الأخرى بها نظام تشغيل قديم يجب استبداله بنظام تشغيل أحدث.

يجب ترحيل نظام تشغيل محطة العمل إلى الإصدارات الأحدث من التوحيد القياسي، يجب على AUTE الاستفادة من تجديد معدات تكنولوجيا المعلومات الخاصة بها لطلب محطات عمل كاملة، مع تراخيص أرخص لـ EOM، وبالنسبة لنظام تشغيل الخادم، في حالة وجود سيناريو الاستيعاب، يجب على AUTE، أولا، تحليل التطبيقات الحالية لمعرفة ما إذا كان من الممكن ترحيلها إلى نظام تشغيل حديث، سيتعين على الوكالة بعد ذلك البدء في ترحيل خوادمها إلى Windows Server 2016 R2، وبالتالي توحيد نظام التشغيل لديها، وفي حالة وجود سيناريو الاستعانة بمصادر خارجية، ستستفيد AUTE من نظام التشغيل المتوفر من المضيف، بالإضافة إلى سياسة الترقية إلى أحدث الإصدارات.[156]

4. على مستوى النسخ الاحتياطي/الاستعادة: تمتلك الوكالة NAS 5 (خوادم تخزين) ذات سعة تخزينية كبيرة جدا، ومع ذلك، يتم ترك النسخ الاحتياطي/الاستعادة لمبادرة المستخدمين، هذا الأخير مسؤول عن إدارة وتنظيم مساحة التخزين هذه.

تتمتع الوكالة بمعدات كبيرة وقدرة تخزينية، مما يسمح لها بضمان النسخ الاحتياطي/الاستعادة بطريقة مهنية ووفقا للممارسات الجيدة في هذا المجال.

---

[155] Plan d'urbanisation technique du futur Sl. Phase 2 : Elaboration des plans d'urbanisation du futur Sl et des scénarios de mise en œuvre. ETUDE D'ELABORATION DU SCHEMA DIRECTEUR DU SYSTEME D'INFORMATION 2020-2024 DE L'AGENCE URBAINE DE TETOUAN. AGENCE URBAINE DE TETOUAN. Ministère de l'Aménagement du Territoire National, de l'Urbanisme, de l'Habitat et de la Politique de la Ville. Royaume du Maroc, p :30-31.

[156] ibid, p :31-32.

ستحتاج NAS إلى إعادة النشر لدعم النسخ الاحتياطية لمختلف التطبيقات التي سيتم تطويرها أو الحصول عليها، ومن ثم، سيتم تنظيم عملية النسخ الاحتياطي/الاستعادة بواسطة قسم تكنولوجيا المعلومات، على أساس إجراء النسخ الاحتياطي/الاستعادة الذي يجب إنشاؤه وإضفاء الطابع الرسمي عليه ونشره.

لا يعتمد تنفيذ النسخ الاحتياطي/الاستعادة على السيناريو المختار للتدخيل أو التخريج، ومع ذلك، في حالة السيناريو الثاني، يمكن لـAUTE ، حسب الرغبة، اختيار:

- ✓ تأكد من النسخ الاحتياطية/الاستعادة باستخدام مواردك الخاصة، في هذه الحالة، سيتعين على AUTEإعادة نشر NAS الخاص به، والحصول على حل نسخ احتياطي آلي (روبوت احتياطي)؛
- ✓ الاستعانة بمصادر خارجية للنسخ الاحتياطية/عمليات الاستعادة للمضيف، سيتم أيضا استضافة خوادم النسخ الاحتياطي الحالية (NAS) بواسطة موفر الخدمة الخارجي، ويجب على الأخير أيضا ضمان النسخ الاحتياطية الثانوية على الأشرطة والتأكد من أمنها.

وفي كلتا الحالتين، يجب على AUTE التأكد من النسخ الاحتياطية واختبارها بشكل دوري، يجب اختبار جميع النسخ الاحتياطية والتحقق منها بشكل منتظم ومستمر.[157]

5. على مستوى قاعدة البيانات: التطبيقات المتاحة حاليا لـ AUTE موجودة على أنظمة إدارة قواعد البيانات (DBMS) المختلفة، يجب على الوكالة إدارة قواعد البيانات ضمن ArcGIS Server أو PostGres أو MySQL أو حتى SQL Server، وسوف تحتاج قواعد البيانات إلى المواءمة، وبالتالي، يجب أن يستفيد AUTE من إعادة تصميم التطبيق لإدارة طلبات التعليمات والإعفاءات والضوابط ومذكرات المعلومات لتحليل جدوى ترحيل قاعدة البيانات من PostGis إلى ArcGIS Server، وهذا التجانس سيجعل من الممكن صيانة المجمع وكذلك التدريب، وبالمثل بالنسبة للتطبيقات الأخرى، يجب على AUTE توحيد نظام إدارة قواعد البيانات (DBMS) الخاص به حول معيار موثوق ودائم، نوصي بالتوجه نحو Microsoft SQL Server.[158]

[157] Ibid, p :32.

[158] Ibid, p : 33.

ثانيا: سياسة الخصوصية للبوابة الالكترونية للوكالة الحضرية تطوان والتوصيات بشأنها

أ - سياسة الخصوصية للبوابة الالكترونية للوكالة الحضرية تطوان

سياسة الخصوصية للبوابة الالكترونية للوكالة الحضرية تطوان صيغت باللغة الفرنسية إلا أنني أكتب باللغة العربية فعملت على ترجمتها للغة العربية، وهي على الترتيب التالي:

1. موافقة CONSENTEMENT

باستخدام موقع الوكالة الحضرية، قد يطلب من المستخدم تزويد الموقع ببيانات المستخدم الشخصية، وعرفت الوكالة البيانات الشخصية في منصتها الرقمية بأنها عبارة عن: "معلومات تم جمعها وتسجيلها بتنسيق يسمح بالتعرف عليك شخصيًا، إما بشكل مباشر (مثل الاسم) أو بشكل غير مباشر (مثل رقم الهاتف) كشخص طبيعي، قبل إرسال هذه المعلومات إلينا، نوصيك بقراءة سياستنا المتعلقة بحماية البيانات الشخصية".

من خلال تحديد المربع لقبول الشروط العامة للاستخدام، ولا سيما الفقرة المتعلقة بمعالجة البيانات الشخصية، يمنح المستخدم موافقته للوكالة الحضرية بتطوان على تسجيل بياناته الشخصية واستخدامها ومعالجتها للاستخدام الداخلي.

1. حماية البيانات الشخصية PROTECTION DES DONNÉES PERSONNELLES

تخضع المعلومات المجمعة على الموقعhttps://aute.gov.ma للمعالجة الحاسوبية المخصصة للاستخدام الداخلي من أجل إدارة ومراقبة طلبات المستخدمين، والمستفيدون من المعطيات هم المصالح الداخلية للوكالة الحضرية لتطوان، ويمكن للمقاول من الباطن (المضيف) لدى الوكالة الرجوع إلى البيانات الشخصية بالقدر اللازم لتنفيذ المهام الموكلة إليه، حيث يتم الاحتفاظ بالبيانات الشخصية المجمعة وفقًا للوائح المعمول بها في قاعدة بيانات الوكالة، ولا يتم الكشف عن أي معلومات شخصية لأطراف ثالثة.

تهدف المعالجة المنفذة على موقع الوكالة إلى الاستجابة لما يلي: طلبات الحصول على مذكرات معلومات التخطيط الحضري؛ طلبات التعيين؛ طلبات الفحص المسبق للملفات؛ تقديم المطالبات؛ طلب الوصول إلى المعلومات؛ والدفع الإلكتروني لملفات التعليمات.

لقد تم الإخطار بهذه العلاجات والترخيص بها من قبل CNDP بموجب التفويضات: رقم (الطلب قيد التقدم)

2. حق الوصول والتصحيح والمعارضة DROIT D'ACCÉS, DE RÉCTIFICATION ET D'OPPOSITION

وفقا للقانون رقم 08-09 الصادر بموجب الظهير الشريف رقم 15-09-1 المؤرخ 18 فبراير 2009 المتعلق بحماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية، لدى المستخدم الحق في الوصول إلى المعلومات التي تهمه وتصحيحها، والتي يمكنه عملها عن طريق الاتصال بعنوان البريد الإلكتروني التاليautetouan@yahoo.fr :، ويمكنه أيضا، لأسباب مشروعة، الاعتراض على معالجة البيانات المتعلقة به.

3. أمن البيانات SÉCURITE DES DONNÉES

تطبيقا لأحكام الفصل 23 وما يليه من القانون رقم 08-09 (الصادر بالظهير الشريف رقم 15-09-1 الصادر في 22 صفر 1430)، تقوم الوكالة الحضرية لتطوان بتنفيذ جميع التدابير التقنية والتنظيمية اللازمة لضمان أمن وسرية البيانات الشخصية التي يتم جمعها ومعالجتها، وعلى وجه الخصوص منع تشويهها أو إتلافها أو نقلها إلى أطراف ثالثة غير مصرح لها، من خلال ضمان مستوى من الأمان يتكيف مع المخاطر المرتبطة بالمعالجة وطبيعة البيانات المراد حمايتها، مع الأخذ في الاعتبار المستوى التكنولوجي وتكلفة التنفيذ.

5.الارتباطات التشعبية LIENS HYPERTEXTES

تنبه الوكالة عبر هاته الجزئية أن قد تحتوي صفحات موقعها على روابط لمواقع أخرى أو تشير إلى مواقع أخرى، ولا تضمن الوكالة الحضرية لتطوان محتوى هذه المواقع الأخرى، ولا يمكن أن تتحمل مسؤولية الأضرار الناجمة عن استخدام محتوى هذه المواقع، ويتم توفير الروابط إلى المواقع الأخرى فقط كوسيلة لراحة مستخدم هذا الموقع.

6.المسؤوليات RÉSPONSABILITÉS

لا يمكن تحميل الوكالة الحضرية لتطوان المسؤولية عن الأضرار المباشرة أو غير المباشرة الناجمة، بأي شكل من الأشكال عن الاتصال بالموقع، ولا عن الأضرار المباشرة أو غير المباشرة المرتبطة بانقطاع أو خلل من أي نوع، لأي سبب من الأسباب، وأن اتصال أي شخص بالموقع يتم تحت مسؤوليته الكاملة.

7.أحكام أخرى AUTRES DISPOSITIONS

الموقع محجوز للاستخدام الخاص لكل مستخدم، ويحتوي الموقع على نصوص القوانين والمراسيم والتعاميم بصيغةPDF، ويتم تحذير المستخدمين من أن النسختين العربية والفرنسية فقط للنصوص المنشورة في الجريدة الرسمية للمملكة المغربية هي الأصلية.

كما أن البيانات والمعلومات والوثائق التي يقدمها الموقع مخصصة فقط للمعلومات العامة غير الشاملة ولا يمكنها تحت أي ظرف من الظروف، أن تكون ملزمة تعاقديا للوكالة الحضرية لتطوان، التي ترفض كل المسؤولية عن أي قرارات يمكن اتخاذها من هذه المعلومات.

8. كوكيز COOKIES

يتم إعلام مستخدم هذا الموقع أنه خلال زياراته للموقع، قد يتم تثبيت ملف تعريف الارتباط تلقائيا على برنامج المتصفح الخاص به وتخزينه مؤقتا على محرك الأقراص الثابتة الخاص به، وقد عرفت الوكالة ضمن هاته الجزئية ملف تعريف الارتباط بأنه "هو عنصر لا يحدد هوية المستخدم، ولكنه يستخدم لتسجيل المعلومات المتعلقة بتنقل المستخدم على موقع الويب".

تستخدم الوكالة الحضرية بتطوان هذه المعلومات لأغراض تحسين أمن هذا الموقع وتقديم الخدمة المثلى، ولذلك، يتم استخدام ملفات تعريف الارتباط من أجل:

- إدارة الإعدادات الشخصية عندما يقوم المستخدم بتسجيل الدخول إلى الموقع الآمن
- تسجيل معلومات حول تنقل المستخدم في الموقع لتوجيه تصفحه نحو المحتوى الأنسب
- قياس عدد الزيارات للموقع

لا يقصد من "ملفات تعريف الارتباط" تحت أي ظرف من الظروف استخدام المعلومات الشخصية المتعلقة بالأشخاص المتصلين بالموقع، ويقر مستخدم الموقع بأنه قد تم إعلامه بهذه الممارسة ويرخص للوكالة الحضرية لتطوان باستعمالها، كما يمكن للمستخدم إلغاء تنشيط ملف تعريف الارتباط هذا عبر الإعدادات الموجودة في برنامج المتصفح الخاص به وبشكل خاص عن طريق تعديل خيارات برنامج المتصفح على جهاز الكمبيوتر الخاص به[159].

أما بالنسبة لسياسة خصوصية موقع رخص فعند الدخول إليها أجد صفحة بيضاء، بمعنى أنه ليس هناك سياسة خصوصية مرتبطة بهذا الموقع أيضا وإن كانت توجد خانة ووعاء لهاته الجزئية.

[159] Mentions légales, CONDITIONS GÉNÉRALES D'UTILISATION, AGENCE URBAINE DE TÉTOUAN, https://aute.gov.ma/mentions-legales/, Date de consultation : 02/06/2024, 21 :02pm.

أ- التوصيات بشأن سياسة الخصوصية للبوابة الإلكترونية للوكالة الحضرية بتطوان

تعتمد حاليا الوكالة الحضرية تطوان، على سياسة خصوصية لبوابتها الإلكترونية على عكس بعض التطبيقات المتعلقة بالمؤسسات العمومية، بما يبدو عليها من الجدة إلا أنها بوابة متكاملة الأركان، اعتمدت سياسة خصوصية مختصرة وشاملة إلا أنها أغفلت ذكر الجهات المسؤولة التي يمكن من خلالها للمواطنات والمواطنين التبليغ في حالة تسرب أو انتهاك البيانات الخاصة بهم كما حصل في صندوق الضمان الاجتماعي بتاريخ 8 أبريل 2025، وعلى شموليتها واختزالها للقواعد القانونية إلا أنه يمكن الرجوع إلى قانون 08-09 المتعلق بحماية الأشخاص الذاتيين لمعالجة المعطيات ذات الطابع الشخصي، فقط لملئ بعض الفراغات في سياسة الخصوصية، كما يلي:

1. التوصية بالإشارة لأهم عناصر حماية البيانات الشخصية في قانون 08-09 بسياسة الخصوصية

للمواطنات والمواطنين كافة الحقوق حول المعطيات الشخصية وفقا لقانون 08-09 المتعلق بحماية الأشخاص الذاتيين لمعالجة المعطيات ذات الطابع الشخصي، تلتزم بها البوابة الإلكترونية للوكالة الحضرية تطوان:

1) الحق في الإخبار أثناء تجميع المعطيات وفقا للمادة 5 من القانون 80-09؛ في حدود المادة 6.
2) الحق في الولوج المادة 7؛
3) الحق في التصحيح المادة 8؛
4) الحق في التعرض المادة 9؛
5) منع الاستقراء المباشر المادة 10.

2. التوصية بعنصر الإبلاغ بسياسة الخصوصية إذا تم تسريب أو انتهاك للبيانات الشخصية

إذا كنت بحاجة إلى الإبلاغ أو الاستشارة، بخصوص تسريب أو انتهاك المعلومات الشخصية، يتم الاتصال بالجهات التالية:

1) اللجنة الوطنية لحماية البيانات الشخصية: رقم الهاتف tel:+212537571124 ، أو tel:+212537572141. التواصل عبر البريد الإلكتروني (contact@cndp.ma). ويمكن تقديم الشكاوى عن طريق المنصة الرسمية.

2) مؤسسة وسيط المملكة: يمكن تقديم الشكاوى عبر البريد الإلكتروني: info@mediateur.ma رقم الهاتف: +212 5 37 57 77 11/00 يمكن تقديم الشكاوى عن طريق المنصة الرسمية: www.mediateur.ma
3) البوابة الوطنية للشكايات: الاتصال بالأرقام الخاصة بمركز الاتصال: من داخل المغرب: 3737 أو 0802003737، ومن خارج المغرب: +212537679906. الولوج إلى البوابة الوطنية للشكايات ثم الى القسم الخاص بتقديم الشكايات أو تتبعها www.chikaya.ma .
4) المديرية العامة للأمن الوطني: رقم هاتف الشرطة: 19. ويمكن للمواطنات والمواطنين الولوج إلى المنصة الرقمية "إبلاغ" عبر عنوانها الإلكتروني www.e-blagh.ma.

تجدر الإشارة إلى أن الاقتراح أعلاه يبقى اجتهادا مني باعتباري طالبة باحثة، قد أصيب وقد أخطئ، إلا أنه يمكن الركون إلى أنه إما دخل الأمر في تحديد المواد القانونية في إطار التفصيل والتوضيح طبقا لقانون 08-09، أما سياسة الخصوصية للوكالة فقد كانت شاملة وتحيل دائما لقانون 09-08، في حين أن بعض المؤسسات العامة لازالت لم تؤطر موقعها الإلكتروني بسياسة خصوصية تبرز عبرها مدى جديتها واهتمامها بحماية البيانات الشخصية سواء أكانت مواقع محلية أو وطنية، إلا أن سياسة البوابة الإلكترونية للوكالة أغفلت باب التبليغ إن وقع تسريب أو انتهاك للمعطيات الشخصية للمستخدم، لكن يمكن تدارك هاته النقطة عبر هذا التقرير المتواضع.

ثالثا: التوصيات المتعلقة بالأمن السيبراني للوكالة الحضرية تطوان

في تقرير دراسة الامتثال لتوجيهات أمن نظم المعلومات الوطنية (DNSSI)[160] بالوكالة الحضرية تطوان، تم تحليل وتقييم الوضع القائم وتحديد المحاور الاستراتيجية، إلا أننا في هاته الجزئية لن نعرض التدقيق التنظيمي وفقا (DNSSI) لا سياقه ولا نتائجه، ومخططات الامتثال، ولا طريقة تحليل المخاطر، بل سنكتفي بإبراز توصيات للامتثال اعتمادا على التوجيه الوطني لأمن نظم المعلومات، كما يلي:

[160] Rapport de l'étude de conformité à la Directive Nationale de Sécurité des Systèmes d'Information (DNSSI). Phase 1 : Analyse et évaluation de l'existant et identification des axes stratégiques. ETUDE D'ELABORATION DU SCHEMA DIRECTEUR DU SYSTEME D'INFORMATION 2020-2024 DE L'AGENCE URBAINE DE TETOUAN. AGENCE URBAINE DE TETOUAN. Ministère de l'Aménagement du Territoire National, de l'Urbanisme, de l'Habitat et de la Politique de la Ville. Royaume du Maroc, p :32-36.

بعد التدقيق الذي تم إجراؤه وفقا للتوجيه الوطني لأمن نظم المعلومات، يتعين على AUTE أن يأخذ في الاعتبار العديد من التوصيات من أجل الامتثال لقواعد هذا التوجيه، وتتلخص هذه الإجراءات على النحو التالي:

1- *السياسة الأمنية:* تنظيم وتنسيق تطبيق DNSSI داخل الوكالة؛ إضفاء الطابع الرسمي على وثائق الطلب والحفاظ عليها محدثة (قواعد وإجراءات محددة)؛ الموافقة على الميثاق الأمني ونشره؛ وضع جدول زمني يحدد مراحل تطبيق DNSSI، وقم بمراجعة تطبيق تدابير DNSSIبانتظام.

2- *التنظيم الأمني:* تطوير الأوصاف الوظيفية التي تحدد أدوار ومسؤوليات المدير المسؤول عن أمن نظم المعلومات؛ التحقق من صحة ونشر الميثاق الأمني؛ تعيين CISO رسميا، لفترة قصيرة المدى، يمكن لرئيس قسم تكنولوجيا المعلومات أن يتولى مسؤوليات CISO (قد تم ذلك)؛ تحديد إجراء للإبلاغ عن التأثيرات الكبرى إلى DGSSI وإدراج هذا الإجراء في إجراء أوسع لإدارة الحوادث الكبرى؛ ومتطلبات الطرف الثالث: الامتثال لقانون حماية المعلومات الشخصية؛ والمخاطر الناشئة عن أطراف ثالثة: إضفاء الطابع الرسمي على الأحكام التنظيمية والتعاقدية المتعلقة بأمن نظم المعلومات وتطبيقها.

3. *الأمن المتعلق بالموارد البشرية:* الالتزام بالسرية: التحقق من صحة ونشر ميثاق أمن المعلومات؛ وتدريب الموظفين: تنظيم دورات تدريبية وتوعوية حول مباحث أمن الدولة بشكل منتظم.

4. *إدارة العمليات والاتصالات؛* إجراءات التشغيل: تطوير/إضفاء الطابع الرسمي على إجراءات التشغيل: إجراءات إدارة وتأمين الأصول الهامة لنظام المعلومات؛ إجراء النسخ الاحتياطي؛ إجراءات إدارة الوصول والترخيص؛ إجراءات إدارة الحوادث؛ التحجيم: تخطيط وتوثيق حجم موارد معالجة المعلومات؛ الحماية ضد الرموز الضارة: تطوير إجراء رد الفعل في حالة وجود عدوى فيروسية؛ إجراء النسخ الاحتياطي: إضفاء الطابع الرسمي على إجراء النسخ الاحتياطي؛ الترميم: اختبار الترميم بانتظام؛ واحتفظ بالنسخ الاحتياطية في مكان آمن مع توفر ظروف تخزين النسخ الاحتياطي المناسبة؛ وضع إجراء لاستخدام محطات العمل المحمولة والوسائط القابلة للإزالة من أجل ضمان أمنها وأمن المعلومات الواردة؛ تطبيق الإجراءات الأمنية على محطات العمل المحمولة والوسائط القابلة للإزالة (التحديث المنتظم لمكافحة الفيروسات، وتطبيق التصحيحات، والتحقق من الامتثال، ...)؛ إعداد الرسائل المهنية، والتحقق من صحة ونشر الميثاق الأمني؛ وضمان التسجيل والتحليل

الدوري الأحداث الأمنية وتحديد الإجراءات التي يجب اتخاذها من خلال وجود نظام أساسي لإدارة السجل.[161]

5. *التحكم في الوصول:* رفع مستوى وعي المستخدم حول إدارة كلمات المرور؛ قم بمراجعة حقوق وصول المستخدم بشكل دوري من قبل مديري الأعمال؛ قم بتعطيل منافذ الوصول عن بعد غير الضرورية المثبتة على أجهزة الشبكة؛ وتقييد الوصول إلى منافذ التشخيص والتكوين ووقت المعالجة المطلوب؛ وإنشاء تجزئة شبكة جديدة (انظر PACT)؛ وحماية المناطق المجزأة (انظر الميثاق).
6. *الاستحواذ والتطوير والصيانة:* التحكم في الوصول إلى كود مصدر البرنامج؛ وتدابير لنقاط الضعف التقنية: ضمان تنظيم عمليات التدقيق المنتظمة، وتنفيذ التوصيات المتعلقة بنقاط الضعف المكتشفة.
7. *إدارة الحوادث:* إضفاء الطابع الرسمي على إجراء الإبلاغ عن الأحداث المتعلقة بأمن نظم المعلومات؛ إضفاء الطابع الرسمي على إجراءات إدارة الحوادث مع تغطية الأنواع المختلفة من الحوادث الأمنية؛ يطلب من كل كيان إدارة تذاكر الحوادث الأمنية؛ وتنفيذ أداة لإدارة الحوادث (GLPI على سبيل المثال)؛ وتنفيذ أداة لإدارة الحوادث (GLPI على سبيل المثال).
8. *إدارة خطة استمرارية الأعمال:* استمرارية الأعمال وتقييم المخاطر: إجراء تحليل لتأثير الأنشطة بشكل منتظم؛ قم بإعداد استبيان مناسب لذلك تحليل؛[162]استمرار العمل (PCA/PRA): تطوير خطة لاستمرارية واستئناف الأعمال تجمع بين جميع حلول طوارئ تكنولوجيا المعلومات؛ إجراء تدريب ورفع مستوى الوعي للموارد المتضررة من إجراءات PCA/PRA لتوضيح أدوارهم ومسؤولياتهم؛ الاختبار المستمر لخطة اختبار PCA/PRA: تطوير خطة الاختبار الفني PCA/PRA؛ قم بتنفيذ خطة اختبار PCA/PRA سنويا؛ وإعداد التمارين وسيناريوهات الأزمات.
9. *الامتثال:* التحقق من صحة ونشر الميثاق الأمني؛ حماية البيانات الشخصية: الامتثال للقانون 08-09؛ التحقق من الامتثال لـ DNSSI: تطوير لوحة معلومات لمراقبة تنفيذ DNSSI؛ الميثاق من الاستخدام SI: الموافقة على الميثاق الأمني وتوزيعه؛ التحقق من المطابقة مع

[161] ibid, P :34.

[162] Ibid, P :35.

RGS: الالتزام بقواعد السلامة العامة؛ وتدقيق نظام المعلومات: تأكد من إجراء عمليات تدقيق SI مرة واحدة على الأقل كل عامين.[163]

المبحث الثاني: سياسة الخصوصية للتطبيقات الإلكترونية للمؤسسات العمومية بكوريا الجنوبية _موقع *حكومة 24* نموذجا

تمثل سياسة الخصوصية للبوابات والتطبيقات الإلكترونية، الحصن الحصين لحقوق هاته المواقع، مع حفظ حقوق المواطنين والمواطنات من جهة، وكذا الطرف الثالث، لذلك سنعمل على موقع *حكومة 24* الكوري الذي الحاضن لموقع *بياناتي* الموازي لموقع *إدارتي* المغربي من حيث الكينونة والطبيعة.

تقوم *الحكومة 24* (المشار إليها فيما يلي باسم *"Government24"*)[164] بمعالجة المعلومات الشخصية وإدارتها بشكل قانوني وآمن وفقا لقانون حماية المعلومات الشخصية والقوانين واللوائح ذات الصلة لحماية حرية وحقوق أصحاب المعلومات، وبناء على ذلك، ووفقا للمادة 30 من قانون حماية البيانات الشخصية، تم وضع سياسة معالجة البيانات الشخصية التالية والإفصاح عنها لإعلام أصحاب البيانات بإجراءات ومعايير معالجة البيانات الشخصية والتعامل مع الشكاوى المتعلقة بها بسرعة وسلاسة (المطلب الأول).

تمثل كل من اللجنة الوطنية لحماية البيانات الشخصية بالمغرب، مؤسسة وسيط المملكة، موقع الرئاسة العامة للشكايات الالكترونية، البوابة الوطنية للشكايات، والمديرية العامة للأمن الوطني لموقعها الالكترونية شكاية، مؤسسات يمكن تبليغها عن وقوع تسريب أو انتهاك للبيانات الشخصية بالمغرب.

يمكن تبليغ هيئات حماية البيانات الشخصية بكوريا الجنوبية عن تسرب أو انتهاك لهاته الحقوق، في كل من لجنة حماية البيانات الشخصية بكوريا الجنوبية، نظام الوساطة في حل نزاعات المعلومات الشخصية، قسم التحقيق في الجرائم الإلكترونية التابع لمكتب المدعي العام الأعلى، مركز الاستجابة للإرهاب السيبراني التابع لوكالة الشرطة الوطنية (المطلب الثاني).

---

[163] Ibid, P :36.

[164] سياسة الخصوصية لموقع حكومة 24، على موقع حكومة 24: https://www.gov.kr/portal/privacy?Mcode=11230، تاريخ الاطلاع: 2025/09/13، على الساعة 11:21 مساء.

المطلب الأول: الإطار القانوني والقضائي لسياسة الخصوصية بالتطبيقات الإلكترونية في كوريا الجنوبية

سنعمد إلى سياسة الخصوصية لموقع حكومة *24*، مع تفصيل المواد المرتبطة بقانون حماية البيانات الشخصية لكوريا الجنوبية، إلى جانب القرارات والأحكام القضائية والأسئلة القانونية بجواب قانوني من طرف جهات رسمية، مرتبطة ببعض المواد المذكورة في السياسات الخصوصية (الفقرة الأولى).

ثم سرد بعض الأحداث المتعلقة بتسريب المعلومات الشخصية من موقع حكومة *24* والأسباب وتسجيل ردود فعل الحكومة بشكل مختصر، ومن تم التعرف على كيفية رفع دعوى جماعية وفقا لقانون حماية البيانات الشخصية بكوريا الجنوبية والذي يفتقر إليها قانون 08-09 (الفقرة الثانية).

الفقرة الأولى: الجزء الأول من سياسة الخصوصية للمنصة الرقمية *للحكومة 24*

سنعمد إلى الجزء الأول من سياسة الخصوصية لموقع حكومة *24*، بالإضافة إلى بعض القرارات القضائية المرتبطة بالمواد القانونية لهاته السياسة، تتكون "سياسة معالجة المعلومات الشخصية" من المحتويات التالية:

أولا: غرض معالجة المعلومات الشخصية

①تقوم *Government24* بمعالجة المعلومات الشخصية للأغراض التالية، لن يتم استخدام المعلومات الشخصية التي تتم معالجتها لأغراض أخرى غير ما يلي، وإذا تغير غرض الاستخدام، فسيتم اتخاذ التدابير اللازمة، مثل الحصول على موافقة منفصلة، وقد تم التفصيل وتوضيح المعلومات الشخصية في موقع *الحكومة 24* كما يلي :

1 .معلومات أعضاء *الحكومة 24*

تتم معالجة المعلومات الشخصية لأغراض تسجيل العضوية، واستخدام خدمات العضوية، وإجراءات التحقق من الهوية المحدودة، والتعرف على الهوية الشخصية، ومنع سوء الاستخدام، ومنع الاستخدام غير المصرح به، وتأكيد نية التسجيل، وتأكيد موافقة الممثل القانوني عند جمع المعلومات الشخصية للأطفال دون سن 14 عاما، والتحقق المستقبلي من هوية الممثل القانوني، وحفظ السجلات لحل النزاعات، ومعالجة الشكاوى، وتسليم الإشعارات.

2 .سجل طلبات الشكوى المدنية الإلكترونية (بما في ذلك سجل الاستشارات)

تتم معالجة المعلومات الشخصية المدرجة في سجل طلب الشكوى المدنية الإلكترونية (بما في ذلك سجل الاستشارة) من قبل وكالات استقبال ومعالجة الشكاوى المدنية لغرض معالجة الشكاوى المدنية وفقا للمادة 12-2 من قانون معالجة الشكاوى المدنية (تشغيل نوافذ الشكاوى المدنية الإلكترونية ونوافذ الشكاوى المدنية الإلكترونية المتكاملة)[165]

3 .شهادة الشكوى المدنية الإلكترونية (نموذج الطلب والوثيقة الصادرة)

تتم معالجة المعلومات الشخصية المدرجة في شهادات الشكاوى المدنية الإلكترونية (نماذج الطلبات والوثائق الصادرة) من قبل وكالات استقبال ومعالجة الشكاوى المدنية لغرض معالجة الشكاوى المدنية وفقا للمادة 12-2 من قانون معالجة الشكاوى المدنية.

4. معلومات حية: بالنسبة لأعضاء *Government24*، تتم معالجة المعلومات الشخصية لغرض عرض معلومات نمط حياة العضو وفقا للمادة 9-2 من قانون الحكومة الإلكترونية (توفير معلومات نمط الحياة من خلال بوابة الحكومة الإلكترونية)[166]

على نفس المنوال، في قرار للمحكمة العليا بتاريخ 27 فبراير 2014، حول انتهاك قانون حماية البيانات الشخصية للمؤسسات العامة (بعض الجرائم المعترف بها: انتهاك قانون تسجيل المقيمين) جاء فيه ما يلي:

[1] معنى "الأساليب الكاذبة أو غير السليمة الأخرى" كما هو محدد في الفقرة 3 من المادة 23 من قانون حماية المعلومات الشخصية للمؤسسات العامة، وما إذا كانت جريمة انتهاك الحكم المذكور أعلاه ترتكب فقط عندما يكون رئيس المؤسسة التي تحتفظ بمعلومات المعالجة قادرا على استخدام أو توفير معلومات المعالجة (كل بند من المادة 10، الفقرة 3 من نفس القانون) ويتم استخدام "الأساليب الكاذبة أو غير السليمة الأخرى" لعرض أو تلقي معلومات المعالجة (سلبي)

---

[165] المادة 12-2 (تشغيل مركز الشكاوى المدنية الإلكتروني ومركز الشكاوى المدنية الإلكتروني المتكامل، إلخ)، قانون معالجة الشكاوى المدنية (اختصار: قانون معالجة الشكاوى المدنية) [دخل حيز التنفيذ في 12 يوليو 2022] [القانون رقم 18748، 11 يناير 2022، تعديل لقوانين أخرى]، على موقع المركز الوطني للمعلومات القانونية بوزارة التشريع الحكومي، موقع رسمي للحكومة الإلكترونية لجمهورية كوريا الجنوبية: https://www.law.go.kr/LSW/lsInfoP.do?lsiSeq=239293#0000، تاريخ الاطلاع: 2025/07/06، تاريخ الساعة 01:26 صباحا.

[166] المادة 9-2 (توفير المعلومات الحية من خلال بوابة الحكومة الإلكترونية)، قانون الحكومة الإلكترونية [تاريخ النفاذ: 16 مايو 2023] [القانون رقم 19030، 15 نوفمبر 2022، معدل جزئيا]، على موقع المركز الوطني للمعلومات القانونية بوزارة التشريع الحكومي، موقع رسمي للحكومة الإلكترونية لجمهورية كوريا الجنوبية: https://www.law.go.kr/LSW/lsInfoP.do?lsiSeq=245293#0000، تاريخ الاطلاع: 2025/07/06، تاريخ الساعة 01:29 صباحا.

[2] ما إذا كانت جريمة "الاستخدام غير القانوني لرقم تسجيل المقيم" كما هو محدد في المادة 37، الفقرة 10 من قانون تسجيل المقيم، ترتكب عندما يتم استخدام رقم تسجيل المقيم لشخص آخر لأغراض أخرى غير التحقق من الهوية دون إذن حامله (سلبي)

ملخص الحكم:

[1] ① الفقرة 3 من المادة 23 من قانون حماية المعلومات الشخصية للمؤسسات العامة السابقة (التي تم إلغاؤها بموجب "قانون حماية المعلومات الشخصية" الذي تم سنه كقانون رقم 10465 في 29 مارس 2011، فإنه يشار إليه في هذا المجال بأنه لا تنص على أن الشخص الذي يصل إلى معلومات المعالجة أو يتلقنه يعاقب على فرضية انتهاك الأحكام التي تقيد استخدام وتوفير معلومات المعالجة من قبل رئيس معلومات المعالجة (المادة 10 من القانون) أو الأحكام التي تحظر على أساس تعامله مع المعالجة الشخصية، وتنص الفقرة 3 من المادة 23 من القانون على التزامات رئيس مؤسسة معالجة معلومات المعالجة أو معالج المعلومات الشخصية بغض النظر عن انتهاك التزامات المادتين 10 و11 من قانون المؤسسة المعالجة معلومات المعالجة أو معالج المعلومات الشخصية.

في الحالة التي يتم فيها توفير معلومات المعالجة من خلال "الأساليب غير القانونية" بخلاف تلك المذكورة أعلاه، يمكن اعتبار هذا الحكم على أنه يفرض بشكل غير مباشر التزاما على شخص يسعى إلى تلقي معلومات معالجة بعدم استخدام "خطأ أو غيرها من الأساليب" عن طريق معاقبة مثل هذه الحالات، يتم استخدام "أساليب كاذبة أو غير عادلة"، سيكون من الصعب تحقيق الغرض من القانون، وهو ما يهدف إلى حماية المعلومات الشخصية؛ على الرغم من أن هذه المعلومات لا يمكن عرضها أو تقديمها من خلال الإجراءات وفقا للقانون؛ لا يتم تحديد ذلك فقط عندما يتم عرض أو تقديم معالجة المعلومات باستخدام "طرق خاطئة أو غير مناسبة أخرى" فيما يتعلق بالحالات (كل بند من المادة 10، الفقرة 3 من القانون).

[2] في ضوء الغرض من معاقبة "الشخص الذي استخدم بشكل غير قانوني بطاقة تسجيل شخص آخر" في الفقرة 8 من المادة 37 من قانون التسجيل المقيم، وحكم في الفقرة 10 من نفس المقال لمعاقبة "الشخص الذي استخدم بشكل غير قانوني في التمييز" يجب النظر إلى القوانين، الفقرة 10 من المادة 37 من قانون التسجيل المقيمين كحكم لمعاقبة أفعال التسجيل المقيمين دون إذن من صاحب التسجيل المقيم أو التصرف كما لو كان يحصل على رقم واحد دون أن يتوافق على التداول AINS رقم تسجيل المقيم في الحامل في مختلف مجالات الحياة العامة والخاصة، وبالتالي حتى لو تم استخدام رقم تسجيل شخص آخر المقيم دون إذن من الحامل، فمن المحظور استخدام رقم التسجيل

المقيم لتأكيد هوية الفرد أو تحديد الفرد أو التعرف على الفرد، ولا تتحقق جريمة إساءة استعمال أرقام تسجيل المقيمين المنصوص عليها في المادة السابقة إلا إذا استعملت لغرض محدد.[167]

في المقابل سنرى ما إذا كانت المادة 26 من قانون معالجة الشكاوى المدنية تتوافق مع "الحالات التي توجد فيها أحكام خاصة في قوانين أخرى" في المادة 18، الفقرة 2، الفقرة الفرعية 2 من قانون حماية المعلومات الشخصية (وزارة التشريع الحكومي 21-0889، 26 أبريل 2022، وزارة الإدارة العامة والأمن)

ملخص السؤال: تنص المادة 26 على التعامل مع الشكاوى المدنية على أن رئيس وكالة إدارية يجوز له التحقيق في رضا صاحب الشكوى ومجالات التحسين فيما يتعلق بالشكاوى المدنية التي تمت معالجتها وتعكس النتائج في عمله/ المادة 18 من قانون المعلومات الشخصية النطاق المنصوص عليه في المادة 15 والفقرة 39-3 الفقرات 1 و2 من نفس القانون أو توفيره إلى طرف ثالث خارج النطاق المنصوص عليه في المادة 17 و 3 من القانون نفسه، في حين أن المادة 18 من الفقرة 2 تنص على أن يكون هناك ما يزيد عن الغرض قد يتم انتهاك S من صاحب البيانات أو طرف ثالث بشكل غير عادل، كما هو الحال في الحالات التي توجد فيها أحكام خاصة في القوانين الأخرى (الفقرة 2)، هل يقع ضمن "الحالات التي توجد فيها أحكام خاصة في قوانين أخرى" وفقا للمادة 18 فقرة 2 فقرة فرعية 2 من "قانون الحماية"؟

خلفية السؤال: لدى وزارة الداخلية والأمن أسئلة حول جوهر التحقيق المذكور أعلاه وطلبت تفسير القانون من وزارة التشريع الحكومي.

الإجابة: لا تنطبق المادة 26 من قانون معالجة الشكاوى المدنية على "الحالات التي توجد فيها أحكام خاصة في قوانين أخرى "بموجب المادة 18، الفقرة 2، البند 2 من قانون حماية البيانات الشخصية".

السبب: تم سن قانون حماية المعلومات الشخصية لتعزيز حماية المواطنين من الأضرار التي يعاني منها بسبب انتهاكات المعلومات الشخصية وضمان حقوقهم ومصالحهم، مثل التسرب وإساءة الاستخدام للمعلومات الشخصية، من بين ما يجب الالتزام به من قبل المعالجين لحماية المعلومات

---

[167] قرار المحكمة العليا بكوريا الجنوبية، رقم do104612013، بتاريخ: 27 فبراير 2014، على موقع CaseNote: https://casenote.kr/%EB%8C%80%EB%B2%95%EC%9B%90/2013%EB%8F%8410461، تاريخ الاطلاع: 2025/09/13، على الساعة 11:32 مساء.

الشخصية، حظر استخدام المعلومات الشخصية لأغراض أخرى غير الغرض المقصود (الفقرة 2) والالتزام بمعالجة المعلومات الشخصية بطريقة تقلل من غزو خصوصية موضوع المعلومات (الفقرة 6)، فإن "الحالات" التي تتمثل فيها في الفقرة يجب أن ينظر إلى الغرض المقصود أو المقدمة إلى طرف ثالث، على الرغم من الفقرة 1 من نفس المقالة، على أنها الحالات التي تسمح فيها القوانين الفردية على وجه التحديد باستخدام المعلومات الشخصية لأغراض أخرى غير الغرض المقصود ومتطلبات توفير هذه المعلومات إلى طرف ثالث، من خلال تحديد نوع المعلومات الشخصية ومتطلباتها لتوفير هذه المعلومات.

وبالتالي السماح لرئيس وكالة إدارية بالاستفادة من النتائج التي تم التحقيق فيها من قبله في تحسين نظام إدارة الالتماس المدني، ومع ذلك، المادة 6-5، الفقرة 2 من قانون الخدمة العامة، المادة السائدة أحكام بشأن القيود المفروضة على استخدام المعلومات الشخصية لأغراض أخرى غير الغرض المقصود إلى أطراف ثالثة وفقا للمادة 18، الفقرة 1 من قانون حماية المعلومات الشخصية، نظرا لأن هذا الحكم غير منصوص عليه على وجه التحديد، وإذا كان ذلك ضروريا لتحسين نظام إدارة الشكاوى المدنية الأكثر كفاءة، فقد يتم التحقيق في رضا المشتكي ومجالات التحسين، بموافقة منفصلة من موضوع المعلومات وفقا للفقرة الفرعية 1 من الفقرة 2 من نفس المادة، ومن الصعب النظر إلى المادة 26 من قانون التعامل مع الشكاوى المدنية على أنها حكم يفترض استخدام المعلومات الشخصية لأغراض أخرى غير الغرض المقصود أو تقديمها إلى طرف ثالث لإدارة متابعة الشكاوى المدنية التي تتم معالجتها.

بالإضافة إلى ذلك، فإن الحق في تقرير المصير للمعلومات الشخصية التي يضمنها الحق العام المستمدة من المادة 10 من دستور جمهورية كوريا والحق في الخصوصية وحرية الحياة الخاصة بموجب المادة 17 من دستور جمهورية كوريا هي حق المعلومات، يتصرف المبدأ الذي يقيد الحق في تقرير المصير للمعلومات الشخصية، ثم أن معالجة المعلومات الشخصية بما يتجاوز الغرض الأصلي من التجميع، ستؤدي إلى تقييد الحق بشكل غير معقول في تقرير المصير للمعلومات الشخصية، ويجب أن يؤخذ في الاعتبار أيضا أنه يسبب الضرر عند تفسير هذه المسألة.

وعليه فإن المادة 26 من قانون معالجة الشكاوى المدنية لا تتوافق مع "الحالات التي توجد فيها أحكام خاصة في قوانين أخرى" بموجب المادة 18، الفقرة 2، البند 2 من قانون حماية البيانات الشخصية، والمادة 26 من قانون معالجة الالتماسات المدنية: (إدارة الالتماسات المدنية اللاحقة) يجوز لرئيس الهيئة الإدارية التحقق من رضا مقدم الالتماس ومجالات التحسين فيما يتعلق بالالتماسات المدنية التي تمت معالجتها وأن يعكس ذلك في عمله.

المادة 18 من قانون حماية البيانات الشخصية: (القيود المفروضة على استخدام/توفير البيانات الشخصية لأغراض أخرى غير الغرض) ① لا يجوز لمعالجي البيانات الشخصية استخدام البيانات الشخصية بما يتجاوز النطاق المنصوص عليه في المادة 15 الفقرة 1 والمادة 39-3 الفقرتين 1 و2، أو تقديم البيانات الشخصية إلى أطراف ثالثة بما يتجاوز النطاق المنصوص عليه في المادة 17 الفقرتين 1 و3. ②على الرغم من الفقرة 1، يجوز لمعالج المعلومات الشخصية استخدام المعلومات الشخصية لأغراض أخرى غير الغرض المقصود أو تقديمها إلى طرف ثالث.

باستثناء الحالات التي يكون فيها خطر الانتهاك غير العادل لمصالح صاحب البيانات أو طرف ثالث في أي من الحالات التالية: ومع ذلك، في حالة مقدمي خدمات المعلومات والاتصالات (بالإشارة إلى الأشخاص الذين يقعون تحت المادة 2، الفقرة 1، الفقرة الفرعية 3 من قانون تعزيز استخدام شبكة المعلومات والاتصالات وحماية المعلومات، وينطبق الشيء نفسه فيما يلي: الذين يقومون بمعالجة المعلومات الشخصية للمستخدمين (بالإشارة إلى الأشخاص الذين يقعون تحت المادة 2، الفقرة 1، الفقرة الفرعية 4 من قانون تعزيز استخدام شبكة المعلومات والاتصالات وحماية المعلومات، وينطبق الشيء نفسه فيما يلي، يتم تقييد الحالتين 1 و2، وتقتصر الحالات من 5 إلى 9 على المؤسسات العامة: 1 .في حالة الحصول على موافقة منفصلة من صاحب البيانات، 2 .في حالة وجود أحكام خاصة في قوانين أخرى.[168]

نطاق معالجي المعلومات الشخصية بموجب قانون حماية المعلومات الشخصية (المتعلق بالمادة 2 من قانون حماية المعلومات الشخصية) بتاريخ 24 يونيو 2019، كما يلي:

ملخص السؤال: عندما تقوم حكومة محلية، وهي مؤسسة عامة بموجب المادة 2، الفقرة 6، الفقرة الفرعية 7 من قانون حماية المعلومات الشخصية، بمعالجة العمل المتعلق بعرائض المواطنين وطلبات الإفصاح عن المعلومات، إذا كان هناك شخص مسؤول عن عمل الاستقبال والتعيين (يشار إليه فيما يلي باسم "مدير الاستقبال / التعيين") وشخص مسؤول عن معالجة عرائض المواطنين المعينة وطلبات الإفصاح عن المعلومات (يشار إليه فيما يلي باسم "المدير الفردي")، فهل يمكن اعتبار مدير

---

168 التفسير الرسمي لوزارة التشريعات الحكومية، [وزارة التشريعات الحكومية 21-0889، 26 أبريل 2022، وزارة الداخلية والأمن]، على موقع CaseNote: https://casenote.kr/%EB%B2%95%EB%A0%B9/%EA%B0%9C%EC%9D%B8%EC%A0%95%EB%B3%B4_%EB%B3%B4%ED%98%B8%EB%B2%95/%EC%A0%9C18%EC%A1%B0، تاريخ الاطلاع: 2025/09/13، على الساعة 11:32 مساء.

الاستقبال / التعيين والمدير الفردي معالجين للمعلومات الشخصية بموجب المادة 2، الفقرة 5 من نفس القانون

خلفية الاستفسار: استفسر مقدم الطلب من وزارة الداخلية والأمن كما هو موضح في الاستفسار أعلاه، ردت وزارة الداخلية والأمن بأنه في الحالة المذكورة أعلاه، فإن الحكومات المحلية، وهي مؤسسات عامة، هي وحدها التي تتولى معالجة المعلومات الشخصية، وأن كل شخص مسؤول هو معالج للمعلومات الشخصية وفقا للمادة 28، الفقرة 1 من قانون حماية المعلومات الشخصية، إلا أن مقدم الطلب كان له رأي مختلف، وطلب من وزارة الداخلية والأمن تفسير القانون من وزارة التشريعات الحكومية.

إجابة: في هذه الحالة لا يمكن اعتبار الشخص المسؤول عن تلقي المعلومات وتخصيصها والشخص المسؤول الفردي معالجا للمعلومات الشخصية وفقا للمادة 2 (التعاريف) الفقرة 5 من قانون حماية المعلومات الشخصية، والتي تقول:" يشير مصطلح "معالج المعلومات الشخصية" إلى مؤسسة عامة أو شركة أو منظمة أو فرد يقوم بمعالجة المعلومات الشخصية بنفسه أو من خلال شخص آخر بهدف تشغيل ملفات المعلومات الشخصية لأغراض تجارية".

السبب: ينظم قانون حماية المعلومات الشخصية عموما معالجي المعلومات الشخصية بموجب الفقرة 5 من المادة 2 من القانون نفسه باعتبارهم أشخاصا ملتزمين بالمعايير في تحديد المحظورات ومعايير السلوك، ويفرض عقوبات جنائية عند انتهاك معالجي المعلومات الشخصية لالتزامات معينة، لذلك، يجب تفسير نطاق معالجي المعلومات الشخصية بموجب الفقرة 5 من المادة 2 من القانون نفسه، والتي تشكل أساس العقوبات الجنائية، تفسيرا دقيقا، ولا يسمح بالتوسع المفرط أو التفسير القياسي لمعنى الأحكام الصريحة في اتجاه غير موات للأطراف، لأنه يتعارض مع مبدأ الشرعية.

ومع ذلك، فإن المادة 2، الفقرة 5 من قانون حماية المعلومات الشخصية تعرف معالج المعلومات الشخصية بأنه مؤسسة عامة أو شركة أو منظمة أو فرد يقوم بمعالجة المعلومات الشخصية بنفسه أو من خلال شخص آخر من أجل تشغيل ملف معلومات شخصية لأغراض تجارية، في حين تشير المادة 28، الفقرة 1 من نفس القانون إلى الشخص الذي يعالج المعلومات الشخصية تحت إشراف معالج المعلومات الشخصية، مثل الموظف باعتباره معالجا للمعلومات الشخصية، في ضوء الأحكام ونظام قانون حماية المعلومات الشخصية، يتضح من النص أن الحكومات المحلية، التي هي مؤسسات عامة بموجب المادة 2 ولا يمكن اعتبارها معالجات المعلومات الشخصية، تحدث المعلومات من قبل مدير الاستقبال/التخصيص أو المديرين الأفراد، وبالتالي يعتبر مدير الاستقبال/التخصيص والمديرين الأفراد معالجين للمعلومات الشخصية بموجب المادة 2، الفقرة 5 من نفس القانون.

هناك رأي مفاده أنه ينبغي أن ينظر إليه، مع ذلك، ينص قانون حماية البيانات الشخصية على أفعال محظورة على "الأشخاص الذين يعالجون أو عالجوا البيانات الشخصية" بالإضافة إلى "معالجي البيانات الشخصية" (المادة 59)، وينص على عقوبات لمن ينتهكون هذه الأفعال المحظورة (المادة 71، الفقرتان 5 و6، والمادة 72، الفقرة 2) لذلك، فإن هذا الرأي غير صحيح، لأنه يمنع الضرر الناجم عن انتهاكات البيانات الشخصية من قبل أشخاص غير معالجي البيانات الشخصية، ويحقق الأغراض التشريعية لقانون حماية البيانات الشخصية، مثل حماية سرية الحياة الخاصة، (مواد من قانون حماية البيانات الشخصية ذات الصلة بالتفسير كما يلي: المادة 2 -التعاريف، المادة 17 -توفير المعلومات الشخصية، المادة 18- القيود المفروضة على استخدام/توفير المعلومات الشخصية لأغراض أخرى غير الغرض المقصود، المادة 36 - تصحيح/حذف البيانات الشخصية، المادة 37 - تعليق معالجة البيانات الشخصية، المادة 59 - الأفعال المحظورة).[169]

ثانيا: حالة تسجيل ملفات المعلومات الشخصية

① الغرض من معالجة وفترة الاحتفاظ وعناصر ملفات المعلومات الشخصية المسجلة والمعلنة من قبل *Government24* وفقا للمادة 32 من قانون حماية المعلومات الشخصية[170]، ويتم جمع المعلومات الشخصية واستخدامها بالحد الأدنى الضروري لتوفير العمل أو الخدمة ذات الصلة، وهي كما يلي :

1 .عناصر المعلومات الشخصية التي تتم معالجتها بموافقة صاحب البيانات

تقوم *Government24* بمعالجة عناصر المعلومات الشخصية التالية بموافقة صاحب البيانات:

معلومات أعضاء*Government24* : سجل طلبات الالتماسات المدنية الإلكترونية (بما في ذلك سجل الاستشارات)؛ شهادة الشكوى المدنية الإلكترونية (الطلب والوثيقة الصادرة): وفقا للمادة 15، الفقرة 1، الفقرة الفرعية 1 من قانون حماية المعلومات الشخصية (موافقة صاحب البيانات) المادة 90 من مرسوم تنفيذ قانون الحكومة الإلكترونية (معالجة المعلومات الحساسة ومعلومات التعريف الفريدة).

---

[169] التفسير الرسمي لوزارة التشريعات الحكومية، نطاق معالجي المعلومات الشخصية بموجب قانون حماية المعلومات الشخصية (المتعلق بالمادة 2 من قانون حماية المعلومات الشخصية، [تشريعات وزارة الحكومة 19-0152، 24 يونيو 2019، وزارة الداخلية والأمن]، على موقع NEPLA Beta: https://apps.osrah.sa/jWScjx ، تاريخ الاطلاع: 2025/09/13، على الساعة 11:49 مساء.

[170] التفسير الرسمي لوزارة التشريعات الحكومية، رقم 19-0314، بتاريخ: 17 سبتمبر 2019، [المشتكي - نطاق المعلومات الحساسة المحظور معالجتها من قبل معالجي المعلومات الشخصية (بخصوص المادة 23 من قانون حماية المعلومات الشخصية)، على موقع CaseNote: https://casenote.kr/%EB%B2%95%EC%A0%9C%EC%B2%98/19-0314-674d2d، تاريخ الاطلاع: 2025/09/13، على الساعة 11:49 مساء.

موضوع المعلومات الشخص الذي يجمع المعلومات الشخصية) مطلوب: الاسم، عنوان المنزل، البريد الإلكتروني، رقم تسجيل المقيم، رقم تسجيل الأجانب اختياري: الهاتف المحمول (معلومات الاتصال) الممثل القانوني (الوصي على طفل يقل عمره عن 14 عاما)؛ مطلوب: الاسم، عنوان المنزل، البريد الإلكتروني؛ اختياري: الهاتف المحمول (معلومات الاتصال).

معلومات المعيشة: وفقا للمادة 15، الفقرة 1، الفقرة الفرعية 1 من قانون حماية البيانات الشخصية (موافقة صاحب البيانات) المادة 9-2 من قانون الحكومة الإلكترونية (توفير المعلومات الحية من خلال بوابة الحكومة الإلكترونية).

ثالثا: المسائل المتعلقة بمعالجة البيانات الشخصية للأطفال دون سن 14 عاما

عند جمع البيانات الشخصية للأطفال الذين تقل أعمارهم عن 14 عاما، يجوز لحكومة *24* طلب الحد الأدنى من المعلومات من الطفل، مثل: اسم الممثل القانوني ومعلومات الاتصال به، والطلب من الممثل القانوني توضيح موافقته على الموقع الإلكتروني الذي نشرت فيه الموافقة، وأما التأكد من موافقة الممثل القانوني في موقع الحكومة 24 فيتم من خلال جعل الممثل القانوني يشير إلى موافقته أو عدم موافقته على الموقع الإلكتروني حيث يتم نشر الموافقة وإخطار الممثل القانوني بتأكيد هذه الموافقة عبر رسالة نصية إلى الهاتف المحمول للممثل القانوني.

رابعا: نتائج تقييم أثر المعلومات الشخصية

①تقوم حكومة *24* "بتقييم تأثير المعلومات الشخصية"، بـ "تقييم تأثير المعلومات الشخصية" وفقا للمادة 33 من قانون حماية المعلومات الشخصية[171] للتحقيق وتحليل وتقييم التأثير الذي قد يحدثه نظام معالجة المعلومات الشخصية الذي تديره على ملفات المعلومات الشخصية لأصحاب البيانات.

خامسا: مدة معالجة البيانات الشخصية والاحتفاظ بها

①تقوم حكومة *24* بمعالجة البيانات الشخصية ضمن فترة الاحتفاظ بالبيانات الشخصية واستخدامها المنصوص عليها في القانون أو ضمن فترة الاحتفاظ بالبيانات الشخصية واستخدامها المتفق عليها من قبل صاحب البيانات عند جمع البيانات الشخصية.

② فترة المعالجة والاحتفاظ بكل معلومة شخصية هي كما يلي:

1 .معلومات أعضاء الحكومة 24: حتى 5 أيام بعد انسحاب العضوية

[171] المادة 33 من قانون حماية المعلومات الشخصية -كوريا الجنوبية، مرجع سابق.

2 .تاريخ تقديم الشكوى المدنية الإلكترونية (بما في ذلك تاريخ الاستشارة): 3 سنوات

3 .شهادة الشكوى المدنية الإلكترونية (نموذج الطلب والوثيقة الصادرة): 180 يوما

4. معلومات المعيشة: يوم واحد.

سادسا: مسائل تتعلق بإجراءات وطرق إتلاف المعلومات الشخصية

تقوم *الحكومة 24* بتدمير البيانات الشخصية دون تأخير عندما تصبح غير ضرورية، مثل انتهاء مدة الاحتفاظ بالبيانات الشخصية أو تحقيق غرض المعالجة، وقد تمت الإشارة إلى إجراءات وطرق لتدمير المعلومات الشخصية.

سابعا: المسائل المتعلقة بتقديم المعلومات الشخصية إلى أطراف ثالثة

① تقوم *Government24* بمعالجة المعلومات الشخصية للكيانات الحكومية فقط ضمن النطاق المحدد في المادة 1 (غرض معالجة المعلومات الشخصية)، وتقدم المعلومات الشخصية إلى أطراف ثالثة فقط في الحالات المقابلة للمادتين 17 (توفير المعلومات الشخصية)[172] و18 من قانون حماية المعلومات الشخصية[173]، مثل موافقة صاحب البيانات أو الأحكام الخاصة للقانون.

ثامنا: معايير الحكم عندما يحدث استخدام أو توفير إضافي بشكل مستمر

يجوز *للحكومة 24* أيضا استخدام وتقديم المعلومات الشخصية دون موافقة صاحب البيانات في ضوء المسائل المنصوص عليها في المادة 14-2 (معايير الاستخدام/التوفير الإضافي للمعلومات الشخصية) من مرسوم تنفيذ قانون حماية المعلومات الشخصية والتي تقول: "① في الحالات التي يعتزم فيها معالج المعلومات الشخصية استخدام أو توفير المعلومات الشخصية دون موافقة صاحب البيانات وفقا للفقرة 3 من المادة 15[174] من قانون حماية المعلومات الشخصية، وعند النظر في الفقرتين نرى أن لهما نفس النص بالحرف.

تاسعا: المسائل المتعلقة بتكليف أعمال معالجة المعلومات الشخصية

①تقوم *حكومة24* بتكليف مهام معالجة المعلومات الشخصية لشركة معالجة الشحنات (المرسل إليه)، لضمان معالجة سلسة للمعلومات الشخصية.

---

[172] المادة 17 (توفير البيانات الشخصية)، قانون حماية البيانات الشخصية -كوريا الجنوبية، نفس المرجع.

[173] المادة 18 (القيود على استخدام وتوفير المعلومات الشخصية لأغراض أخرى غير تلك المذكورة)، قانون حماية المعلومات الشخصية، نفس المرجع.

[174] المادة 15 (جمع واستخدام المعلومات الشخصية)، قانون حماية المعلومات الشخصية، نفس المرجع.

②عند إبرام عقد الإرسال، وفقا للمادة 26 (القيود المفروضة على معالجة البيانات الشخصية بسبب الاستعانة بمصادر خارجية للعمل)[175] من قانون حماية المعلومات الشخصية، تنص *الحكومة 24* في العقد أو أي وثيقة أخرى مسائل تتعلق بالمسؤوليات مثل حظر معالجة المعلومات الشخصية لأغراض أخرى غير أداء العمل المرسل، وتدابير الحماية الفنية والإدارية، والقيود المفروضة على إعادة الإرسال، وإدارة وإشراف المرسل إليه، والتعويض عن الأضرار، والإشراف على ما إذا كان المرسل إليه يعالج المعلومات الشخصية بأمان.

③ وفقا للمادة 26، الفقرة 6 من قانون حماية المعلومات الشخصية، تحصل شركة المعالجة الموكلة (المؤتمن) على موافقة وزارة الداخلية والأمن عندما يعهد المؤتمن مرة أخرى إلى شركتهم بأعمال معالجة البيانات الشخصية.

④ في حالة تغير محتوى العمل الموكل أو الوصي، سوف تقوم حكومة 24 بالكشف عنه دون تأخير من خلال سياسة معالجة المعلومات الشخصية هذه.

عاشرا: المسائل المتعلقة بجمع ونقل المعلومات الشخصية إلى الخارج

لا تقوم *Government24* بجمع أو معالجة المعلومات الشخصية في الخارج، وفي حالة الجمع أو المعالجة الإضافية، ستقدم المعلومات حتى يتمكن صاحب البيانات من تأكيدها، كما لا تقوم بتوفير أو تكليف أي معلومات شخصية إلى الخارج، وفي حالة تقديم أو تكليف إضافي، فستقدم إرشادات حتى يتمكن صاحب المعلومات من تأكيدها.

الفقرة الثانية: الجزء الثاني من سياسة الخصوصية للتطبيقات الإلكترونية_ موقع حكومة *24* نموذجا

من هنا نستكمل الجزء الثاني من سياسة الخصوصية التي تنطبق على جميع التطبيقات الإلكترونية بكوريا الجنوبية وفقا لقانونها المتعلق بحماية البيانات الشخصية، كما يلي:

أحد عشر: المسائل المتعلقة بالتدابير الرامية إلى ضمان سلامة المعلومات الشخصية

تتخذ حكومة *24* التدابير التالية لضمان سلامة البيانات الشخصية: من إنشاء وتنفيذ خطة إدارة داخلية؛ تقليل وتدريب الموظفين المسؤولين عن التعامل مع المعلومات الشخصية؛ تنفيذ التوجيه الذاتي

---

[175] المادة 26 (القيود المفروضة على معالجة البيانات الشخصية بسبب الاستعانة بمصادر خارجية للعمل)، من قانون حماية المعلومات الشخصية، نفس المرجع.

بشكل منتظم كل عام؛ تقييد الوصول إلى المعلومات الشخصية؛ تخزين سجلات الوصول؛ إدارة حقوق الوصول؛ تشفير المعلومات الشخصية؛ الإجراءات الفنية ضد القرصنة وغيرها؛ التحكم في الوصول للأشخاص غير المصرح لهم؛ إجراء عمليات تفتيش ذاتية منتظمة؛ وإنشاء خطة إدارة داخلية.

اثنا عشر: إمكانية الكشف عن المعلومات الحساسة وطريقة اختيار عدم الكشف

عندما تقرر حكومة *24* أن هناك خطر انتهاك الخصوصية بسبب إدراج معلومات حساسة لموضوع المعلومات في المعلومات التي تم الكشف عنها في عملية تقديم الخدمة المدنية، فإنها ستقدم إرشادات حتى يتمكن موضوع المعلومات من التحقق من إمكانية الكشف عن المعلومات الحساسة وكيفية تحديد عدم الإفصاح قبل تقديم الخدمة.

ثلاثة عشر: المسائل المتعلقة بمعالجة المعلومات المستعارة

لا تقوم *Government24* بإخفاء هوية المعلومات الشخصية، وإذا فعلت ذلك، فسوف تقدم إرشادات حتى يتمكن صاحب المعلومات من تأكيد المعلومات ذات الصلة.

تدخل المادتين 28-2 و28-3 من قانون حماية البيانات الشخصية[176] في إطار معالجة المعلومات المستعارة:

- مسائل تتعلق بمعالجة المعلومات المستعارة.
- مسائل تتعلق بتقديم معلومات مجهولة المصدر إلى أطراف ثالثة.
- مسائل تتعلق بتكليف معالجة المعلومات المستعارة

في نفس السياق تم تأكيد عدم دستورية المادة 28-7 من قانون حماية البيانات الشخصية في قرار للمحكمة الدستورية، في الجلسة بتاريخ 26 أكتوبر 2023، حيث يذهب القرار إلى ما إذا كانت المادة 28-5 من قانون حماية البيانات الشخصية (المشار إليها فيما يلي باسم "حكم حظر إعادة التعريف") تنتهك حق المدعين في تقرير مصيرهم بشأن البيانات الشخصية من خلال حظر إعادة التعريف بالمعلومات المستعارة دون استثناء (سلبي)، ثم ما إذا كانت المادة 28-7 من قانون حماية المعلومات الشخصية والمادة 40-3 من قانون استخدام وحماية معلومات الائتمان (المشار إليها فيما يلي بشكل جماعي باسم "استثناءات التطبيق") تنتهك حق المدعين في تقرير مصيرهم بشأن المعلومات

[176] المادة 28-2 (معالجة المعلومات المستعارة، إلخ) قانون حماية المعلومات الشخصية؛ المادة 28-3 (القيود المفروضة على دمج المعلومات المستعارة)، من قانون حماية المعلومات الشخصية لكوريا الجنوبية، نفس المرجع.

الشخصية من خلال استبعاد بعض أحكام حماية المعلومات الشخصية من تطبيقها على المعلومات المستعارة (سلبي)

ملخص القرار: يهدف حظر إعادة التعريف إلى حماية حق صاحب البيانات في تقرير مصيره بشأن المعلومات الشخصية بشكل كاف من خلال منع التعرف على أفراد محددين من خلال معلومات مستعارة، والغرض التشريعي منه مشروع، وتقليل إمكانية التعرف على أفراد محددين من خلال حظر إعادة التعريف هو وسيلة مناسبة لتحقيق هذا الغرض التشريعي.

إذا سمح بإعادة تحديد الهوية فقط للمعالج الأصلي المستعار، فهناك خطر إعادة المعلومات التي عولجت كمعلومات مستعارة إلى معلومات ذات تأثير كبير على صاحب البيانات، مما قد يسبب له ضررا غير متوقع، بالإضافة إلى ذلك، إذا سمح بإعادة تحديد الهوية فقط بناءً على طلب صاحب البيانات، فهناك خطر إعادة تحديد الهوية أيضا للمعلومات المُستعارة لجميع أصحاب البيانات الآخرين، ومن ثم، فمن الصعب أن نرى وسيلة أقل تدخلا من فرض حظر شامل وموحد على إعادة تحديد الهوية، وبالتالي يتم الاعتراف بالحد الأدنى من الانتهاك.

إن المصلحة العامة في تقليل احتمالية انتهاك المصالح القانونية لأصحاب البيانات من خلال حظر إعادة التعريف أكبر من المصالح الخاصة لأصحاب البيانات المقيدة بذلك، وبالتالي يتم الاعتراف أيضا بتوازن المصالح القانونية، وعليه فإن حكم منع إعادة التعريف لا ينتهك حق المطالبين في تقرير مصيرهم فيما يتعلق بالمعلومات الشخصية.

الغرض من هذا الاستثناء هو تسهيل استخدام المعلومات المستعارة، وبالتالي تفعيل استخدام البيانات، الغرض التشريعي مبرر، واستبعاد الأحكام التي يصعب تطبيقها نظرا لطبيعة المعلومات المستعارة يعد وسيلة مناسبة لتحقيق هذا الغرض التشريعي.

نظرا لأن المعلومات المستعارة لا يمكنها تحديد هوية فرد معين بمفردها، فمن الصعب أو المستحيل تطبيق التزامات الإخطار التي تنطبق على المعلومات الشخصية العامة بشكل مباشر، ونظرا لوجود لوائح أخرى لحماية صاحب البيانات، فمن المسلم به أن الانتهاك ضئيل، إن المصلحة العامة المترتبة على الاستخدام السلس للمعلومات المستعارة كبيرة، وبما أن المعلومات المستعارة التي لا يمكن التعرف عليها في حد ذاتها يمكن معالجتها دون موافقة لأغراض محدودة، فإن العيب

الذي يلحق بموضوع البيانات ليس كبيرا، وبالتالي هناك أيضا توازن بين المصالح القانونية، وعليه فإن بند الاستثناء لا ينتهك حق المطالبين في تقرير مصيرهم فيما يتعلق بالمعلومات الشخصية.[177]

ضمانا لسلامة المعلومات المستعارة يتم ذلك وفقا للمادة 28-4 من قانون حماية المعلومات الشخصية (الالتزام باتخاذ تدابير السلامة للمعلومات المستعارة، إلخ)[178]

أربعة عشر: المسائل المتعلقة بتثبيت وتشغيل الأجهزة التي تجمع المعلومات الشخصية تلقائيا ورفضها

تم تركيب وتشغيل جهاز جمع المعلومات الشخصية التلقائي:

①تستخدم حكومة *24* ملفات تعريف الارتباط لتخزين معلومات الاستخدام واسترجاعها بشكل دوري من أجل تقديم الخدمات الفردية والراحة للمستخدمين.

②ملفات تعريف الارتباط هي كمية صغيرة من المعلومات التي يرسلها الخادم (http) المستخدم لتشغيل موقع الويب إلى متصفح المستخدم ويتم تخزينها على جهاز الكمبيوتر الشخصي أو الهاتف المحمول الخاص بالمستخدم/ صاحب المعلومات.

③يمكن لموضوع المعلومات تعيين خيارات للسماح بملفات تعريف الارتباط أو حظرها من خلال خيارات متصفح الويب، ومع ذلك، إذا رفضت تخزين ملفات تعريف الارتباط، فقد تواجه صعوبات في استخدام الخدمات المخصصة.

لا تقوم *Government24* بجمع أو استخدام أو توفير معلومات سلوكية، وبالتالي لا يوجد شيء من هذا القبيل، فيما يتعلق بالمسائل المتعلقة بجمع المعلومات الصرفية واستخدامها وتوفيرها ورفضها.

---

[177] قرار المحكمة الدستورية بكوريا الجنوبية -قرار الهيئة الكاملة –2020 هيونما 1477، بتاريخ: 26 أكتوبر 2023، لتأكيد عدم دستورية المادة 28-7 من قانون حماية المعلومات الشخصية، على موقع CaseNote: https://casenote.kr/%ED%97%8C%EB%B2%95%EC%9E%AC%ED%8C%90%EC%86%8C/2020%ED%97%8C%EB%A7%881477، تاريخ الاطلاع: 2025/09/14، على الساعة 00:29 مساء.

[178] المادة 28-4 (واجب اتخاذ التدابير الأمنية بشأن المعلومات المستعارة وما إلى ذلك)، من قانون حماية المعلومات الشخصية لكوريا الجنوبية، مرجع سابق.

خمسة عشر: المسائل المتعلقة بالجمع والاستخدام والرفض عند السماح لطرف ثالث بجمع المعلومات السلوكية من خلال جهاز جمع المعلومات الشخصية التلقائي

لا تقوم *Government24* بجمع أو استخدام أو توفير معلومات سلوكية، وبالتالي لا يوجد شيء من هذا القبيل.

ستة عشر: المسائل المتعلقة بحقوق والتزامات صاحب المعلومات والممثل القانوني وطرق ممارستها

①يجوز لأصحاب البيانات ممارسة حقوقهم لدى حكومة *24* في أي وقت، بما في ذلك طلب الوصول إلى البيانات الشخصية أو تصحيحها أو حذفها أو تعليق معالجتها أو سحب الموافقة أو رفض القرارات الآلية أو طلب التوضيحات.

※يجب تقديم طلبات الاطلاع على البيانات الشخصية للأطفال دون سن الرابعة عشرة مباشرة من قبل الممثل القانوني، ويجوز للقاصرين الذين تزيد أعمارهم عن الرابعة عشرة ممارسة حقوقهم المتعلقة ببياناتهم الشخصية بأنفسهم أو من خلال ممثلهم القانوني.

②يجوز ممارسة الحقوق ضد حكومة *24* من خلال الوثائق المكتوبة، والبريد الإلكتروني، والفاكس (FAX)، وفقا للفقرة 1 من المادة 41 (إجراءات الاطلاع على البيانات الشخصية) من مرسوم تنفيذ قانون حماية المعلومات الشخصية، وستتخذ حكومة *24* الإجراءات اللازمة دون تأخير، كل من موقعه.

وتتضمن الفقرة 1 من المادة 41 من مرسوم تنفيذ القانون[179]: " إذا رغب صاحب البيانات في طلب الاطلاع على بياناته الشخصية وفقا للمادة 35 فقرة 1 من القانون، فيجب عليه طلب الاطلاع وفقا للطرق والإجراءات التي وضعها معالج البيانات الشخصية، على عناصر ومحتويات المعلومات الشخصية؛ الغرض من جمع المعلومات الشخصية واستخدامها؛ فترة الاحتفاظ بالمعلومات الشخصية واستخدامها؛ حالة تقديم المعلومات الشخصية إلى أطراف ثالثة؛ حقائق وتفاصيل الموافقة على معالجة المعلومات الشخصية".

[179] مرسوم تنفيذ قانون حماية البيانات الشخصية [المرسوم الرئاسي رقم 35343، 25 فبراير 2025، منقح جزئيا]، على موقع المركز الوطني للمعلومات القانونية بوزارة التشريع الحكومي، موقع رسمي للحكومة الإلكترونية لجمهورية كوريا الجنوبية: https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EA%B0%9C%EC%9D%B8%EC%A0%95%EB%B3%B4%EB%B3%B4%ED%98%B8%EB%B2%95%EC%8B%9C%ED%96%89%EB%A0%B9، تاريخ الاطلاع: 2025/09/14، على الساعة 00:40 صباحا.

③يجوز ممارسة الحقوق من خلال وكيل، مثل الممثل القانوني لصاحب البيانات أو الشخص المخول، في هذه الحالة، يجب عليك تقديم توكيل رسمي بالتنسيق الموضح في الملحق 11 من "إشعار بشأن أساليب معالجة المعلومات الشخصية".

④يجوز تقييد حق صاحب البيانات في طلب الوصول إلى المعلومات الشخصية وإيقاف معالجتها وفقا للفقرة 4 من المادة 35 (إدارة ودعم نقل المعلومات الشخصية)[180].

ثم الفقرة 2 من المادة 37 (حقوق أصحاب البيانات فيما يتعلق بالقرارات الآلية) من قانون حماية المعلومات الشخصية، التي تقول: " إذا اتخذ معالج البيانات الشخصية قرارا آليا، فيجوز لصاحب البيانات أن يطلب توضيحا للقرار".[181]

⑤إذا تم تحديد المعلومات الشخصية كهدف للتجميع في قوانين أخرى، فلا يمكنك طلب حذف المعلومات الشخصية.

⑥إذا وافق صاحب المعلومات على اتخاذ قرار آلي، أو تم إخطاره مسبقا من خلال عقد أو وسيلة أخرى، أو إذا كانت هناك أحكام واضحة في القانون، فلا يجوز رفض القرار الآلي ويسمح فقط بطلبات التوضيح والمراجعة، بالإضافة إلى ذلك، يجوز رفض طلبات الرفض أو تفسير القرارات الآلية إذا كانت هناك أسباب مشروعة، مثل المخاوف من أنها قد تنتهك بشكل غير عادل حياة أو جسد أو ممتلكات أو مصالح أخرى لشخص آخر.

⑦تتحقق *حكومة 24* مما إذا كان مقدم الطلب، مثل طلب التفتيش، أو التصحيح/الحذف، أو تعليق المعالجة أو سحب الموافقة، أو رفض القرار الآلي أو طلب التوضيح، هو الشخص المعني أو وكيل شرعي.

⑧يمكن *لحكومة 24* أن تطلب الوصول إلى المعلومات الشخصية من القسم الخاص بها، ويمكن لأصحاب البيانات أيضا طلب الوصول إلى معلوماتهم الشخصية من خلال موقع "بوابة المعلومات الشخصية(www.privacy.go.kr) ".

---

[180] المادة 35-4 (إدارة ودعم نقل المعلومات الشخصية)، قانون حماية المعلومات الشخصية -كوريا الجنوبية، مرجع سابق.

[181] المادة 37-2 (حقوق أصحاب البيانات فيما يتعلق بالقرارات الآلية)، قانون حماية البيانات الشخصية -كوريا الجنوبية، نفس المرجع.

سبعة عشر: اسم المسؤول عن حماية البيانات الشخصية (حسب المجال)، أو القسم المسؤول عن عمل البيانات الشخصية، والقسم الذي يتعامل مع الشكاوى

تتحمل حكومة *24* مسؤولة عن الإدارة الشاملة لمعالجة المعلومات الشخصية، وقد عينت مسؤولا لحماية المعلومات الشخصية (حسب المجال) للتعامل مع الشكاوى وتوفير سبل الانتصاف للأضرار الناجمة عن أصحاب البيانات فيما يتعلق بمعالجة المعلومات الشخصية، ويجوز لأصحاب البيانات الاستفسار عن جميع المسائل المتعلقة بحماية البيانات الشخصية، بما في ذلك الشكاوى، وتخفيف الأضرار، التي تنشأ أثناء استخدام خدمات حكومة *24*.

ثمانية عشر: سبل الانتصاف في حالة انتهاك حقوق أصحاب البيانات

①للحصول على تعويض في حالة انتهاك المعلومات الشخصية، يجوز لصاحب البيانات التقدم بطلب لحل النزاع أو التشاور مع لجنة الوساطة في نزاعات المعلومات الشخصية، ومركز الإبلاغ عن انتهاكات المعلومات الشخصية التابع لوكالة الإنترنت والأمن الكورية، لأي تقارير أو استفسارات أخرى بخصوص انتهاك المعلومات الشخصية، يتم الاتصال بالمنظمات التالية :

1 .لجنة الوساطة في نزاعات المعلومات الشخصية: (بدون رمز المنطقة) 1833-6972 (www.kopico.go.kr)

2 .مركز الإبلاغ عن انتهاكات المعلومات الشخصية: (بدون رمز المنطقة) 118 (privacy.kisa.or.kr)

3 .مكتب المدعي العام الأعلى: (بدون رمز المنطقة) 1301(www.spo.go.kr)

4 .وكالة الشرطة الوطنية: (بدون رمز المنطقة) 182(ecrm.cyber.go.kr)

②تضمن *Government24* حق صاحب المعلومات في تقرير مصيره فيما يتعلق بالمعلومات الشخصية، وتسعى جاهدة إلى تقديم المشورة والتعويض عن الأضرار الناجمة عن انتهاك المعلومات الشخصية.

③ يجوز لأي شخص تم انتهاك حقوقه أو مصالحه بسبب تصرف أو تقاعس رئيس مؤسسة عامة استجابة لطلب بموجب المادة 35 (الوصول إلى المعلومات الشخصية) أو المادة 36 (تصحيح/حذف المعلومات الشخصية) أو المادة 37 (تعليق معالجة المعلومات الشخصية، إلخ) من قانون حماية المعلومات الشخصية، أن يطلب مراجعة إدارية وفقا لقانون الاستئناف الإداري.

- لجنة الطعون الإدارية المركزية: (بدون رمز المنطقة) 110(www.simpan.go.kr)

تسعة عشر: نتائج تقييم مستوى حماية المعلومات الشخصية

تتلقى *Government24* (وزارة الداخلية والأمن) "تقييم مستوى حماية المعلومات الشخصية" الذي تجريه لجنة حماية المعلومات الشخصية كل عام وفقا للمادة 11-2 من قانون حماية المعلومات الشخصية،[182] وحصلت على درجة "أ" في تقييم مستوى حماية المعلومات الشخصية لعام 2023.

عشرين: المسائل المتعلقة بتشغيل وإدارة أجهزة معالجة معلومات الفيديو الثابتة

لا تقوم *Government24* بتشغيل معدات معالجة معلومات الفيديو الثابتة، لذا لا ينطبق هذا على الموقع..

واحد وعشرون: المسائل المتعلقة بتشغيل وإدارة أجهزة معالجة معلومات الفيديو المحمولة

لا تقوم *Government24* بتشغيل جهاز معالجة معلومات الفيديو المحمول، لذا لا ينطبق هذا على المستخدم.

المطلب الثاني: تسريب الخصوصية وكيفية رفع دعوى قضائية جماعية وفقا لقانون حماية البيانات الشخصية بكوريا الجنوبية

سنعمد إلى اختصار حوادث ووقائع تسريب الخصوصية بحكومة *24* بكوريا الجنوبية باعتبارها من بين التطبيقات الإلكترونية بالقطاع العام (الفقرة الأولى)، ثم سننظر في كيفية رفع دعوى قضائية جماعية لانتهاك المعلومات الشخصية وفقا لقانون حماية البيانات الشخصية بكوريا الجنوبية، وكذا العقوبات المطبقة على المخالفين لهذا القانون (الفقرة الثانية).

الفقرة الأولى: حوادث ووقائع تسريب الخصوصية بحكومة 24 بكوريا الجنوبية

وقعت حادثة شلل الكمبيوتر في أعطال حاسوبية بشكل مستمر في الشبكة الإدارية الوطنية التي تديرها هيئة موارد المعلومات الوطنية منذ 17 نوفمبر 2023، وتوالت عدة أيام من الحوادث التي تدخل في باب تسريب البيانات الشخصية بسبب أعطال في أغلب ما صرحت به حكومة كوريا الجنوبية آنذاك، ولا يدخل في باب الهجمات السيبرانية.

---

[182] المادة 11-2 (تقييم مستوى حماية المعلومات الشخصية)، قانون حماية المعلومات الشخصية-كوريا الجنوبية، نفس المرجع.

أولا: سبب الحادث

حتى تاريخ 20 نوفمبر 2023، لم يتم الكشف عن أي شيء بشكل واضح، في 19 نوفمبر/تشرين الثاني، أعلنت وزارة الداخلية والأمن أن سبب الفشل هو مشكلة في مفتاحL4 ، ويتكهن العاملون في صناعة تكنولوجيا المعلومات الخاصة بغير ذلك، في غضون ذلك، ووفقا لبيان نائب وزير الإدارة العامة والأمن، فإن المشكلة لم تكن بسبب مشكلة مادية في المعدات، بل حدثت مشكلة أثناء عملية تصحيح وتحديث برمجيات المعدات، وعندما واجه هذا الجهاز مشكلة.

كان هناك أيضا جهاز احتياطي، ولكن تم تصحيح هذا الجهاز الاحتياطي وتحديثه في نفس الوقت أيضا، مما أدى إلى عدم إمكانية استخدام كلا الجهازين، في 23 نوفمبر 2023، في جلسة عامة للجنة الإدارة العامة والأمن المنعقدة في الجمعية الوطنية، أشار نائب من حزب الدخل الأساسي إلى نائب وزير الإدارة العامة والأمن إلى وجود خطأ في النظام الحكومي يتعلق بـ "شلل الشبكة الإدارية".

من بين الآراء الحكيمة رأي بروفيسور في كلية الدراسات العليا لأمن المعلومات بجامعة كوريا الذي يقول بأنه: *"سواء كان الأمر يتعلق بالذكاء الاصطناعي أو الحوسبة السحابية، يجب أن يكون النظام الأساسي متينا أولا، ومع ذلك، فبينما تتزايد خوادم وأجهزة الكمبيوتر الحكومية، فإن ميزانية الصيانة في الواقع تتناقص"*، واقترح كما قال: *"بأن نقوم بإجراء تحقيق شامل لجميع الأنظمة المرتبطة بالحكومة الإلكترونية"*، وتابع: *"نظرا لأن ميزانية صيانة نظام الحكومة الإلكترونية وصيانته صغيرة جدا، فإن الشركات الكبيرة مترددة في المشاركة"*، وأشار إلى أنه: *"نتيجة لذلك، فإن الشركات الصغيرة والمتوسطة الحجم التي لديها عدد أقل من الموظفين تنتهي إلى الاستحواذ، وتصبح خبرة الموظفين المدنيين أكثر أهمية مما هي عليه عندما تقوم الشركات الكبيرة بذلك".*[183]

ثانيا: رد فعل الحكومة

في 19 نوفمبر/تشرين الثاني، أجرى وزير الداخلية والأمن تفتيشا ميدانيا على "خطأ الشبكة الإدارية" وأكد على أن: *"الخدمات التي تم استئنافها يجب أن تحظى بمزيد من الاستقرار حتى لا يواجه الجمهور أي إزعاج اعتبارا من الغد"*، وفي الرابع من ديسمبر/كانون الأول، صرح رئيس أركان الرئاسة في اجتماع لكبار المسؤولين في الحزب والحكومة والإدارة عقد في مقر إقامة رئيس

[183] كيم سونغ جو، بروفيسور في كلية الدراسات العليا لأمن المعلومات بجامعة كوريا

الوزراء في اليوم السابق بشأن حادث فشل شبكة الكمبيوتر، بأن: *"كل هذا ينبع من حقيقة أننا لم نستثمر بشكل صحيح في شبكة الكمبيوتر في الماضي"*.[184]

الفقرة الثانية: رفع دعوى قضائية جماعية لانتهاك المعلومات الشخصية والعقوبات

إذا رفض معالج المعلومات الشخصية التوسط في نزاع جماعي وفقا للمادة 49 من قانون حماية البيانات الشخصية أو لم يقبل نتائج الوساطة، يجوز للمنظمة رفع دعوى قضائية (يشار إليها فيما يلي باسم "الدعوى الجماعية") في المحكمة لطلب حظر أو وقف الفعل المخالف: منظمة المستهلكين المسجلة لدى لجنة التجارة العادلة وفقا للمادة 29 من القانون الأساسي للمستهلك والتي تستوفي جميع المتطلبات التالية:

- يجب أن تكون المنظمة التي يكون هدفها الرئيسي هو تعزيز حقوق أصحاب المعلومات بشكل منتظم وفقا للنظام الأساسي للشركة.
- يجب أن يكون عدد الأعضاء المنتظمين للمجموعة 1000 على الأقل.
- يجب أن تمضي ثلاث سنوات منذ التسجيل وفقا للمادة 29 من قانون حماية المستهلك.

منظمة خاصة غير ربحية وفقا للمادة 2 من "قانون دعم المنظمات الخاصة غير الربحية" والتي تلبي جميع المتطلبات التالية:

- سيتم رفع دعوى قضائية جماعية من قبل 100 أو أكثر من أصحاب البيانات الذين عانوا من نفس الانتهاك القانوني أو الواقعي؛ بعد تحديد غرض المنظمة لحماية المعلومات الشخصية في النظام الأساسي للشركة، يجب أن يكون هناك سجل للأنشطة لهذا الغرض خلال السنوات الثلاث الماضية أو أكثر؛ يجب أن يبلغ عدد أعضاء المجموعة الدائمين 5000 عضوا على الأقل؛ كما يجب أن تكون مسجلة لدى الوكالة الإدارية المركزية، ومن هنا سنعمل على التعرف على كيفية رفع دعوى قضائية جماعية لانتهاك المعلومات الشخصية (أولا)، ثم العقوبات التي تطال كل مخالف لهذا القانون (ثانيا).

---

[184] لي سانغ مين، حادثة شلل الحاسوب في الشبكة الإدارية الوطنية لعام 2023، آخر تعديل: 08-05-2025، على موقع Namu: https://namu.wiki/w/2023%EB%85%84%20%EA%B5%AD%EA%B0%80%ED%96%89%EC%A0%95%EB%A7%9D%20%EC%A0%84%EC%82%B0%EB%A7%88%EB%B9%84%20%EC%82%AC%ED%83%9C#fn-8، تاريخ الاطلاع: 2025/09/14، على الساعة 15:23 مساء.

أولا: رفع دعوى قضائية جماعية لانتهاك المعلومات الشخصية

يضمن الفصل 8 من دعوى قضائية جماعية بشأن المعلومات الشخصية الذي تم تعديله في 4 فبراير 2020، من قانون حماية المعلومات الشخصية [تم تنفيذه في 13 مارس 2025] [القانون رقم 19234، 14 مارس 2023، (تم تعديله جزئيا)، كما يلي:

أ. الاختصاص الحصري: تخضع دعوى الدعوى الجماعية للاختصاص الحصري للقسم الجماعي للمحكمة الجزئية التي يقع في موقع المكتب الرئيسي أو مكتب الأعمال للمدعى عليه، أو في حالة عدم وجود مكتب رئيسي أو مكتب أعمال، في موقع عنوان مدير الأعمال الرئيسي، في حالة تطبيق ما سبق على مشغلي الأعمال الأجانب، يتم تحديد ذلك على أساس عنوان مكتبهم الرئيسي أو مكان عملهم أو مدير أعمالهم في جمهورية كوريا.

ب. تعيين ممثل في الدعوى: يجب على المدعي في دعوى جماعية أن يعين محاميا ممثلا له في الدعوى.

ت. طلب الإذن برفع الدعوى: يجب على المنظمة التي ترفع دعوى جماعية أن تقدم طلب الإذن برفع الدعوى إلى المحكمة مع الشكوى، متضمنا المعلومات التالية: المخطوطة ومحاميها - المدعى عليه - تفاصيل حقوق صاحب المعلومات التي تم انتهاكها، مع يجب إرفاق المستندات التالية بطلب الحصول على إذن برفع دعوى قضائية بموجب بما سبق: المستندات التي تثبت أن المنظمة الطالبة تستوفي أيا من المتطلبات (أهداف الدعاوى الجماعية)، والمستندات التي تثبت أن معالج البيانات الشخصية رفض التعديل أو لم يقبل نتيجة التعديل.

ث. شروط الإذن برفع الدعوى وغيرها: لا يجوز للمحكمة أن تمنح الإذن برفع الدعوى الجماعية بقرار إلا إذا توافرت الشروط التالية جميعها: رفض معالج البيانات الشخصية وساطة لجنة وساطة النزاعات أو لم يقبل نتائج الوساطة، ويجب ألا يكون هناك أي عيب في المعلومات المقدمة في طلب الحصول على إذن برفع الدعوى بموجب المادة 54 (طلب الإذن بالدعوى)، ويجوز تقديم استئناف فوري ضد القرار الذي يسمح أو يرفض دعوى قضائية جماعية.

ج. أثر الحكم النهائي: إذا أصبح الحكم الصادر برفض دعوى المدعي نهائيا فلا يجوز للمجموعات الأخرى المنصوص عليها في المادة 51 رفع دعوى جماعية بشأن نفس الموضوع ومع ذلك، لا ينطبق هذا عندما يتم اكتشاف أدلة جديدة من قبل الدولة أو الحكومة المحلية أو منظمة أنشأتها الدولة أو الحكومة المحلية بعد الانتهاء من الحكم، وإذا تبين أن قرار الفصل كان بسبب نية المدعي.

ح. تطبيق قانون المرافعات المدنية وغيرها: في الحالات التي لا توجد فيها أحكام خاصة في هذا القانون بشأن الدعاوى الجماعية، يسري قانون المرافعات المدنية، وفي حالة صدور قرار بالسماح برفع دعوى جماعية وفقا للمادة 55، يجوز اتخاذ إجراء حفظ وفقا للجزء الرابع من قانون التنفيذ المدني، وتحدد قواعد المحكمة العليا الأمور اللازمة لإجراءات الدعاوى الجماعية.[185]

ثانيا: العقوبات

العقوبات على انتهاك/تسرب البيانات الشخصية على حسب قانون حماية البيانات الشخصية بكوريا الجنوبية، بحيث يمثل لنا الفصل العاشر من قانون حماية البيانات الشخصية الكوري فصل العقوبات من المادة 70 إلى المادة 76 مما يشكل لنا رادعا لكل من سولت له نفسه انتهاك البيانات الشخصية للمواطنين والمؤسسات، كما يلي:

أ. يعاقب بالسجن مدة لا تزيد على عشر سنوات أو بغرامة لا تتجاوز مائة مليون وون كل شخص يقوم بتغيير أو حذف البيانات الشخصية التي تتم معالجتها بواسطة مؤسسة عامة مما يتسبب في حدوث خلل خطير، مثل تعليق أو شلل عمل المؤسسة العامة؛ الشخص الذي حصل على معلومات شخصية يتم معالجتها من قبل شخص آخر من خلال وسائل أو أساليب خاطئة أو غير لائقة وقدم هذه المعلومات إلى طرف ثالث لتحقيق الربح أو لأغراض غير لائقة، والشخص الذي حرض أو توسط في مثل هذا التوفير.

ب. يعاقب بالسجن مدة لا تزيد على خمس سنوات أو بغرامة لا تتجاوز خمسين مليون وون كل شخص على سبيل المثال لا الحصر، الشخص الذي يقدم معلومات شخصية إلى طرف ثالث دون موافقة صاحب البيانات والشخص الذي يتلقى معلومات شخصية على الرغم من علمه بالظروف؛ كل من قام بتصدير معلومات مجمعة خارج المؤسسة التي قامت بالدمج أو قدمها إلى طرف ثالث دون الحصول على موافقة رئيس المؤسسة المتخصصة؛ من سرب معلومات شخصية اطلع عليها أثناء عمله، أو قدم معلومات شخصية إلى شخص آخر دون إذن، وكذلك في جميع الحالات السابقة كل شخص تلقى معلومات شخصية بقصد الربح أو لأغراض غير مشروعة رغم علمه بالظروف؛ وكل من استخدم أو أتلف أو دمر أو غير أو زور أو سرب معلومات شخصية تخص شخصا آخر مخالفا.

---

[185] الفصل 8 من دعوى قضائية جماعية بشأن المعلومات الشخصية <تم تعديله في 4 فبراير 2020>، قانون حماية المعلومات الشخصية لكوريا الجنوبية، مرجع سابق.

يعاقب بالحبس مدة لا تزيد على ثلاث سنوات أو بغرامة لا تتجاوز ثلاثين مليون وون كل شخص يقوم بتشغيل جهاز معالجة معلومات الصورة الثابتة بشكل تعسفي لغرض آخر غير الغرض الذي تم تركيبه من أجله، ...؛ كل من حصل على معلومات شخصية أو حصل على موافقة لمعالجة المعلومات الشخصية بوسائل أو أساليب كاذبة أو غير لائقة، وكل من تلقى معلومات شخصية بغرض الربح أو لأغراض غير لائقة مع علمه بالظروف؛ من أفشى أسرارا اطلع عليها أثناء تأدية عمله أو استعملها في غير أغراض عمله.

ت. يعاقب بالحبس مدة لا تزيد على سنتين أو بغرامة لا تتجاوز عشرين مليون وون كل شخص يستمر في استخدام المعلومات الشخصية أو تقديمها إلى طرف ثالث دون اتخاذ التدابير اللازمة مثل التصحيح أو الحذف أو دون إيقاف معالجة المعلومات الشخصية؛ كل من خالف أمر السرية دون مبرر مقبول سواء على الصعيد المحلي أو الدولي، ولا يجوز مقاضاة الشخص الذي ارتكب الجريمة الأخيرة دون شكوى من الشخص الذي طلب أمر السرية؛ الشخص الذي يرفض تقديم البيانات أو يقدم بيانات كاذبة ردا على طلب تقديم البيانات، بالإضافة إلى الشخص الذي يرفض أو يعيق أو يتهرب من التحقيق عن طريق إخفاء أو التخلص من البيانات أو رفض الوصول أو تزوير أو تغيير البيانات أثناء الدخول أو التفتيش بغرض إخفاء أو تقليل انتهاكات القانون.

ث. يجوز مصادرة أي أموال أو فوائد أخرى حصل عليها شخص ارتكب جريمة تقع تحت طائلة أي من المواد من 70 إلى 73 فيما يتصل بالمخالفة ذات الصلة (وتجدر الإشارة إلى الفقرات السابقة هي المعنية بذلك)؛ إذا لم يكن من الممكن مصادرتها، يجوز تحصيل قيمتها، وفي هذه الحالة يجوز فرض المصادرة أو التحصيل الإضافي بالإضافة إلى العقوبات الأخرى.

ج. يعاقب بغرامة لا تزيد على خمسين مليون وون كل من ارتكب على سبيل المثال لا الحصر، ويفشل في إخطار تفاصيل استخدام/توفير المعلومات الشخصية أو طريقة الوصول إلى نظام المعلومات الذي يمكن من خلاله تأكيد تفاصيل الاستخدام/التوفير؛ الشخص الذي يفشل في اتخاذ التدابير اللازمة، مثل إتلاف البيانات الشخصية؛ والذي قام بمعالجة رقم تسجيل مقيم بالمخالفة؛ الشخص الذي يفشل في اتخاذ تدابير التشفير.

يتم فرض وتحصيل الرسوم الإضافية المنصوص عليها في الفقرات من 1 إلى 4 من قبل لجنة الحماية وفقا لأحكام القرار الجمهوري، وفي هذه الحالة يجوز للجنة الحماية تخفيض الغرامة أو الإعفاء منها مع مراعاة درجة المخالفة ودوافعها ونتيجة المخالفة وحجم معالج البيانات الشخصية.[186]

[186] الفصل العاشر العقوبات <تم تعديله في 4 فبراير 2020>، قانون حماية المعلومات الشخصية لكوريا الجنوبية، نفس المرجع.

الخاتمة:

تعمل المملكة المغربية وبرؤية ملكية سامية على استراتيجية المغرب الرقمي 2030، على بناء بنية تحتية متطورة وقوية تكون حاضنة للتكنولوجيات المتطورة مثل البيانات الضخمة والذكاء الاصطناعي، بالمقابل فإن التطوير من التكنولوجيا المادية والمعنوية يعزز احترام مبدأ الخصوصية ويقوي الأمن السيبراني، اللذان يجسدان صفة الحارس لبوابة الرقمنة، وتدعيما للابتكار الرقمي بكل أطيافه، بما يساهم في ضخ الاستثمارات الواعدة، والشراكات القيمة، وبالتالي خلق فرص شغل مبتكرة تواكب التطور العصري من جهة، ومن جهة ثانية تبني ثقة المواطنين بالمؤسسات العامة.

ومن الضروري أن لا أخفي صدمتي العلمية والتشريعية عند البحث عن قانون الذكاء الاصطناعي اكتشفت بأنه لازال يعتبر مشروع قانون في بلد مثل كوريا الجنوبية، والأدهى من ذلك كله لازال قانون الأمن السيبراني الذي يعد أساس الأمن والاستقرار لجميع التكنولوجيات ومادة الرقمنة بشموليتها، حتى أنه يعد من القوانين الحامية للأمن القومي بالبلدان كافة، وجدت أنه عبارة عن لوائح أعمال الأمن السيبراني وأنه هناك مشروع قانون لم تتم المصادقة عليه إلى يومنا هذا (عام 2025)، في المقابل عند معرفة السبب يبطل العجب!

حقيقة هناك عدة أسباب أغلبها شأن داخلي مرتبط بطبيعة كوريا الجنوبية وسياساتها، نذكر منها المعارضة القوية للحزب الحاكم، والتخوف من استبداد جهاز المخابرات الكوري الجنوبي بالبيانات الخاصة بالمواطنين، خاصة مع الأحداث الأخيرة التي وقعت بها، وإن كانت حاليا تعرف استقرارا، بالتالي كما قلت سابقا يبقى شأنا داخليا لا علاقة لنا به، وأفضل سبب قد تصدره لنا كوريا الجنوبية لعدم إصدارها قانون للأمن السيبراني هو أنها تحترم مبدأ الخصوصية وتقدسه لذلك تأخرت في إعداد قانون للأمن السيبراني، واكتفت باللوائح والأنظمة، والتي لا تشكل قوة ملزمة كالقانون، وإنما لوائح ذات طابع إداري محض.

في هذا الصدد، تتطلع كوريا الجنوبية لتجربة اليابان في تشريعها لقانون الأمن السيبراني، بالرغم من أنها أي كوريا الجنوبية لديها مشروع قانون للأمن السيبراني، تبقى تجربة الإمبراطورية اليابانية هي الأقرب لتجربة المملكة المغربية، بالرغم مما واجهته اليابان منذ عام 2014، من اختراق لتطبيق المعاشات، كما حصل في المغرب بهذا العام (عام 2025) وتسريب بيانات المواطنات والمواطنين، بل الأكثر من ذلك اختراق موقع اللجنة الوطنية لمراقبة حماية المعطيات الشخصية المغربي، مما يؤجج الرغبة في تعديل وتطوير الأمن السيبراني أخلاقيا وعلميا وبشريا وتقنيا وتشريعيا.

قبل الخوض في التوصيات المتعلقة بوضع سياسة الخصوصية للتطبيقات الإلكترونية وتعديل قانون رقم 09-08 المغربي، يمكن استخلاص الآثار والتوصيات على مستوى التقنيات، والقوانين المؤطرة لها كالتالي:

I. على مستوى الذكاء الاصطناعي

الحاجة إلى بناء نموذج ذكاء اصطناعي ضخم للغاية ومخصص للقطاع العام، من أجل تقديم الخدمات للجمهور بناء على المعلومات العامة دون تضمين معلومات حساسة عند تحديد الحجم أثناء عملية البناء، فمن الفعال الدفع واستخدام نموذج ذكاء اصطناعي خاص كبير في شكل واجهة برمجة التطبيقات، وبالنسبة للخدمات العامة التي تحتوي على معلومات حساسة، يمكن القيام ببناء وتأمين نماذج الذكاء الاصطناعي ذات الحجم المناسب لهذا الغرض.

يعد إنتاج واستخدام البيانات التي يمكن استخدامها بكفاءة بشكل منهجي، والتوجيه بشأن إنتاجها في القطاع العام أمرا في غاية الأهمية، الحذر مطلوب عند تقديم ChatGPT في هذا المجال، إذ في مايو 2023 أعلنت وزارة الإدارة العامة والأمن الكورية أنه يجب استخدام ChatGPT بشكل صحيح، حيث تم تقديم "دليل حول كيفية استخدام ChatGPT والاحتياطات" إلى حوالي 300 وكالة إدارية مركزية وحكومات محلية حتى يتمكنوا من الاستفادة منه، وعلى غرار ذلك نوصي بإعداد دليل شبيه بهذا الدليل الكوري في إطار التوعية بكيفية الاستخدام وبالتالي اتخاذ الاحتياطات اللازمة.

نوصي بتطوير الخدمات بناء على نماذج الذكاء الاصطناعي الضخمة للغاية وإنشاء بيئة تضمن صيانة الخدمات المطورة وتشغيلها بشكل جيد وتوسعتها، ومن المهم أيضا توفير بيئة تطوير قائمة على واجهة برمجة التطبيقات (API) أو ساحة حيث يمكن تطوير الخدمات المختلفة والتحقق منها بسهولة باستخدام نموذج لغة كبير جدا، وتوفير البنية التحتية ذات الصلة حتى تتمكن الخدمات المطورة من العمل بسلاسة، مع الجمع بين البيانات والبنية التحتية التي تقودها الحكومة مع التكنولوجيا من معاهد البحوث والأكاديمية المحلية، وتوسيع فهم الذكاء الاصطناعي، بالإضافة إلى وضع معايير وأنظمة إصدار الشهادات لضمان التوافق وإعادة استخدام البيانات وبيئات التطوير والخدمات متوافقة وقابلة لإعادة الاستخدام، ولا ينبغي إغفال هذا.

وفي نفس السياق تتزايد عدد الحالات التي يتم فيها تطبيق الذكاء الاصطناعي في الخدمات العامة والعمل الإداري الحكومي بكوريا الجنوبية، وبالتالي تظهر المخاطر والآثار الجانبية للذكاء الاصطناعي في الخدمات العامة أيضا، ويكمن رصد مثل هاته المخاطر والآثار الجانبية لدولة أجنبية كرؤية لآفاق الذكاء الاصطناعي بالمغرب، لذلك نوصي قبل الخوض بتطبيقه في الخدمات العامة عمل تقييم تأثير الذكاء الاصطناعي الذي يهدف إلى تقييم وتخفيف الآثار السلبية منذ المرحلة الأولية،

وضمان الاستخدام الأخلاقي والقانوني للذكاء الاصطناعي، كما نؤكد على الحاجة إلى التحسين المؤسسي لتمكين تقييمات أثر الذكاء الاصطناعي عند إدخاله أو استخدامه في القطاع العام.

وتأسيسا على ما سبق، في حالة عدم وجود لوائح أو تدابير تحكم للذكاء الاصطناعي وهذا هو الحال بالمغرب حاليا، وخاصة أن الوضع يتطلب قدرا أكبر من الرقابة، نظرا لتأثيره الكبير على حقوق وواجبات المواطنين، وينبغي أن يشمل هذا التقييم ليس فقط تقييم الأثر الوظيفي لأنظمة الذكاء الاصطناعي، بل وأيضا تقييم قيمة المنفعة الاجتماعية الناتجة عن إدخال أنظمة وخدمات الذكاء الاصطناعي، وتأثير ذلك على الحقوق الأساسية للمواطنين.

بالإضافة إلى ذلك، خاصة وأنه بسبب المخاطر غير المؤكدة بسبب حماية المعلومات الشخصية والتغييرات الجديدة، قد يزيد القلق لدى الجمهور، ومع ذلك، لا توجد حتى الآن مبادئ توجيهية محلية أو تقارير فنية فيما يتعلق بالتقنيات الأمنية الجديدة، ومن الضروري دراسة المفاهيم والفئات المناسبة للبلد بشكل متعمق، لتوقع نتائج من تدابير التوسيع وعلى نطاق صغير في استعمالات الذكاء الاصطناعي فيما بعد في الخدمات العمومية من أجل المواطنين، واستخدامها من قبل الموظفين لتحسين جودة العمل والزيادة في الإنتاجية، وبالتالي نوصي بوضع أساس قانوني لضمان إمكانية تشغيل تقييم تأثير الذكاء الاصطناعي بشكل مستقر، وينبغي أن يشمل ذلك لوائح بشأن إنشاء نظام حوكمة لإدارته وتشغيله، ومعايير الاختيار لهدف التقييم، وبنود التقييم الرئيسية، وطرق وإجراءات اختيار بنود التقييم، وردود الفعل على نتائج التقييم، ودعم تنفيذ تقييم الأثر.

بالرغم من أن حكومة المنصة الرقمية بكوريا الجنوبية تستخدم بنشاط الذكاء الاصطناعي على نطاق واسع لتحسين الخدمات العامة، إلا أن هناك ميل للتردد في استخدامه بسبب المعلومات الشخصية أو القضايا الأخلاقية، مع الاحترام الشديد لهذا التوجه، وعلى غرار ذلك نوصي بعمل إرشادات توجيه باستخدام الذكاء الاصطناعي للموظفين بالمغرب حماية للمقدرات الرقمية على المدى القريب، والعمل على توحيد الاستخدام الآمن للذكاء الاصطناعي فائق الضخامة على المدى البعيد.

كما نوصي بتطوير وتوزيع منهج عملي، نظرا لوجود نقص في الكتب المدرسية والبرامج التعليمية المتعلقة بالبيانات الضخمة والذكاء الاصطناعي، بحيث هناك حاجة إلى جهود على مستوى الحكومة لتطوير وتوسيع نطاق توزيع منهج البيانات الضخمة والذكاء الاصطناعي.

II. على مستوى راحة المستخدم

من الضروري تعزيز الأساس التقني (نظام تحليل البيانات الضخمة/الذكاء الاصطناعي، ...) والمؤسسي (أساس جمع بيانات الملف الشخصي) للخدمات المخصصة مثل الملفات الشخصية وسجل الاستخدام، والتوسع من الخدمات التي تعكس راحة المستخدم، وتشريع قانون للحكومة الإلكترونية.

III. على مستوى السحابة المحلية

يجب على الحكومة "وضع سياسات ولوائح من منظور كلي" وتنفيذ السياسات من خلال "التأكيد على التنفيذ" واستكمال أي أوجه قصور، وبالتالي نوصي بسن "قانون تعزيز الحوسبة السحابية"، ونعمد إلى تشريعه بما يوجب علينا الضمير الوطني، وألا نقع فيما وقعت فيه كوريا الجنوبية منذ عام 2015 وهو تاريخ إصدار قانونهم حول تعزيز الحوسبة السحابية، بحيث تم رصد فجوة متزايدة الاتساع للمنتجات الأجنبية مقارنة بالمنتجات المحلية بكوريا في سوق السحابة الخاصة، من قبل خبراء الاقتصاد بكوريا الجنوبية.

IV. على مستوى حماية المعلومات

يتم بالفعل استخدام بنية الثقة المعدومة من قبل شركات التكنولوجيا الكبرى أو الشركات الكبيرة، أو تم بالفعل تسويقها تجاريا كجزء من خدمات المؤسسة "الخدمات البنية التحتية السحابية مثل Google" لذلك من الصعب الانتشار من منظور حكومي، إذ تعتبر الثقة المعدومة منهجية واضحة، فمن الصعب توقع النتائج من خلال تنفيذ النموذج الأمني والتحقق منه، بحيث يعد ضربا من الخيال حسب رأي خبراء التكنولوجيا بكوريا الجنوبية.

في كوريا، هناك أوجه قصور في المبادئ التوجيهية والتقارير الفنية لذلك تتم مراجعة المفاهيم والفئات بشكل متعمق، ومن الملح إنشاء أساس سياسي عندهم، وكذلك يرجع الأمر لحماية الخصوصية، لذلك لا يمكننا الاعتماد على النموذج الكوري لأنه لا زال غير ناضج بالنسبة لهم على الأقل، لذلك نوصي بالإحاطة بالأمن السيبراني بسياج تقني ورقمي قوي وتشريعي قيادي ملائم بالمغرب.

V. على مستوى الأمن السيبراني

من خلال دراسة التجربة الكورية تعتبر ضعيفة في مجال الأمن السيبراني، على المستوى التشريعي مقارنة مع التجربة اليابانية، فالتجربة الأولى بفرط حرصها على مبدأ الخصوصية، وعمق خلافاتها الداخلية، وجدت غريمتها الجارة كوريا الشمالية موطئ قدم لانتهاك أمنها السيبراني، إلا أنه مع توالي الهجمات ستعمل كوريا الجنوبية على إصدار قانون للأمن السيبراني في العام القادم 2026، وعلى العكس من ذلك تجربة الإمبراطورية اليابانية التي تتشابه مع تجربة المملكة المغربية،

حتى في الهجمات التي استهدفتهما في كل من شبكة المعلومات التابعة لدائرة المعاشات التقاعدية، وبالتالي تسرب المعلومات الشخصية للمواطنين في كلا البلدين.

من هذا المنطلق نوصي بتعديل القانون الأساسي للأمن السيبراني للسماح للقطاعين العام والخاص بالعمل معا لاتخاذ التدابير اللازمة لضمان الاستعداد الكامل لهذا التجمع الكبير والعالمي، بالنظر للتجربة اليابانية نوصي كذلك بوضع التغييرات التالية بالمغرب:

الاستعانة بشركات محددة ملزمة بالتزامات السرية داخل البلاد، لتمكين التواصل السريع مع الأطراف ذات الصلة في المغرب والخارج.

يجب على الجامعات والمؤسسات التعليمية والبحثية الأخرى أن تسعى بشكل مستقل واستباقي إلى ضمان الأمن السيبراني، وتنمية الموارد البشرية بهذا المجال، وإجراء البحوث حوله ونشر نتائج هذه البحوث، فضلا عن السعي إلى التعاون مع التدابير المتعلقة بالأمن السيبراني التي تنفذها الحكومات الوطنية أو المحلية.

يتعين على الحكومة أن تتخذ التدابير التشريعية والمالية وغيرها من التدابير اللازمة لتنفيذ سياسات الأمن السيبراني، كما يجب عليها أن تسعى جاهدة إلى تحسين التنظيمات والعمليات الإدارية، عند اتخاذ التدابير المتعلقة بالأمن السيبراني، خاصة ضمان الأمن السيبراني في الأجهزة الإدارية الوطنية، كما يتعين على الجمهور أن يسعى إلى تعميق اهتمامه وفهمه لأهمية الأمن السيبراني واتخاذ الاحتياطات اللازمة.

تعزيز الصناعة وتعزيز القدرة التنافسية الدولية: وذلك عبر اتخاذ المغرب التدابير اللازمة من خلال تحسين الظروف التنافسية، والمشاركة في التوحيد الدولي للمعايير المتعلقة بسلامة وموثوقية التكنولوجيا وأطر الاعتراف المتبادل، وغير ذلك، من أجل إنشاء أعمال جديدة، وتعزيز التنمية الصناعية في مناخ صحي، وتعزيز القدرة التنافسية الدولية، بحيث يمكن للصناعات المتعلقة بالأمن السيبراني خلق فرص العمل.

تعزيز البحث والتطوير: يجب اتخاذ تدابير تتعلق بالأمن السيبراني، مثل تحسين أنظمة البحث، وتعزيز البحث الأساسي حول سلامة وموثوقية التكنولوجيا والبحث والتطوير للتكنولوجيات الأساسية، ورعاية الباحثين والمهندسين، وتعزيز التعاون بين معاهد الاختبار والبحث الوطنية والجامعات والقطاع الخاص، وتعزيز التعاون الدولي من أجل البحث والتطوير.

تأمين الموارد البشرية: عمل الدولة بشكل وثيق مع الجامعات والمعاهد التقنية والمدارس المهنية والشركات الخاصة وغيرها لاتخاذ التدابير اللازمة لضمان المعاملة المناسبة للعاملين في مجال الأمن

السيبراني، بحيث تكون واجباتهم وبيئات عملهم جذابة ومتناسبة مع أهمية العمل، وعمل الدولة أيضا مع الجهات التي سبق أن ذكرتها للاستفادة من أنظمة التأهيل وتدريب المهندسين الشباب واتخاذ التدابير الأخرى اللازمة لتأمين وتدريب وتحسين جودة الموارد البشرية المتعلقة بالأمن السيبراني.

في الجانب المتعلق بالعقوبات يبقى قانون الأمن السيبراني المغربي، هو الأكثر تفصيلا في تحديد الأفعال المخالفة للقانون والجزاءات بالإحالة على الغرامات دون الإخلال بالعقوبات الجنائية المنصوص عليها في التشريع الجاري به العمل، مقارنة بلوائح أعمال الأمن السيبراني كوريا الجنوبية، وبالتالي ليست لها قوة الالزام مثل القانون، وبالتبع لا يمكن إدراج العقوبات الجنائية.

أما قانون الأمن السيبراني الياباني، فقد جاء عاما وشاملا، بحيث شدد بالمادة 38 من الفصل الخامس المتعلق بالعقوبات بعقوبة الحبس مدة لا تزيد على سنة أو بغرامة لا تزيد على خمسمائة ألف ين كل من يخالف الفقرة 4 من المادة 17، التي تقول: *" لا يجوز لأي شخص كان أو كان يعمل في شؤون المجلس أن يفشي أو يسيء استخدام أي سر اطلع عليه فيما يتصل بالشؤون المذكورة دون سبب مبرر"*، والفقرة 2 من المادة 31: *" المادة 16-3 لا يجوز لموظف أو مستخدم في شركة أوكلت إليه أعمال بموجب أحكام الفقرة السابقة، أو لمن شغل مثل هذا المنصب، أن يفشي أو يسيء استعمال أي سر اطلع عليه فيما يتصل بالأعمال الموكلة إليه دون مبرر مقبول"*، ونقول بأن أغلب قوانين الأمن السيبراني قد لا تحدد كثيرا من الجزاءات، وتتكفل بذلك باقي القوانين المرتبطة بالرقمنة بصفة خاصة مثل قانون حماية البيانات الشخصية، وقوانين أخرى بصفة عامة مثل القانون الجنائي، وبالتالي لا حاجة للإعادة أو التكرار.

كجزء من الدفاع السيبراني النشط، تحصل الحكومة على معلومات الاتصالات المحلية والدولية حول الهجمات السيبرانية من الشركات من أجل الكشف عن مصدر الهجمات، بالتالي نوصي بفرض عقوبات على الأشخاص الذين يقومون بتسريب معلومات الاتصالات التي تم الحصول عليها ومشاركتها في عملية التعاون بين القطاعين العام والخاص لتحديد علامات الهجمات الإلكترونية، وسوف يؤدي هذا إلى إنشاء نظام يمكن للقطاعين العام والخاص من خلاله الحفاظ على السرية.

في خضم الهجمات الالكترونية التي توجب تقوية الجانب التقني قبل التشريعي، توالت التعديلات التشريعية في قانون الأمن السيبراني باليابان، وتخلت كوريا الجنوبية مؤخرا من جهتها عن حذرها ومخاوفها حول انتهاك الخصوصية، والمغرب الذي أمسك العصا من الوسط لديه قانون للأمن السيبراني إلا أنه لا يصل لما حققته اليابان بقانونها السيبراني، يبقى هناك خلاف فقهي هل يمكن القول بأن قانون الأمن السيبراني ينتمي إلى القانون العام كما في كوريا الجنوبية أم إلى القانون الخاص، أو حتى الجمع بين المصدرين؟

نتيجة اطلاعي على التوجه الفقهي بكوريا الجنوبية بخصوص ما سبق، رغم انحيازي الأولي بأن قانون الأمن السيبراني ينتمي لفئة القانون الخاص، أرجح ببعد نظر وشمولية للأوضاع المختلفة وطبيعة كل بلد في صياغة قانونها، بأن قانون الأمن السيبراني ينتمي لكلا المصدرين القانون العام والخاص معا، وقد ترجح الكفة على حسب طبيعة ومضمون القانون في كل بلد.

من هذا المنطلق نوصي بوضع مدونة للأمن السيبراني تضم جميع ما يربط بين القوانين الرقمية وقانون الأمن السيبراني خاصة منها المتعلقة بالعقوبات، لكن بعد نضوج القانون ووضع مبادئ واستراتيجية كتلك التي باليابان، وضبط عناصر هذا القانون ككل.

بناء على مبدأ ضمان التدفق الحر للمعلومات، ينبغي للقطاعين العام والخاص العمل معا للاستجابة بشكل استباقي لهذه القضية، كما يحتاج كل مواطن إلى تعميق وعيه بالأمن السيبراني، واتخاذ إجراءات تطوعية، وبناء نظام مرن، وكذلك بناء مجتمع اقتصادي نابض بالحياة من خلال تطوير شبكات المعلومات والاتصالات المتقدمة واستخدام تكنولوجيا المعلومات.

إضافة إلى لعب دور قيادي في تشكيل النظام الدولي فيما يتعلق بالأمن السيبراني وتنفيذه وفقا للتعاون الدولي، وعدم التعدي على حقوق المواطنين بشكل غير مبرر، يجب إقرار هاته المبادئ وعلى أساسها العمل على تنفيذ التدابير اللازمة.

على سبيل التوجه العام للتحول الرقمي الصناعي، وضعت كوريا الجنوبية قانون تعزيز التحول الرقمي الصناعي لتعزيز التحول الرقمي للصناعات الذي صدر في ديسمبر عام 2021، بناء على ما سبق نوصي بسن قانون تعزيز التحول الرقمي الصناعي لتعزيز التحول الرقمي للصناعات، من أجل إرساء الأساس لدعم استخدام المعلومات الصناعية بشكل شامل ومنهجي بالمغرب.

من جهة أخرى، تشكل التطبيقات الإلكترونية النافذة التي تقدم عبرها المؤسسات العامة خدماتها للمواطنين وتوفر الوقت والمال والجهد، في المقابل لا تفتر الهجمات السيبرانية أن تهدد مصالح المواطنين وتفقد الثقة بين المواطنين والمؤسسات العامة، ثم من منطلق المجال القانوني الذي يمثل سياجا من الرقابة والحماية عبر قانون 08-09 المتعلق بحماية الأشخاص الذاتيين اتجاه معالجة المعطيات ذات الطابع الشخصي، وباقي القوانين الموازية له مثل قانون حماية البيانات الشخصية بكوريا الجنوبية، بحيث تكون سياسة الخصوصية للتطبيقات مبنية على ذاك الأساس، إلا أنه من خلال اطلاعي على *موقع إدارتي وموقع رخص* المغربيين، لم أتحصل على سياسة خصوصية لهما، من هذا المنطلق نوصي بوضع سياسة خصوصية *لموقع إدارتي* على غرار أغلب المواقع للمؤسسات العامة بالمغرب بناء على قانون 08-09.

بالموازاة مع الاقتراح السابق وأثناء وضع إصلاحات *بموقع إدارتي* فكما أشرنا سابقا بأن استراتيجية المغرب الرقمي 2030 ترنو لوضع منصة موحدة للخدمات الإدارية، من هذا المنطلق أقترح النظر على *موقع حكومة 24* المتعلق بموقع يحتوي على حزمة من المنصات التي تقدم خدمات عامة للمواطنين بكوريا الجنوبية، خاصة وأن تجربة كوريا الجنوبية بهذا الصدد قد تصدرت المرتبة الأولى على الصعيد العالمي مرتين بشأن موقع *حكومة 24*، والاطلاع كذلك *على موقع رخص* على أساس وضع سياسة خصوصية له بناء على قانون 08-09 وباقي القوانين المغربية المتعلقة بالبناء والتعمير، على غرار سياسة الخصوصية لموقع نظام "*سوميتيو*" الذي جمع بين قانون حماية البيانات الشخصية وقوانين البناء والتعمير الخاصة بكوريا الجنوبية.

من وجهة نظري وأمام قانون حماية البيانات الشخصية بكوريا الجنوبية يبقى قانون 08-09 تكسوه بعض النواقص والعلل، أولها شكليا اسم القانون الطويل حبذا لو تم اختصاره بقانون حماية البيانات الشخصية، كما أن قانون حماية البيانات الشخصية الكوري يتميز على قانون 08-09 بالتفصيل في إنشاء سياسة حماية البيانات الشخصية ومعالجتها والإدارة الآمنة للمعلومات الشخصية إضافة إلى العقوبات، مع ضمان حقوق أصحاب البيانات، وكلها تم اختزالها في جموع قانون 08-09، وتجدر الإشارة إلى أن القانون الكوري يتميز بفصلين هما الفصل السابع الذي يضم تأطيرا للجنة الوساطة في نزاعات المعلومات الشخصية، من هذا المنطلق نوصي بإحداث نظام الوساطة في حل نزاعات المعلومات الشخصية بالمغرب على غرار كوريا الجنوبية وتأطيرها قانونيا عبر قانون 08-09، ثم الفصل الثامن بالقانون الكوري طبعا الذي يوضح كيفية رفع دعوى قضائية جماعية عند وقوع تسريب أو انتهاك للمعلومات الشخصية، نوصي بإضافة هاته الجزئية بقانون 08-09.

وجدير بالذكر بأنه خلال دراستي لموضوع الرسالة لاحظت الإطار التشريعي بكوريا الجنوبية للقوانين الرقمية ومسارها، سواء المرتبطة بالقانون العام أو القانون الخاص، من ديناميكية سريعة ومهولة في التعديل والتغيير والحذف في كل عام في عدة جزئيات، هو إيقاع متسارع وخفيف للقانون على خطى التكنولوجيا والرقمنة وتنظيمها، وحتى نسخ القانون بالكامل في بعض الأحيان، فهل يمكن أن نرى المشرع المغربي يعمل بالديناميكية السريعة التي تواكب التطور التكنولوجي في العالم، وبشكل مسؤول ومنضبط كما يعمل المشرع الكوري، في احترام تام لمبدأ الخصوصية، والأمن السيبراني؟

لائحة المراجع

لائحة المراجع (باللغة العربية)

الخطب الملكية

جلالة الملك يوجه رسالة إلى المشاركين في أشغال اجتماع التجمع الإفريقي لوزراء المالية ومحافظي البنوك المركزية للدول الأفريقية، الأعضاء في البنك وصندوق النقد الدوليين بتاريخ 5 يوليوز 2022.

نص الخطاب الملكي السامي الذي ألقاه صاحب الجلالة الملك محمد السادس في افتتاح الدورة الأولى من السنة التشريعية الأولى من الولاية التشريعية العاشرة بالرباط بتاريخ 14 أكتوبر 2016.

صفحات الويب (باللغة العربية)

الظهائر

ظهير شريف رقم 1-93-51 صادر في 22 من ربيع الأول 1414 (10 سبتمبر 1993) معتبر بمثابة قانون يتعلق بإحداث الوكالات الحضرية، على الرابط التالي: https://2u.pw/d7D6Kr6j

بلاغات الديوان الملكي

بلاغ للديوان الملكي، الثلاثاء 17 أكتوبر 2023، وزارة إعداد التراب الوطني والتعمير والإسكان وسياسة المدينة: https://2u.pw/fVumLpxy.

المراسيم

مرسوم رقم 2.97.361 صادر في 27 من جمادى الآخرة 1418 (30 أكتوبر 1997) يتعلق بالوكالات الحضرية للعيون ومكناس وتطوان ووجدة وآسفي-الجديدة والقنيطرة – سيدي قاسم وسطات وتازة، على الرابط التالي: https://2u.pw/qHay0GJR.

نشر المرسوم رقم 2.24.921 المتعلق بلجوء الهيئات والبنيات التحتية ذات الأهمية الحيوية المتوفرة على نظم معلومات حساسة أو معطيات حساسة إلى مقدمي الخدمات الرقمية السحابية بالجريدة الرسمية، على الموقع التالي: https://n9.cl/smruv.

القوانين

القانون رقم 20-43 المتعلق بخدمات الثقة بشأن المعاملات الإلكترونية، موقع المديرية العامة لأمن نظم المعلومات إدارة الدفاع الوطني المملكة المغربية: https://n9.cl/sxltg0 .

القانون رقم 31.13 المتعلق بالحق في الوصول إلى المعلومات، على موقع acaps: https://n9.cl/fcafc.

القانون رقم 20-05 المتعلق بالأمن السيبراني، على الموقع الرسمي المديرية العامة لأمن نظم المعلومات: https://n9.cl/5skuo .

مشروع قانون

مذكرة تقديمية لمشروع القانون رقم ... يتعلق بإحداث الوكالات الجهوية للتعمير والإسكان، المملكة المغربية وزارة إعداد التراب الوطني والتعمير والإسكان وسياسة المدينة الوزيرة، نسخة منشورة على صفحة الأستاذ كريم لملوج موثق في مراكش على موقع لينكدن: https://2u.pw/Cwas501Q.

المواقع الرسمية

الإدارة الرقمية، موقع رئيس الحكومة، وزارة الانتقال الرقمي وإصلاح الإدارة: https://n9.cl/j2are.

إدارتي: https://idarati.ma/ .

البوابة الوطنية للشكايات: https://h1.nu/165kx .

راجع رسم خرائط استخدام تكنولوجيا المعلومات والاتصالات في القطاعات العامة www.mmsp.gov.ma.

رخص: https://rokhas.ma/.

رئاسة النيابة العامة: https://plaintes.pmp.ma/.

مؤسسة وسيط المملكة: https://www.mediateur.ma/ar.

الوكالة الوطنية الوكالة الوطنية لتقنين المواصلات (ANRT)، على موقعها الرسمي: https://www.anrt.ma/ar/a-propos/presentation?csrt=17500348124919813617 .

الموارد السمعية البصرية

الذكاء الاصطناعي بالمغرب .. السغروشني تعلن إطلاق خمس مبادرات، Medi1News، 2025/05/20، YouTube: https://n9.cl/zk59y .

العرض الرسمي للإستراتيجية الوطنية المغرب الرقمي 2030 (التغطية الكاملة)، Transition Numérique et Réforme de l'Administration (Ministère_TNRA)، على تطبيق يوتيوب YoutYoub: https://www.youtube.com/watch?v=gma9OzisnxA .

الدراسات

هند الإدريسي، الأمن السيبراني في المغرب" بين الإنجازات والتحديات، 2025/04/15، المعهد المغربي لتحليل السياسات: https://mipa.institute/?p=11681&lang=ar .

المقالات العلمية

أمينة أعتاب، الإطار القانوني لحماية المعطيات الشخصية كمدخل لتنمية الإدارة الرقمية بالمغرب، مجلة النداء التربوي، منشور بتاريخ 27-12-2022، إصدار عدد مزدوج 29-30 (2022)، قسم دراسات وأبحاث، على الموقع الالكتروني لمجلة النداء التربوي:https://goo.su/XIT9ZY .

محمد القاسمي، قراءة في قانون 05.20 المتعلق بالأمن السيبراني، منشورات موقع الباحث القانوني، موقع مجلة الباحث للدراسات والأبحاث: https://www.allbahit.com/2021/05/0520.html .

التقارير

الاستراتيجية الوطنية "المغرب الرقمي 2030"، كتيب مؤسساتي، المغرب الرقمي DIGITAL MOROCCO 2030، وزارة الانتقال الرقمي وإصلاح الإدارة، موقع رئيس الحكومة، وزارة الانتقال الرقمي وإصلاح الإدارة، المملكة المغربية: https://h1.nu/11Uok.

تقرير المجلس الإداري للوكالة الحضرية لتطوان، الدورة التاسعة عشر-2023، الوكالة الحضرية لتطوان، وزارة إعداد التراب الوطني والتعمير والإسكان وسياسة المدينة، ص: 14-15، على الرابط التالي:https://goo.su/dOaROu .

التكنولوجيا السحابية(cloud)، رافعة استعجالية لتسريع التحول الرقمي، رأي المجلس الاقتصادي والاجتماعي والبيئي، إحالة ذاتية رقم 2023/71، المجلس الاقتصادي والاجتماعي والبيئي، على الرابط التالي: https://h1.nu/165kA .

الذكاء الاصطناعي بالمغرب: أي استخدامات وأي آفاق للتطوير؟، رأي المجلس الاقتصادي والاجتماعي والبيئي، إحالة ذاتية رقم 2024/78، المجلس الاقتصادي والاجتماعي والبيئي، على الرابط التالي:https://goo.su/Mpx39kE .

مهام الوكالات الحضرية، موقع الكتروني لفدرالية الوكالات الحضرية بالمغرب، على الرابط التالي: https://www.federation-majal.ma/ar/Missions .

البلاغات الصحفية الرسمية

بلاغ صحفي تفعيل الإدارة الرقمية والتدبير اللامادي من أهم الإجراءات المعتمدة من طرف الوكالة الحضرية لتطوان لضمان استمرارية خدماتها في ظل الأزمة الصحية الاستثنائية الناتجة عن وباء كورونا (كوفيد19)، متوفر على الرابط التالي: https://autetouan.ma/web/uploads/dossier/5e984c4fc8131.pdf .

المقالات الصحفية

أنفاس بريس، هذه هي استراتيجية المديرية العامة للأمن الوطني في محاربة الجرائم الإلكترونية، تاريخ النشر: 10 نوفمبر 2019، على موقع أنفاس بريس: https://2cm.es/1a6fu .

أهمية مؤسسة الوسيط وكيفية تقديم الشكاوى إليها، على الرابط: https://n9.cl/wsvvh .

جمال أزضوض، هل تتيح "استراتيجية المغرب الرقمي" بناء اقتصاد إلكتروني تنافسي؟، مقال صحفي، الثلاثاء 4 مارس 2025 - 03:00، موقع هسبريس: https://2u.pw/QIxcC .

حميد بحكاك، المغرب والتحول الرقمي، الإطار التشريعي والمؤسساتي والاستراتيجي، تاريخ النشر: 20 سبتمبر 2024 - 13:00، موقع حزب العدالة والتنمية:https://n9.cl/0atfwz .

حميد بحكاك، حميد بحكاك يكتب: المغرب والأمن السيبراني الإطار التشريعي والمؤسساتي والاستراتيجي، تاريخ النشر: 17 أكتوبر 2024 - 0:00، موقع حزب العدالة والتنمية: https://n9.cl/uaq7b .

الحوسبة السحابية رافعة مستعجلة لتسريع التحول الرقمي، على موقع مرصد التحول الرقمي: https://n9.cl/p0une .

سلمى درداف، خبير يُعدّد أسباب اختراق مواقع مغربية ويؤكد أن الهجمات "حرب سيبرانية"، النشر بتاريخ 9 أبريل 2025 - 14:00، على موقع مدار 24: https://madar21.com/334204.html.

عدنان مصطفى البار، أمن المعلومات والأمن السيبراني، ص: 8، مقال منشور بالموقع الإلكتروني: www.kau.edu.sa .

عزيز أخنوش، تفعيل استراتيجية "المغرب الرقمي 2030" رافعة أساسية لخارطة الطريق الحكومية للنهوض بالتشغيل، 25 سبتمبر 2024، موقع وكالة المغرب العربي للأنباء: https://2u.pw/U4eAn .

عماد السعيدي، المغرب يطلق مركزا وطنيا للابتكار في الأمن السيبراني لتعزيز البحث والتطوير الرقمي، تاريخ النشر: 04 يونيو 2025، على موقع DETA FOUR العربية: https://detafour.com/%D8%A7%D9%84%D9%85%D8%BA%D8%B1%D8%A8-%D9%8A%D8%B7%D9%84%D9%82-%D9%85%D8%B1%D9%83%D8%B2%D8%A7-%D9%88%D8%B7%D9%86%D9%8A%D8%A7-%D9%84%D9%84%D8%A7%D8%A8%D8%AA%D9%83%D8%A7%D8%B1-%D9%81%D9%8A/ .

مجلس الحكومة يصادق على مشروع قانون إحداث الوكالات الجهوية للتعمير والإسكان، تاريخ النشر: 2025/06/26، على موقع SNRTNEWS: https://snrtnews.com/article/129265.

المديرية العامة للأمن الوطني تطلق المنصة الرقمية "إبلاغ" المخصصة للتبليغ عن المحتويات غير المشروعة على الأنترنيت، 26 يونيو 2024، المديرية العامة للأمن الوطني: https://n9.cl/ovecj .

المغرب الرقمي 2030... استراتيجية إلكترونية هذه أبرز تفاصيلها، مقال صحفي، الرباط – العربي الجديد، 30 سبتمبر 2024، موقع العربي الجديد: https://2u.pw/pXpX3 .

المهدي الزوات، الفشل في حماية البيانات الشخصية: أي مسلك قانوني للمتضررين، تاريخ النشر 9 أبريل 2025 - 22:11، على موقع مدار 21: https://madar21.com/334316.html.

وديع المودن، الهجوم السيبراني على صندوق الضمان الاجتماعي: لا يمكن استبعاد عقوبات إدارية وجنائية، النشر بتاريخ 2025/04/11 على الساعة 18:09، على موقع le 360: https://h1.nu/11Uo5.

يونس أباعلي ومحمد شافعي، "أخنوش يوضح أهداف الاستراتيجية الوطنية للتحول الرقمي"، على موقع SNRT NEWS: https://snrtnews.com/article/103530.

مدونة

دور السلطات المغربية في مكافحة الابتزاز الإلكتروني في المغرب، على موقع مكتب محاماة تهوم والصغير في الدار البيضاء: https://ar.thoumetsghair.com/%D8%A7%D9%84%D8%A7%D8%A8%D8%AA%D8%B2%D8%A7%D8%B2-%D8%A7%D9%84%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A/ .

قائمة المراجع (باللغة الفرنسية)Une bibliographie

التقاريرRapports

Bilan, diagnostic et plan d'amélioration de l'infrastructure systèmes, réseaux, SGBD et messagerie. Phase 1 : Analyse et évaluation de l'existant et identification des axes stratégiques. ETUDE D'ELABORATION DU SCHEMA DIRECTEUR DU SYSTEME D'INFORMATION 2020-2024 DE L'AGENCE URBAINE DE TETOUAN. AGENCE URBAINE DE TETOUAN. Ministère de l'Aménagement du Territoire National, de l'Urbanisme, de l'Habitat et de la Politique de la Ville. Royaume du Maroc. Etude d'élaboration du Schéma Directeur des Systèmes d'Information 2020-2024 pour Urbaine de Tétouan. IL Consultant. Réf. : AUTE-SDSI-P1-BDPA.

Plan d'Assurance Qualité. Phase 1 : Analyse et évaluation de l'existant et identification des axes stratégiques. ETUDE D'ELABORATION DU SCHEMA DIRECTEUR DU SYSTEME D'INFORMATION 2020-2024 DE L'AGENCE URBAINE DE TETOUAN. AGENCE URBAINE DE TETOUAN. Ministère de l'Aménagement du Territoire National, de l'Urbanisme, de l'Habitat et de la Politique de la Ville. Royaume du Maroc.

Plan d'urbanisation fonctionnel du futur Sl. Phase 2 : Elaboration des plans d'urbanisation du futur Sl et des scénarios de mise en œuvre. ETUDE D'ELABORATION DU SCHEMA DIRECTEUR DU SYSTEME D'INFORMATION 2020-2024 DE L'AGENCE URBAINE DE TETOUAN. AGENCE URBAINE DE TETOUAN.

Ministère de l'Aménagement du Territoire National, de l'Urbanisme, de l'Habitat et de la Politique de la Ville. Royaume du Maroc.

Plan d'urbanisation technique du futur Sl. Phase 2 : Elaboration des plans d'urbanisation du futur Sl et des scénarios de mise en œuvre. ETUDE D'ELABORATION DU SCHEMA DIRECTEUR DU SYSTEME D'INFORMATION 2020-2024 DE L'AGENCE URBAINE DE TETOUAN. AGENCE URBAINE DE TETOUAN. Ministère de l'Aménagement du Territoire National, de l'Urbanisme, de l'Habitat et de la Politique de la Ville. Royaume du Maroc.

Rapport d'analyse et d'évaluation de l'existant et des besoins. Phase 1 : Analyse et évaluation de l'existant et identification des axes stratégiques. ETUDE D'ELABORATION DU SCHEMA DIRECTEUR DU SYSTEME D'INFORMATION 2020-2024 DE L'AGENCE URBAINE DE TETOUAN. AGENCE URBAINE DE TETOUAN. Ministère de l'Aménagement du Territoire National, de l'Urbanisme, de l'Habitat et de la Politique de la Ville. Royaume du Maroc.

Rapport de l'étude de conformité à la Directive Nationale de Sécurité des Systèmes d'Information (DNSSI). Phase 1 : Analyse et évaluation de l'existant et identification des axes stratégiques. ETUDE D'ELABORATION DU SCHEMA DIRECTEUR DU SYSTEME D'INFORMATION 2020-2024 DE L'AGENCE URBAINE DE TETOUAN. AGENCE URBAINE DE TETOUAN. Ministère de l'Aménagement du Territoire National, de l'Urbanisme, de l'Habitat et de la Politique de la Ville. Royaume du Maroc.

Scénarii de mise en œuvre. Phase 2 : Elaboration des plans d'urbanisation du futur Sl et des scénarios de mise en œuvre. ETUDE D'ELABORATION DU SCHEMA DIRECTEUR DU SYSTEME D'INFORMATION 2020-2024 DE L'AGENCE URBAINE DE TETOUAN. AGENCE URBAINE DE TETOUAN. Ministère de l'Aménagement du Territoire National, de l'Urbanisme, de l'Habitat et de la Politique de la Ville. Royaume du Maroc.

Sites Web officiels مواقع رسمية

AGENCE URBAINE DE TÉTOUAN ,PRÉSENTATION, QUI SOMMES NOUS ?: https://aute.gov.ma/presentation/01/.

CNDP : https://goo.su/vpMjVM .

Le Centre Marocain de Recherches Polytechniques et d'Innovation (CMRPI) : https://www.cmrpi.ma/cmrpi-v2/presentation-du-cmrpi/.

Rokhas, YouTube: https://www.youtube.com/rokhas.

المراجع (باللغة الكورية) [참고문헌]

المقالات في المجلات القانونية 정기간행

بارك سانج دون، "دراسة في القانون العام حول تحسين حوكمة الأمن السيبراني"، مجلة القانون العام، المجلد 17، العدد 4 (الجمعية الكورية للقانون العام المقارن، 2016).

البحث الأساسي حول سن قانون حماية شبكة المعلومات والاتصالات (أبحاث السياسات 00-12) (معهد أبحاث سياسات المعلومات والاتصالات، 2000).

جونغ جون هيون، "مراجعة لقانون الأمن السيبراني الوطني في مجتمع المعلومات المتقدمة"، مجلة دراسات القانون، المجلد 37، العدد 2 (معهد أبحاث القانون بجامعة دانكوك، 2013).

عروض المؤتمرات 컨퍼런스

بارك هي وون، دراسة حالة حول تطبيق إطار عمل Agile القائم على التعلم في مشاريع تكنولوجيا المعلومات واسعة النطاق، وقائع مؤتمر الكمبيوتر الكوري، 2016.

أطروحات (الدكتوراه) 학위논문

بارك سانج دون، "دراسة حول المسؤولية الوطنية عن البنية التحتية للمعلومات والاتصالات"، أطروحة دكتوراه، جامعة سونغ كيون كوان، 2016.

الوسائط الإلكترونية 전자매체

كتاب (إلكتروني) 도서

كيم جاي كوانج، الاعتبارات الإدارية والقانونية لقانون الأمن السيبراني الوطني، تاريخ التقديم: 2019/08/10، تاريخ المراجعة وتأكيد النشر: 2019/08/31، على الرابط التالي: http://itnlaw.knu.ac.kr/?task=json&cmd=board-file-download&fid=237&filename=7.%EA%B9%80%EC%9E%AC%EA%B4%91.pdf .

أطروحات (الدكتوراه)학위논문

هونغ سوك هان، "دراسة حول التنظيم الذاتي المنظم وفقا لتغيرات دور الدولة - مع التركيز على مجال حماية المعلومات الشخصية-"، أطروحة دكتوراه، جامعة سونغ كيون كوان، 2008، ص 74، على موقع مكتبة الجمعية الوطنية الكورية: https://docviewer.nanet.go.kr/reader/viewer .

المقالات القانونية الإلكترونية 정기간행물

بارك إن-سو، "الدستور والأمن السيبراني"، "دراسات قانون وسياسة الأمن السيبراني"، المجلد 3 (جمعية قانون وسياسة الأمن السيبراني الكورية، أبريل 2018)، على الرابط التالي: http://www.kcsa2012.or.kr/wp-content/uploads/2019/01/3rd.pdf .

بارك سانغ دون، "دراسة حول قانون الأمن السيبراني الأساسي في اليابان: التركيز على آثار إعادة تنظيم نظام قانون الأمن السيبراني في كوريا"، مجلة كيونغهي للقانون، المجلد 50، العدد 2 (معهد أبحاث القانون بجامعة كيونغهي، 2015)، على موقع kci: https://www.kci.go.kr/kciportal/ci/sereArticleSearch/ciSereArtiView.kci?sereArticleSearchBean.artiId=ART002003738 .

بانغ سوك-هو، "خصائص القانون الأساسي للذكاء الاصطناعي، والتحديات التشريعية المستقبلية، وتداعياتها على الشركات"، تاريخ النشر: 14 يناير 2025، على موقع صحيفة قانونية 75 -المجلة الوحيدة للمهنة القانونية التي تأسست عام 1950: https://www.lawtimes.co.kr/LawFirm-NewsLetter/204689 .

جونغ تاي جين، "دراسة حول أنظمة الاستجابة للأمن السيبراني في الدول الكبرى"، مجلة قانون وسياسة الأمن السيبراني، المجلد 2 (الجمعية الكورية لقانون وسياسة الأمن السيبراني، ديسمبر 2016)، على الرابط التالي: http://www.kcsa2012.or.kr/wp-content/uploads/2019/01/2nd.pdf?ckattempt=1 .

جونغ مي-آي وآخرون، التغيرات في أنشطة الابتكار المؤسسي واستراتيجيات الاستجابة في عصر التحول الرقمي، أبحاث سياسات STEPI 7-2021، مجلة STEPI، تاريخ النشر: 30 ديسمبر 2012، على موقع STEPI: https://www.stepi.re.kr/site/stepiko/report/View.do?cbIdx=1292&reIdx=996&cateCont=A0201 .

كيم جاي كوانغ وكيم جونغ إيم، " الوضع الحالي وآفاق التشريعات المتعلقة بالجرائم الإلكترونية في اليابان"، مجلة دراسات القانون، المجلد 33، العدد 1 (معهد أبحاث القانون بجامعة دانكوك، يونيو/حزيران 2009)، على موقع kci: https://www.kci.go.kr/kciportal/ci/sereArticleSearch/ciSereArtiView.kci?sereArticleSearchBean.artiId=ART001362217 .

لي تشانج بوم، دور الأمن السيبراني في نجاح الحكومة 3.0، مجلة قانون وسياسة الأمن السيبراني، المجلة الكورية لقانون الأمن السيبراني، العدد 2، 2016، على الرابط التالي: http://www.kcsa2012.or.kr/wp-content/uploads/2019/01/2nd.pdf?ckattempt=1 .

لي سونغ يوب، "ضرورة واعتبارات سن قانون الأمن السيبراني الوطني استجابةً للتهديدات السيبرانية"، مجلة سياسة قانون الأمن السيبراني، المجلد 2 (رابطة سياسة قانون الأمن السيبراني الكورية، ديسمبر 2016)، على الرابط التالي: http://www.kcsa2012.or.kr/wp-content/uploads/2019/01/2nd.pdf?ckattempt=1 .

هونغ سيونغ مان، "استكشاف مجتمع المخاطر والعلنية: التركيز على حالات تسرب الماء والإشعاعات"، مجلة دراسات السياسة الكورية، المجلد 13، العدد 2 (جمعية الإدارة العامة في كيونغين، 2013)، على موقع (GIAPA): https://giapa.or.kr/journal_article/%EC%9C%84%ED%97%98%EC%82%AC%ED%9A%8C%EC%99%80-%EA%B3%B5%EA%B3%B5%EC%84%B1-/%ED%83%90%EC%83%89 .

공적 보고서 (على الإنترنت) التقارير العامة

اتجاه تقديم الذكاء الاصطناعي واسع النطاق في القطاع العام استنادا إلى نموذج اللغة واسع النطاق، استراتيجية تكنولوجيا المعلومات والمستقبل، العدد 3، وكالة مجتمع المعلومات الاستخباراتية الكورية، تاريخ النشر: 2023/04/07، على موقع وكالة مجتمع المعلومات الاستخباراتية الكورية NIA: https://www.nia.or.kr/site/nia_kor/ex/bbs/View.do?cbIdx=25932&bcIdx=25490&parentSeq=25490 .

بارك تاي-غيون، إرشادات التوزيع والاستخدام لواجهة المستخدم وتجربة المستخدم لمواقع الحكومة الإلكترونية، غرفة بيانات معايير وإرشادات المعلومات، تاريخ النشر: 21 مارس 2019، على الموقع الرسمي لوزارة الداخلية والأمن بكوريا الجنوبية: https://www.mois.go.kr/frt/bbs/type001/commonSelectBoardArticle.do?bbsId=BBSMSTR_000000000045&nttId=69451 .

تقرير مراجعة لجنة الاستخبارات في الجمعية الوطنية، على الموقع الرسمي لافتتاح الجمعية الوطنية بكوريا الجنوبية: https://watch.peoplepower21.org/index.php?mid=Committee&sangim=%EC%A0%95%EB%B3%B4#watch .

الخطة الأساسية الثالثة للحوسبة السحابية (ما بين عامي 2022-2024)، لجنة استراتيجية المعلومات والاتصالات، تاريخ النشر: شهر 9 سنة 2021، على الرابط التالي: file:///C:/Users/pc/Downloads/R2109209-1.pdf .

سون سونغ هيون وآخرون، تقرير حول مشكلة توحيد معايير المنصات الرقمية الحكومية، جمعية تكنولوجيا المعلومات والاتصالات الكورية، نظام إدارة أداء البحث والتطوير لمعايير تكنولوجيا المعلومات والاتصالات"، تاريخ النشر 2023، على الرابط التالي: file:///C:/Users/pc/Downloads/%EB%94%94%EC%A7%80%ED%84%B8%ED%94%8C%EB%9E%AB%ED%8F%BC%EC%A0%95%EB%B6%80%ED%91%9C%EC%A4%80%ED%99%94%EC%9D%B4%EC%8A%88%EB%B3%B4%EA%B3%A0%EC%84%9C%20(2).pdf.

كيم جاي كوانج، "الاستراتيجية التشريعية استجابة للتغيرات في البيئة التشريعية للأمن السيبراني"، مجلة قانون وسياسة الأمن السيبراني، المجلة الكورية لقانون الأمن السيبراني، العدد 2، 2016، على الرابط التالي: http://www.kcsa2012.or.kr/wp-content/uploads/2019/01/2nd.pdf

لي جاي دو، معايير المرجع ومواقع البيانات في سياسة البيانات الوطنية، تاريخ النشر: 2022.10، على الرابط التالي: https://h1.nu/10hnW .

البيانات الصحفية الصادرة عن المؤسسات العامة 공공기관 보도자료

يساهم إطلاق خدمة بياناتي العامة في ابتكار جديد في الحكومة الرقمية، بيان صحفي لوزارة الإدارة العامة والأمن، العدد الصباحي 210225، قسم توزيع البيانات العامة، وزارة الإدارة العامة والأمن -كوريا الجنوبية، 2021، على موقع KDI: https://eiec.kdi.re.kr/policy/materialView.do?num=210954&topic=&pp=20 =&datecount=&recommend=&pg .

مقالات صحفية (إلكترونية) 신문기사

بارك هيون سون، أعلنت شركة جارتنر عن أهم 12 اتجاها استراتيجيا للتكنولوجيا لعام 2022، تاريخ النشر: 2021/10/22، على موقع NextDaily: https://www.nextdaily.co.kr/news/articleView.html?idxno=200342.

جو جي وان، 2025، المؤسسات المالية تشارك أيضا في "منع الوصول إلى DeepSec، تاريخ النشر: 6 فبراير 2025، على موقع هانكيوريه: https://www.hani.co.kr/arti/economy/economy_general/1181020.html.

كيم سون-آي، هجوم سلسلة التوريد 1: أضرار جسيمة ناجمة عن هجمات سلسلة التوريد، تاريخ النشر: 2021/11/01، على موقع NetworkTIMS: https://www.datanet.co.kr/news/articleView.html?idxno=165985 .

لجنة العلوم والدفاع في الجمعية الوطنية تقر مشروع قانون الذكاء الاصطناعي الأساسي، تاريخ النشر: 04 ديسمبر 2024، النشرة الإخبارية، باللغة الكورية على موقع KIM & CHANG: https://www.kimchang.com/ko/insights/detail.kc?sch_section=4&idx=30837 .

لي سانغ سيو، أوقفت لجنة حماية المعلومات الشخصية (PIPC) الخدمة المحلية الجديدة لشركة DeepSeak، مشيرة إلى سياسة معلومات شخصية غير كافية، تاريخ النشر: 17 فبراير 2025، على موقع وكالة يونهاب للأنباء: https://www.yna.co.kr/view/AKR20250217066600530.

مدونة (على الإنترنت) 블로그

DevOps ، على موقع ويكيبيديا: https://ko.wikipedia.org/wiki/devops .

جارتنر تعلن عن "12 اتجاها للتكنولوجيا الحكومية لعام 2022"، على موقع brunch story: https://brunch.co.kr/@choimeal/10.

لي سانغ مين، حادثة شلل الحاسوب في الشبكة الإدارية الوطنية لعام 2023، آخر تعديل:2025/05/08، على موقع Namu: https://namu.wiki/w/2023%EB%85%84%20%EA%B5%AD%EA%B0%80%ED%96%89%EC%A0%95%EB%A7%9D%20%EC%A0%84%EC%82%B0%EB%A7%88%EB%B9%84%20%EC%82%AC%ED%83%9C#fn-8.

مشكلة حظر Deepseek: مرحلة جديدة في سباق الذكاء الاصطناعي العالمي، تاريخ النشر: 1 فبراير 2025، على موقع Blog: https://inblog.ai/ringo/deepseek-blockade-issue .

공식 웹사이트 مواقع إلكترونية رسمية

موقع (Seumteo): https://www.eais.go.kr/moct/awp/aha01/AWPAHA01V01 .

موقع حكومة 24: https://www.gov.kr/portal/main/nologin .

موقع وكالة الإنترنت والأمن الكورية KISA: https://isms.kisa.or.kr/main/csap/intro/ .

법률 القانون (على الإنترنت)

قانون تعزيز الحوسبة السحابية وحماية المستخدمين (المختصر باسم قانون الحوسبة السحابية)، [دخل حيز التنفيذ في 31 يناير 2025] [القانون رقم 20732، 31 يناير 2025، المعدل جزئيا]، على موقع المركز الوطني للمعلومات القانونية بوزارة التشريع الحكومي، موقع رسمي للحكومة الإلكترونية لجمهورية كوريا الجنوبية: https://www.law.go.kr/lsInfoP.do?lsId=012266&ancYnChk=0#0000 .

إشعار تشريعي بشأن مشروع القانون الأساسي للأمن السيبراني الوطني، إشعار جهاز المخابرات الوطني رقم 2022-5، بتاريخ : 8 نوفمبر 2022، على موقع وزارة التشريع الحكومي: https://www.moleg.go.kr/lawinfo/makingInfo.mo?lawSeq=70698&lawCd=0&&lawType=TYPE5&mid=a10104010000 .

بارك جيون سيونج وكيم جاي جوانج، قانون إدارة الشرطة (الطبعة الثالثة)، (بارك يونغ سا، 2016)، متوفر باللغة الكورية على مكتبة المحكمة: https://e-

book.scourt.go.kr/contents/category?type=FOREIGN&lcate=001&mcate=003 .

قانون حماية البنية التحتية للمعلومات والاتصالات [تاريخ النفاذ: 24 يناير 2025] [القانون رقم 20068، 23 يناير 2024، تعديل جزئي]، على موقع المركز الوطني للمعلومات القانونية بوزارة التشريع الحكومي، موقع رسمي للحكومة الإلكترونية لجمهورية كوريا الجنوبية: https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%A0%95%EB%B3%B4%ED%86%B5%EC%8B%A0%EA%B8%B0%EB%B0%98%EB%B3%B4%ED%98%B8%EB%B2%95.

القانون الجنائي [تاريخ التنفيذ: 8 أبريل 2025] [القانون رقم 20908، 8 أبريل 2025، معدل جزئيا]، على موقع المركز الوطني للمعلومات القانونية بوزارة التشريع الحكومي، موقع رسمي للحكومة الإلكترونية لجمهورية كوريا الجنوبية: https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%ED%98%95%EB%B2%95 .

قانون معالجة الشكاوى المدنية (اختصار: قانون معالجة الشكاوى المدنية) [دخل حيز التنفيذ في 12 يوليو 2022] [القانون رقم 18748، 11 يناير 2022، تعديل لقوانين أخرى]، على موقع المركز الوطني للمعلومات القانونية بوزارة التشريع الحكومي، موقع رسمي للحكومة الإلكترونية لجمهورية كوريا الجنوبية: https://www.law.go.kr/LSW/lsInfoP.do?lsiSeq=239293#0000 .

القانون الأساسي بشأن المعلومات الذكية، [تاريخ النفاذ: 27 مارس 2025] [القانون رقم 20410، 26 مارس 2024، التعديل الجزئي]، على موقع المركز الوطني للمعلومات القانونية بوزارة التشريع الحكومي، موقع رسمي للحكومة الإلكترونية لجمهورية كوريا الجنوبية: https://www.law.go.kr/lsInfoP.do?lsId=000028&ancYnChk=0#0000 .

قانون الحكومة الإلكترونية [تاريخ النفاذ: 16 مايو 2023] [القانون رقم 19030، 15 نوفمبر 2022، معدل جزئيا]، على موقع المركز الوطني للمعلومات القانونية بوزارة التشريع الحكومي، موقع رسمي للحكومة الإلكترونية لجمهورية كوريا الجنوبية: https://www.law.go.kr/LSW/lsInfoP.do?lsiSeq=245293#0000 .

قانون تسجيل المقيمين [تاريخ التنفيذ: 27 ديسمبر 2024] [القانون رقم 19841، 26 ديسمبر 2023، التعديل الجزئي]، على موقع المركز الوطني للمعلومات القانونية بوزارة التشريع الحكومي،

موقع رسمي للحكومة الإلكترونية لجمهورية كوريا الجنوبية: https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%A3%BC%EB%AF%BC%EB%93%B1%EB%A1%9D%EB%B2%95 .

لوائح عمل الأمن السيبراني [تاريخ التنفيذ: 1 يناير 2025] [المرسوم الرئاسي رقم 34287، 5 مارس 2024، منقح جزئيا]، على موقع المركز الوطني للمعلومات القانونية بوزارة التشريع الحكومي، موقع رسمي للحكومة الإلكترونية لجمهورية كوريا الجنوبية: https://www.law.go.kr/LSW//lsInfoP.do?lsiSeq=261003&efYd=&ancYnChk=undefined#0000 .

قانون حماية المعلومات الشخصية، [تاريخ التنفيذ: 13 مارس 2025] [القانون رقم 19234، 14 مارس 2023، التعديل الجزئي]، على موقع المركز الوطني للمعلومات القانونية بوزارة التشريع الحكومي، موقع رسمي للحكومة الإلكترونية لجمهورية كوريا الجنوبية: https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EA%B0%9C%EC%9D%B8%EC%A0%95%EB%B3%B4%EB%B3%B4%ED%98%B8%EB%B2%95

قانون حماية المعلومات الشخصية، [تاريخ التنفيذ: 13 مارس 2025] [القانون رقم 19234، 14 مارس 2023، مراجع جزئيا]، على موقع المركز الوطني للمعلومات القانونية بوزارة التشريع الحكومي، موقع رسمي للحكومة الإلكترونية لجمهورية كوريا الجنوبية: https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EA%B0%9C%EC%9D%B8%EC%A0%95%EB%B3%B4%EB%B3%B4%ED%98%B8%EB%B2%95

قانون الإطار بشأن المعلومات الذكية، [تاريخ التنفيذ: 22 يناير 2026] [القانون رقم 20672، 21 يناير 2025، تعديل لقوانين أخرى]، وزارة العلوم وتكنولوجيا المعلومات والاتصالات (قسم إدارة سياسة المعلومات والاتصالات)، 044-202-6124، 6119، على موقع المركز الوطني للمعلومات القانونية بوزارة التشريع الحكومي، موقع رسمي للحكومة الإلكترونية لجمهورية كوريا الجنوبية: https://www.law.go.kr/LSW//lsEfInfoP.do?lsiSeq=268535# .

مرسوم رئاسي 대통령령

مرسوم تنفيذ قانون حماية البيانات الشخصية [المرسوم الرئاسي رقم 35343، 25 فبراير 2025، منقح جزئيا]، على موقع المركز الوطني للمعلومات القانونية بوزارة التشريع الحكومي، موقع رسمي للحكومة الإلكترونية لجمهورية كوريا الجنوبية: https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EA%B0%9C%EC%9D%B8%EC%A0%95%EB%B3%B4%EB%B3%B4%ED%98%B8%EB%B2%95%EC%8B%9C%ED%96%89%EB%A0%B9 .

المقررات القضائية (على الإنترنت) 사법적 결정

التفسير الرسمي لوزارة التشريعات الحكومية، [وزارة التشريعات الحكومية 21-0889، 26 أبريل 2022، وزارة الداخلية والأمن]، على موقع CaseNote: https://casenote.kr/%EB%B2%95%EB%A0%B9/%EA%B0%9C%EC%9D%B8%EC%A0%95%EB%B3%B4_%EB%B3%B4%ED%98%B8%EB%B2%95/%EC%A0%9C18%EC%A1%B0 .

التفسير الرسمي لوزارة التشريعات الحكومية، [وزارة التشريعات الحكومية 21-0889، 26 أبريل 2022، وزارة الداخلية والأمن]، على موقع CaseNote: https://casenote.kr/%EB%B2%95%EB%A0%B9/%EA%B0%9C%EC%9D%B8%EC%A0%95%EB%B3%B4_%EB%B3%B4%ED%98%B8%EB%B2%95/%EC%A0%9C18%EC%A1%B0 .

التفسير الرسمي لوزارة التشريعات الحكومية، رقم 19-0314، بتاريخ: 17 سبتمبر 2019، [المشتكي - نطاق المعلومات الحساسة المحظور معالجتها من قبل معالجي المعلومات الشخصية (بخصوص المادة 23 من قانون حماية المعلومات الشخصية)، على موقع CaseNote: https://casenote.kr/%EB%B2%95%EC%A0%9C%EC%B2%98/19-0314-674d2d .

التفسير الرسمي لوزارة التشريعات الحكومية، نطاق معالجي المعلومات الشخصية بموجب قانون حماية المعلومات الشخصية (المتعلق بالمادة 2 من قانون حماية المعلومات الشخصية، [تشريعات

وزارة الحكومة 19-0152، 24 يونيو 2019، وزارة الداخلية والأمن]، على موقع NEPLA Beta: https://apps.osrah.sa/jWScjx .

قرار المحكمة الدستورية بكوريا الجنوبية -قرار الهيئة الكاملة –2020 هيونما 1477، بتاريخ: 26 أكتوبر 2023، لتأكيد عدم دستورية المادة 28-7 من قانون حماية المعلومات الشخصية، على موقع CaseNote:

https://casenote.kr/%ED%97%8C%EB%B2%95%EC%9E%AC%ED%8C%90%EC%86%8C/2020%ED%97%8C%EB%A7%881477 .

قرار المحكمة العليا بكوريا الجنوبية، رقم do104612013، بتاريخ: 27 فبراير 2014، على موقع CaseNote:

https://casenote.kr/%EB%8C%80%EB%B2%95%EC%9B%90/2013%EB%8F%840461

يوتيوب

[مباشر] الرئيس يون سوك يول، الاجتماع الطارئ الثالث والعشرون للاقتصاد وسبل عيش الشعب، يدعوا إلى "تخفيف العبء، وزيادة الحيوية"، على يوتيوب: https://www.youtube.com/watch?v=tRUJSY2Qz4E .

مراجع على الإنترنت (باللغة اليابانية)インターネット文献

雑誌論文 المقالات الصحفية

الدفاع السيبراني وعقوبات تسريب معلومات الاتصالات للمسؤولين الحكوميين والمواطنين، تاريخ النشر: 15 يناير 2025، nikkei: https://www.nikkei.com/article/DGXZQOUA15B8T0V10C25A1000000/.

ما هو "القانون الأساسي للأمن السيبراني"؟ شرح واضح لخلفيته ومحتوياته، تاريخ النشر: 2025/01/27، على موقع JBS: https://www.jbsvc.co.jp/useful/security/cyber-security-fundamental-law.html .

القوانين واللوائح اليابانية

قانون الاتصالات السلكية، القانون رقم 96 لسنة 1950، ساري المفعول اعتبارا من 17 يونيو 2020 - القانون الياباني، على موقع e-GOV البحث القانوني: https://laws.e-gov.go.jp/law/328AC0000000096/20220617_504AC0000000068 .

القانون الأساسي للأمن السيبراني، القانون رقم 104 لسنة 2014، ساري المفعول اعتبارا من 17 يونيو 2022، على موقع e-GOV البحث القانوني: https://laws.e-gov.go.jp/law/426AC1000000104 .

قانون تعديل قانون العقوبات وغيره للتعامل مع تقدم معالجة المعلومات، القانون رقم 74 (24 يونيو 2011) – القانون الياباني، على موقع مجلس النواب، اليابان: https://www.shugiin.go.jp/internet/itdb_housei.nsf/html/housei/17720110624074.htm .

قانون حظر الوصول غير المصرح به إلى أجهزة الكمبيوتر، القانون رقم 128 لسنة 1999، الصادر في 17 يونيو 2022، على موقع e-GOV البحث القانوني: https://laws.e-gov.go.jp/law/411AC0000000128/20220617_504AC0000000068 .

مصادر (باللغة الإنجليزية)Sources

مواقع الويب Websites

كتاب إلكتروني e-Book

Jim highsmith, Agile Project Mangement, Addison- Wesley, 2010, Retrieved from: https://www.researchgate.net/publication/234809670_Agile_Project_Management_Creating_Innovative_Products.

e-Journal article مقالة في مجلة إلكترونية

Bill Finnerty, A Digital Government Technology Platform Is Essential to Government Transformation, Gartner, Retrieved from: https://www.gartner.com/en/doc/344044-a-digital-government-technology-platform-is-essential-to-government-transformation.

Alper Kerman, Zero Trust Cybersecurity : Never Trust, Always Verify, 2020.08.28, NIST, Retrieved from: https://www.ncsc.gov.uk/collection/zero-trust-architecture.

DevOps, JFrog, Retrieved from: https://jfrog.com/devops-tools/what-isdevops/.

Zero Trust Architecture Design Principles Peter.R, Zero Trust 1.0, 2021, NCSC, Retrieved from: https://www.ncsc.gov.uk/collection/zero-trust-architecture.

Official websites مواقع رسمية (إلكترونية)

Privacy principles, Organisation for Economic Co-operation and Development (OECD), Retrieved from : https://www.oecd.org/en/topics/privacyprinciples.html#:~:text=They%20set%20out%20eight%20basic,%2C%20individual%20participation%2C%20and%20accountability.

الفهرس

كلية العلوم القانونية والاقتصادية والاجتماعية
تطوان

جامعة عبد المالك السعدي
Université Abdelmalek Essaadi