مجلس الوزراء
مركز المعلومات ودعم اتخاذ القرار

الإطار القانوني للأمن السيبراني في مصر

giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

منتدى السياسات العامة
IDSC Public Policy Forum

عن مركز المعلومات ودعم اتخاذ القرار التابع لمجلس الوزراء المصري

مركز المعلومات ودعم اتخاذ القرار مركز فكر رائد ومُصنَّف دوليًا تابع للسيد رئيس مجلس الوزراء، أنشئ عام ١٩٨٥، وشهد منذ نشأته عددًا من التحولات في طبيعة مهامه وأدواره المختلفة بما يتلاءم مع متطلبات متخذ القرار واحتياجاته، ويتواكب في الوقت ذاته مع طبيعة التغيُّرات التي مر بها المجتمع المصري؛ حيث اهتم في مراحله الأولى **بخلق بنية معلوماتية والإسهام في عمليات التطوير التكنولوجي** في مصر، ثم شهد نقلة نوعية في طبيعة دوره ليصبح أكثر تخصصًا في مجال دعم القرار مع الاهتمام **ببناء مجتمع المعرفة**، ثم سار بخطًى راسخة ليصبح مركز فكر مجلس الوزراء المصري، تتمثَّل مهمته الرئيسة في دعم جهود متخذ القرار في مختلف القضايا التنموية، وطرح مجموعة من البدائل والتوصيات والسيناريوهات الداعمة له. وصولًا إلى مرحلته الراهنة، والتي يضطلع فيها المركز بمهام وأدوار أكثر تعددًا وتنوعًا، وذلك تزامنًا مع **صدور قرار معالي دولة رئيس مجلس الوزراء رقم ٢٠٨٥ لسنة ٢٠٢٣ بشأن إعادة تنظيم المركز**، والذي يعد تدشينًا لمرحلة عمل جديدة امتدت وتوسعت فيها اختصاصات المركز.

ومنذ نشأته كان للمركز العديد من الإنجازات والمشروعات والمبادرات المرموقة التي أسهمت في تعزيز دوره في تطوير البنية الرقمية والمعلوماتية ودعم عملية صنع القرار في مصر على عدد من الأصعدة، ولعل من أبرزها دوره فيما يتعلق بتطوير مشروع الرقم القومي للمواطن، وإدخال شبكة المعلومات الدولية "الإنترنت" للاستخدام في مصر، وإنشاء مركز الوثائق الاستراتيجية، وإنشاء مركز استطلاع الرأي العام، بالإضافة إلى دوره في تطوير وإنشاء مراكز المعلومات بالمحافظات والوزارات، وتدشين "منظومة الشكاوى الحكومية"، وإنشاء منظومة إدارة الأزمات على المستوى القومي والمحلي، وإنشاء المراصد المتخصصة، مثل: مرصد أحوال الأسرة المصرية، والمرصد المصري للتعليم والتدريب والتشغيل، ومرصد الغذاء المصري، بجانب إطلاق وثيقتي سياسة ملكية الدولة للأصول، والتوجهات الاستراتيجية للاقتصاد المصري (٢٠٢٤ - ٢٠٣٠).

ويتبنَّى المركز رؤية مفادها أن يكون الأكثرَ تميُّزًا في مجال دعم اتخاذ القرار في قضايا التنمية الشاملة، وإقامة حوار مجتمعي بنَّاء، وتعزيز قنوات التواصل مع المواطن المصري الذي يُعَدُّ غاية التنمية وهدفها الأسمى، الأمر الذي يؤهِّله للاضطلاع بدور أكبر في صنع السياسة العامة، وترسيخ مجتمع المعرفة.

هذا ويسعى المركز باستمرار لأن يكون إحدى أفضل مؤسسات الفكر (Think Tank) على المستويات كافة؛ المحلية والإقليمية والدولية، وقد واكب ذلك اعترافٌ إقليميٌّ ودوليٌّ بدوره الجوهري كمؤسسة فكر، وهو ما ظهر جليًّا في نتائج تصنيف برنامج مراكز الفكر والمجتمعات المدنية (Think Tanks and Civil Societies Program, TTCSP) بجامعة "بنسلفانيا" الأمريكية، التي أُعلِن عنها في فبراير ٢٠٢١؛ حيث اختِير مركز المعلومات ودعم اتخاذ القرار ليكون:

- ضمن **أفضل ٢٠ مركز فكر على مستوى العالم** استجابةً لجائحة "كوفيد-١٩" لعام ٢٠٢٠.
- في المرتبة ٢١ من بين ٦٤ مركز فكر على مستوى العالم كصاحب **أفضل فكرة أو نموذج جديد** طوَّره خلال عام ٢٠٢٠.
- في المرتبة ١٤ من بين ١٠١ مراكز فكر على مستوى إفريقيا والشرق الأوسط لعام ٢٠٢٠.

وقد فاز المركز خلال السنوات الخمس الأخيرة بـ **(١٨) جائزة دولية** في مجالات عمله كافة؛ حيث فاز في يونيو ٢٠٢٢ **بجائزة (SAG Award)** الأمريكية الممنوحة لإصدارة المركز الرقمية "وصف مصر بالمعلومات" من بين نحو ١٠٠ ألف مؤسسة دولية حول العالم.

وفي مايو ٢٠٢٣، حصل المركز على **٦ جوائز في مسابقة درع الحكومة الذكية** في دورتها السادسة عشرة، والتي عُقدت بإمارة دبي، عن فئات: الابتكار الحكومي، والمسؤولية الاجتماعية والحكومية، والعمل عن بُعد، والمواقع الإلكترونية الحكومية، وحسابات التواصل الاجتماعي الحكومية، والتطبيقات الذكية.

كما نال المركز **ثلاث جوائز من مؤسسة "جلوبي" للأعمال** (Globee Business Awards) بالولايات المتحدة الأمريكية في سبتمبر ٢٠٢٣، والتي تُمنَح لأفضل المنظمات على مستوى العالم تقديرًا لإنجازاتها في مختلف الأعمال والمجالات التكنولوجية.

وكذلك حصد المركز **ثماني جوائز من مؤسسة "ستيفي أووردز" (STEVIE Awards)** العالمية لمنطقة الشرق الأوسط وشمال إفريقيا؛ **ففي أبريل ٢٠٢٢ فاز بخمس جوائز من بينها جائزة ذهبية**، وذلك بعد منافسة بين أكثر من ٧٠٠ فريق من ١٧ دولة في الشرق الأوسط وشمال إفريقيا، **وفي يناير من عام ٢٠٢٤ حاز المركز ثلاث جوائز منها جائزتان ذهبيتان**.

فريق عمل المركز

رئيس المركز

السيد الدكتور / أسامة الجوهري

مساعد رئيس مجلس الوزراء
رئيس مركز المعلومات ودعم اتخاذ القرار

د. مي محسن

رئيس محور المكتب الفني لرئيس المركز ومدير الإدارة العامة للمكتب الفني لرئيس المركز

أ. سالي عاشور

مدير الإدارة العامة للدراسات المستقبلية

أ. منال طلعت

خبير اقتصادي

الفريق القانوني:

د. مروة زين

(مدرس القانون الدولي الخاص بالجامعة البريطانية والمشرف علي البوابة القانونية للتشريعات المصرية)

رغد الحلواني

بسنت إبراهيم

هاجر الخولي

محمد رافع

الإدارة العامة للجودة

أ.عبد الحميد حلمي

التصميم الجرافيكي

الإدارة العامة للتصميم الجرافيكي والمطبوعات

الإطار القانوني للأمن السيبراني في مصر

• الغرض والنطاق

في العقود الثلاثة الماضية لوحظ ازدياد عدد الأشخاص الذين يستخدمون الهواتف الذكية والإنترنت في الأعمال والتجارة والخدمات الحكومية والتعليم وتوافر المعلومات والترفيه والسفر والصحة بالإضافة إلى الأنشطة التجارية والاجتماعية، ويتجلى الاهتمام في التصدي للتهديدات والتحديات التي تستهدف البنية التحتية لتكنولوجيا المعلومات والاتصالات والمعاملات الإلكترونية بشكل عام، فضلاً عن تقويض الثقة في الخدمات الإلكترونية والأعمال الإلكترونية بشكل خاص، وقد أصبح فهم مجال الأمن السيبراني في مصر أمرًا ضروريًّا، ويوضح هذا المقال نظام الأمن السيبراني في مصر ويؤكد أهمية القواعد والقوانين؛ إذ يعَد قانون الأمن السيبراني في مصر ضروريًّا في توجيه الجمهورية للنمو السريع في الصناعة الرقمية.

حيث يمكن أن تسبب الهجمات السيبرانية أضرارًا وخسائر كبيرة في البنية التحتية؛ مما قد يؤثر على الكيانات الحيوية وأعداد كبيرة من المواطنين. ولمكافحة هذه الهجمات؛ يجب الجمع بين آليات التعاون الدولي التقليدية والأطر التشريعية والتنظيمية. وتتطلب الاستجابة الفعالة التعاون والتنسيق على المستوى الوطني بين مقدمي خدمات البنية التحتية، وكذلك التعاون الدولي والإقليمي مع المنظمات الدولية والتجمعات الإقليمية والنقابات المهنية.

قائمة المحتويـات

مقدمة	٣
الإطار القانوني للأمن السيبراني	٣
التعريف القانوني للأمن السيبراني	٣
العناصر الأساسية للأمن السيبراني	٥
١- التنظيم القانوني	٧
حوكمة الأمن السيبراني	٩
مرونة الأمن السيبراني	٩
الاتحاد الدولي للاتصالات ٢٠١٠	١٠
٢- اللوائح القانونية المختلفة للأمن السيبراني	١١
المملكة المتحدة	١٣
الولايات المتحدة الأمريكية	١٧
الهند	٢٥
بلجيكا	٣٣
الصين	٣٧
اليابان	٣٩
كوريا	٤٣
إستونيا	٤٧

٣- مصر	٥١
التعريف بالجرائم الإلكترونية وأنواعها	٥٣
الأبعاد القانونية للأمن السيبراني في مصر	٥٥
١- الإطار القانوني والكيانات التشريعية	٥٥
- المجلس الأعلى المصري للأمن السيبراني ٢٠١٤ (ESCC)	٥٥
- الاستراتيجية الوطنية للأمن السيبراني ٢٠١٧ - ٢٠٢١	٥٥
- المركز المصري للاستجابة لطوارئ الكمبيوتر (EG-CERT)	٥٦
- البنية التحتية للمعلومات المصرية الحيوية	٥٦
- وزارة الاتصالات وتكنولوجيا المعلومات (MCIT)	٥٦
- تكنولوجيا المعلومات والاتصالات (ICT)	٥٦
٢- تنفيذ القوانين وفعالية التشريعات	٥٧
- قانون مكافحة الجرائم الإلكترونية وجرائم تكنولوجيا المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨	٥٧
- قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠	٥٩
قانون تنظيم الاتصالات القومي رقم ١٠ لسنة ٢٠٠٣ (الجهاز القومي لتنظيم الاتصالات)	٦٠
- قرار رئيس مجلس الوزراء رقم ٩٩٤ لسنة ٢٠١٧	٦١
- قانون تنظيم التوقيع الإلكتروني وإنشاء هيئة صناعة تكنولوجيا المعلومات رقم ١٥ لسنة ٢٠٠٤	٦١
- قانون رقم ٩٤ لسنة ٢٠١٥ لمكافحة الإرهاب	٦٢
٣- الاتفاقيات والمعاهدات	٦٢
اتفاقية الاتحاد الإفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية	٦٢
خاتمة	٦٣
التوصيات	٦٣
المراجع	٦٥

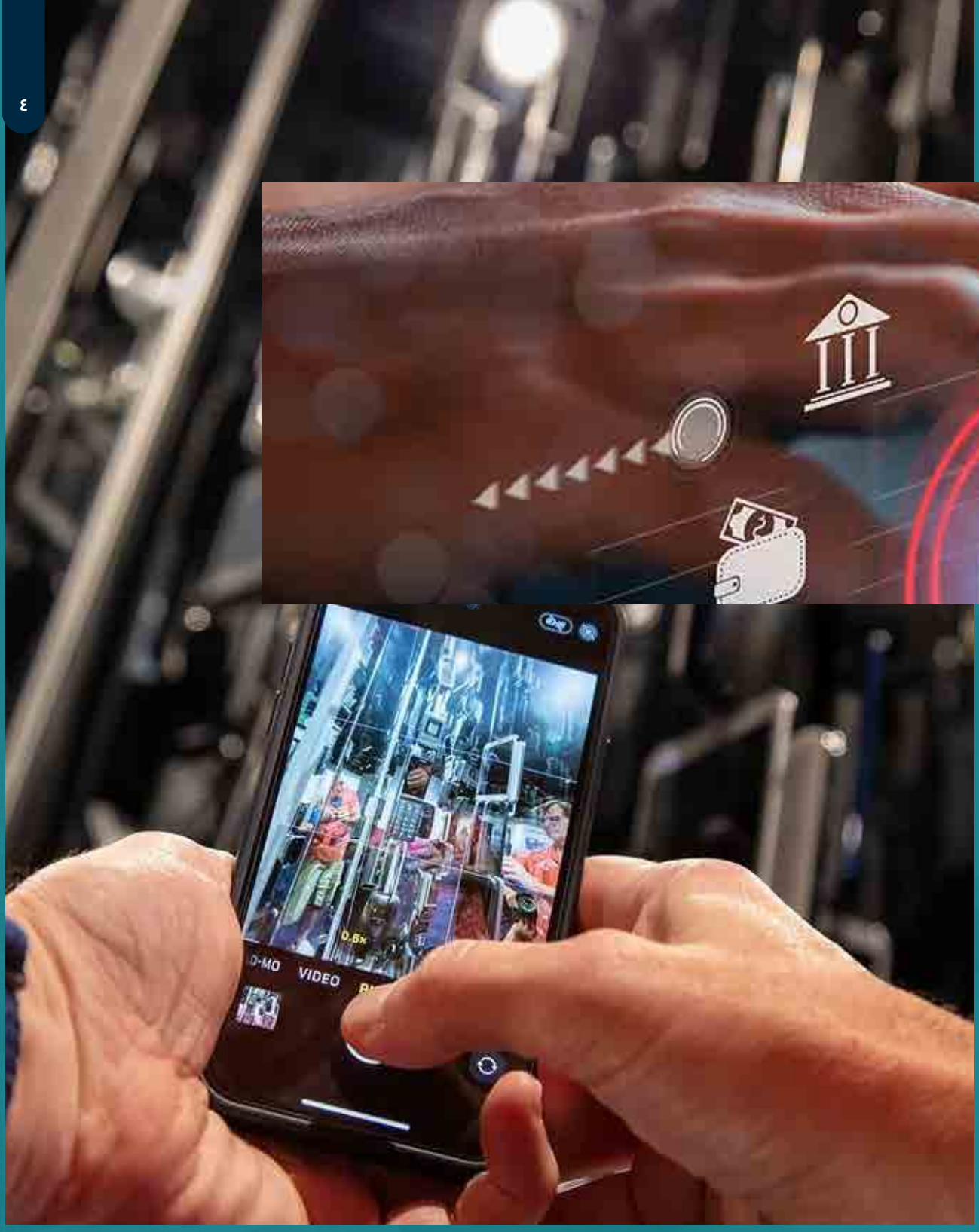
مقدمة

- الإطار القانوني للأمن السيبراني

يؤثر قانون مكافحة الجرائم الإلكترونية وجرائم تكنولوجيا المعلومات المصري بشكل مباشر على حوكمة الشركات بالإضافة إلى غرضه الأساسي وهو حماية المجالات الرقمية. ولتجنب الغرامات؛ يجب على الشركات الآن تنفيذ إجراءات صارمة لإدارة البيانات والأمن السيبراني. ومع ذلك، فإن قانون الاستثمار (رقم ٧٢ لسنة ٢٠١٧) وقانون الشركات المصري (رقم ١٥٩ لسنة ١٩٨١) يضعان الأساس القانوني لعمليات الشركة، ويغطي مسائل مثل إدارة البيانات والملكية الفكرية والسلوك عبر الإنترنت؛ حيث نفذت الحكومات في جميع أنحاء العالم قوانين ولوائح الأمن السيبراني لمكافحة التهديدات السيبرانية، وتغطي هذه القوانين مجالات مثل: حماية البيانات والإبلاغ عن الحوادث وسلطات إنفاذ القانون. ففي الولايات المتحدة يشجع قانون مشاركة معلومات الأمن السيبراني (CISA) شركات القطاع الخاص على مشاركة معلومات تهديدات الأمن السيبراني مع الحكومة، في حين أن اللائحة العامة لحماية البيانات في الاتحاد الأوروبي (GDPR) تتطلب من المؤسسات اتخاذ تدابير قوية للأمن السيبراني لحماية البيانات الشخصية.[1]

- التعريف القانوني للأمن السيبراني

ا- "الأمن السيبراني هو تطبيق التقنيات والعمليات والضوابط لحماية الأنظمة والشبكات والبرامج والأجهزة والبيانات من الهجمات السيبرانية. والهدف هو تقليل مخاطر الهجمات السيبرانية والحماية من الاستغلال غير المصرح به للأنظمة والشبكات والتقنيات".[2]



٢- "الأمن السيبراني هو ممارسة حماية الأنظمة المتصلة بالإنترنت مثل الأجهزة والبرامج والبيانات من التهديدات السيبرانية؛ حيث يتم استخدامه من قبل الأفراد والمؤسسات للحماية من الوصول غير المصرح به إلى مراكز البيانات والأنظمة المحوسبة الأخرى".[3]

٣- "مجموعة الأدوات والسياسات والمبادئ التوجيهية وأساليب إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات والضمانات والتقنيات التي يمكن استخدامها لحماية البيئة السيبرانية والتنظيم، وكذلك أصول المستخدمين".[4]

- العناصر الأساسية للأمن السيبراني

يستخدم الأفراد والمنظمات التدريب للحماية من الوصول غير المصرح به إلى الخوادم وأنظمة الكمبيوتر الأخرى.

- العناصر المختلفة للأمن السيبراني:

١- أمن التطبيقات: هو العنصر الأساسي في الإنترنت الذي يعزز مميزات أمان التطبيقات في أثناء تحسينها لمحاربة التطفلات. إنه يحمي مواقع الويب والتطبيقات عبر الإنترنت من مجموعة من تهديدات الأمن السيبراني التي تستغل نقاط الضعف في التعليمات البرمجية المصدرة، ويرتبط الحفاظ على مبرمجي البرامج في مأمن من التهديدات بأمان التطبيقات. ويركز أمان التطبيقات عمومًا على المؤسسات القائمة على الخدمات السحابية.

٢- أمن المعلومات: هو جزء من الأمن السيبراني الذي يشير إلى التقنيات المستخدمة لمنع الوصول غير المصرح به للبيانات أو استخدامها أو الكشف عنها أو انقطاعها أو تغييرها أو حذفها. ويحمي أمن المعلومات رمز الشركة وبياناتها والمعلومات التي تجمعها من العملاء. وتتثمل المبادئ الثلاثة الرئيسة لأمن المعلومات في: التوفر [5]، والنزاهة [6]، والسرية، ويشار إليها بشكل جماعي باسم CIA [7].

٣- أمان الشبكة: هو الحماية التي تتلقاها الشبكة ضد التهديدات والوصول غير المصرح به؛ حيث يتحمل مسؤولو الشبكات مسؤولية تنفيذ الخطوات الوقائية لحماية شبكاتهم من التهديدات الأمنية المحتملة. عنصر آخر من عناصر أمن تكنولوجيا المعلومات هو أمن الشبكات، وهو أسلوب للحماية ومنع الوصول غير المصرح به إلى شبكات الكمبيوتر [8].

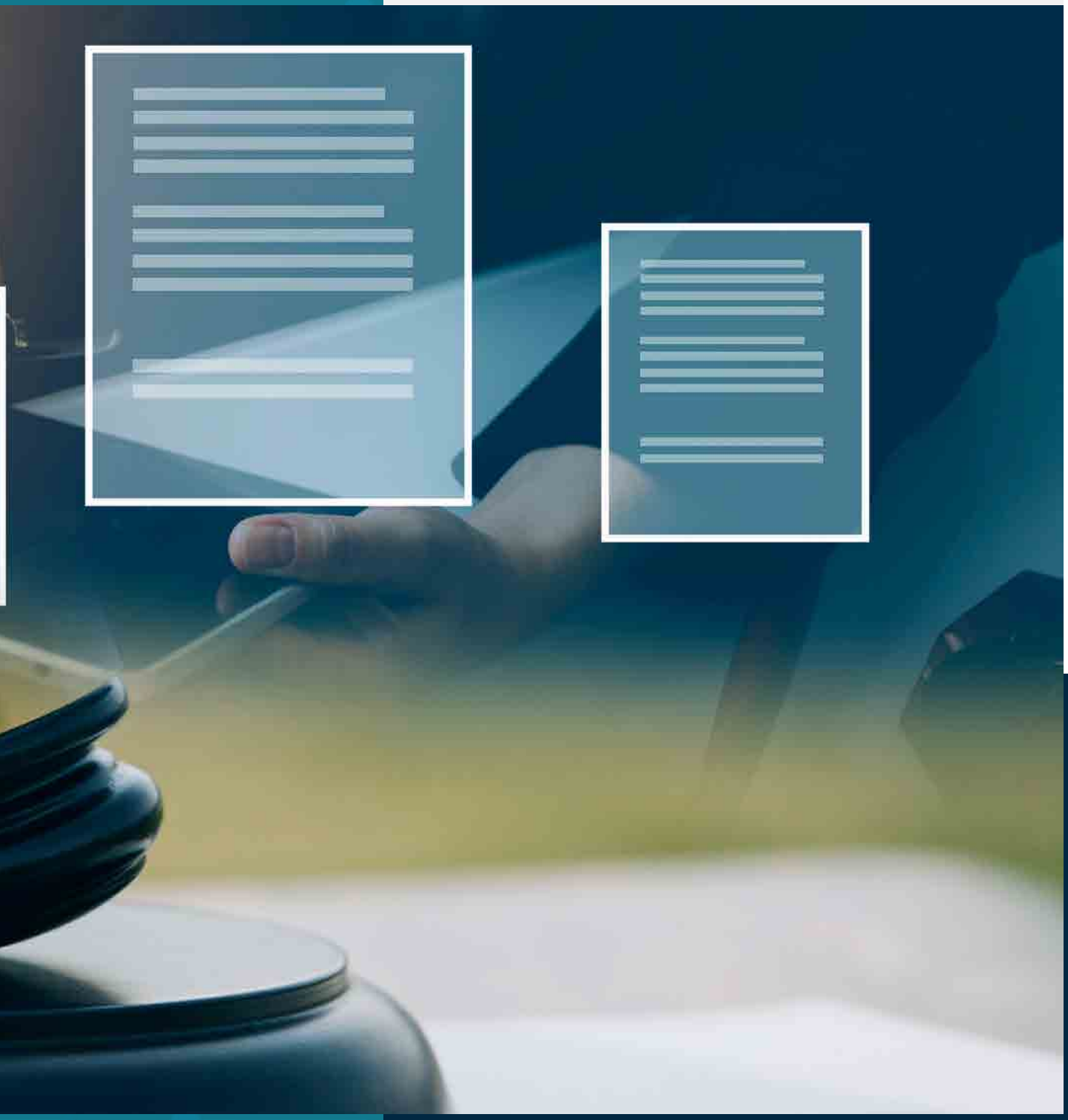
٤- التخطيط للتعافي من الكوارث: التعافي من الكوارث أو التخطيط لاستمرارية الأعمال هو عملية وصف كيفية استمرار العمل بسرعة وفعالية بعد وقوع الكارثة. بدءًا من مستوى الأعمال، يجب أن تحدد استراتيجية التعافي من الكوارث التطبيقات التي تعَد ضرورية عادةً للعمليات اليومية للجمعية. يرتبط الاستعداد لمواجهة التهديدات السيبرانية ارتباطًا وثيقًا بتخطيط استمرارية الأعمال (BCP)، الذي يحدد التهديدات التي تواجه المنظمة في وقت مبكر وينظر في التأثيرات المحتملة على العمليات وكيفية التخفيف منها [9].

٥- الأمن التشغيلي (OPSEC) أو الأمن الإجرائي: هو العملية التي تدفع الشركات إلى تقييم الإجراءات من منظور المتسلل من أجل حماية البيانات الحساسة من المخاطر المختلفة. الغرض من أمن العمليات (OPSEC) هو حماية المعلومات المهمة؛ حيث يقوم بتتبع المعلومات والأصول الأساسية لتحديد أي عيوب، وتحسين التدابير الأمنية واتباع أفضل الممارسات في حماية المعلومات الحساسة من الاستغلال.

٦- أمان المستخدم النهائي: إن أهم عنصر في أمان الكمبيوتر هو تدريب المستخدم النهائي؛ حيث يُعَد الخطأ البشري أحد الأخطاء الفادحة الرئيسة التي تتسبب في تسرب المعلومات، ويجب تثقيف الموظفين حول الأمن السيبراني، كما يجب أن يكون كل ممثل على دراية بمحاولات التصيد الاحتيالي عبر الاتصالات وواجهات المستخدم، ليكون قادرًا على التعامل مع التهديدات عبر الإنترنت.

٧- تهديدات المستخدم النهائي: هناك طرق عديدة يمكن أن تنشأ بها التهديدات؛ حيث يمكن استخدام الطرق التالية لإنشاء مخاطر على المستخدم النهائي: استخدام وسائل التواصل الاجتماعي والرسائل النصية، واستخدام تطبيق البريد الإلكتروني[10].

التنظيم القانوني



التنظيم القانوني

حوكمة الأمن السيبراني

حوكمة الأمن السيبراني هي استراتيجية شاملة للأمن السيبراني تتكامل مع العمليات التنظيمية وتمنع انقطاع الأنشطة بسبب التهديدات أو الهجمات السيبرانية، وتشمل ميزات حوكمة الأمن السيبراني:

- أطر المساءلة
- التسلسل الهرمي لصنع القرار
- تحديد المخاطر المتعلقة بأهداف العمل
- خطط واستراتيجيات التخفيف
- عمليات وإجراءات الرقابة

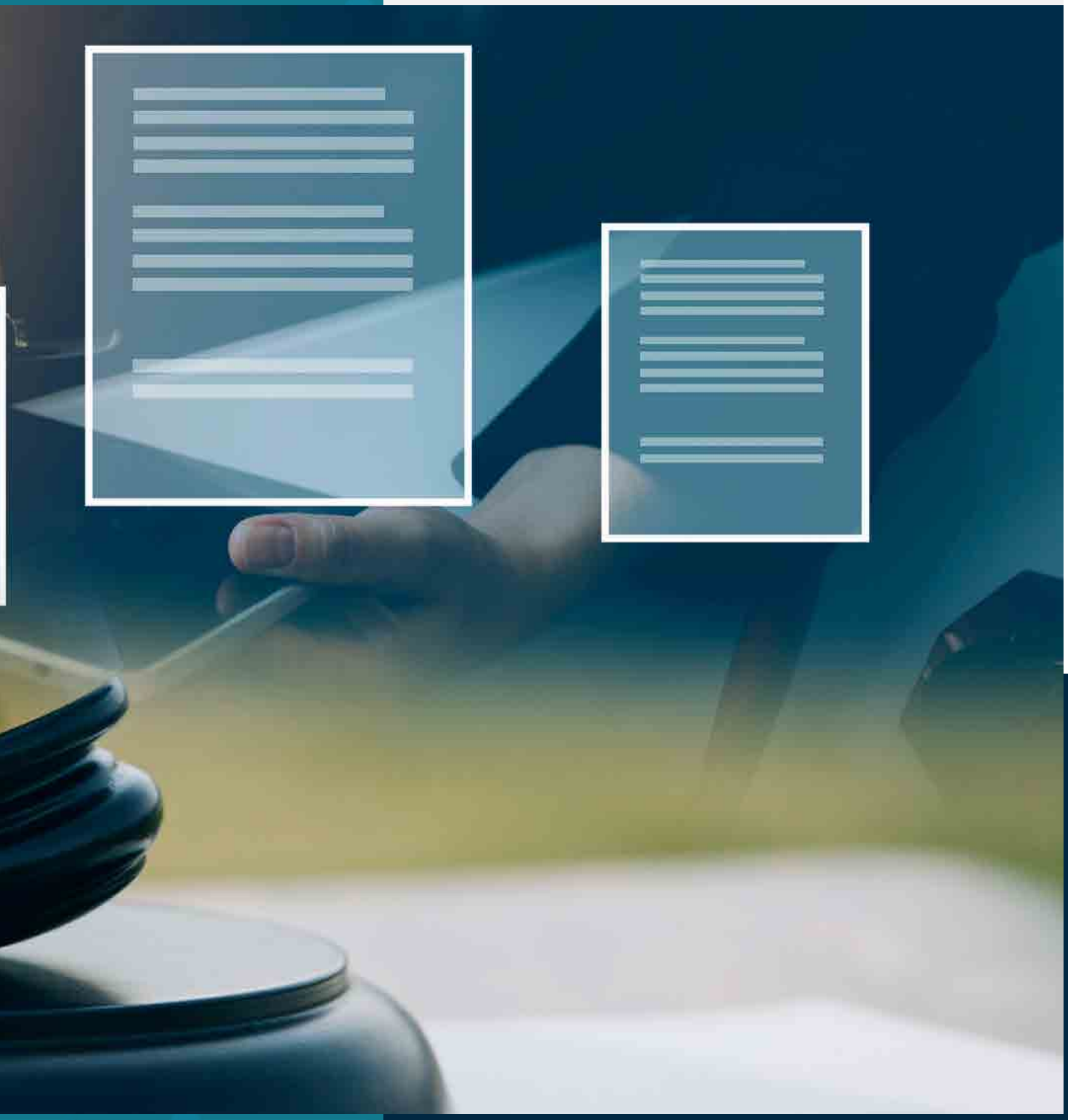
مرونة الأمن السيبراني

مرونة الأمن السيبراني هي القدرة على توقع الظروف المعاكسة أو الضغوط أو الهجمات أو التنازلات والصمود فيها والتعافي منها والتكيف معها على الأنظمة التي تستخدم الموارد السيبرانية أو التي يتم تمكينها بها، والمقصود بالمرونة السيبرانية تمكين المهمة أو أهداف العمل التي تعتمد على الموارد السيبرانية التي يتعين تحقيقها في بيئة سيبرانية متنازع عليها [11].

الاتحاد الدولي للاتصالات ٢٠١٠ (ITU)

الاتحاد الدولي للاتصالات هو وكالة الأمم المتحدة المتخصصة في مجال تكنولوجيا المعلومات والاتصالات (ICT)، ويعمل الاتحاد الدولي للاتصالات على تسهيل الاتصال الدولي في شبكات الاتصالات، وتخصيص الطيف الراديوي العالمي والمدارات الساتلية، ووضع المعايير التقنية التي تضمن توصيل الشبكات والتكنولوجيات بسلاسة، والعمل على تحسين الوصول إلى التقنيات الرقمية في المجتمعات المحرومة في جميع أنحاء العالم [12].

اللوائح القانونية المختلفة للأمن السيبراني

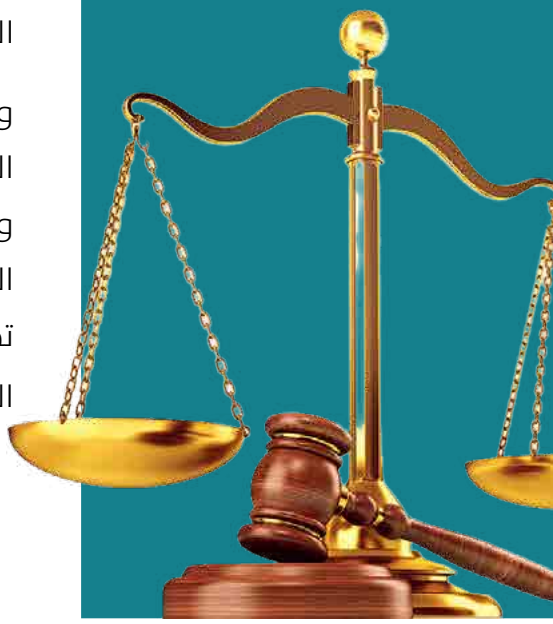


المملكة المتحدة

1 قانون حماية البيانات لعام ٢٠١٨ (DPA)

قانون حماية البيانات لعام ٢٠١٨ (DPA) هو القانون الأساسي لحكومة المملكة المتحدة بشأن معالجة البيانات الشخصية في المملكة المتحدة، والذي يتم تنفيذه جنبًا إلى جنب مع اللائحة العامة لحماية البيانات في المملكة المتحدة. إنه بمثابة إطار لحماية البيانات ينظم جميع جوانب كيفية تحكم الشركات والمؤسسات والهيئات الحكومية في البيانات الشخصية ومعالجتها.

وينطبق هذا على جميع مراقبي البيانات؛ حيث يتطلب قانون حماية البيانات من جميع مراقبي البيانات في المملكة المتحدة (الشركات والمؤسسات التي تتحكم في معالجة البيانات الشخصية) تنفيذ التدابير الأمنية المناسبة لحماية البيانات الشخصية والحفاظ عليها وبشكل أكثر تحديدًا ينطبق هذا على الشركات التي تقوم عادةً بمعالجة بيانات العملاء وسجلاتهم[13].



2

اللائحة العامة لحماية البيانات في المملكة المتحدة (UK-GDPR)

هي لائحة أمن البيانات في المملكة المتحدة والتي تم تصميمها كلائحة مكملة لقانون حماية البيانات لعام ٢٠١٨، كما تم تصميمها أيضًا على غرار اللائحة العامة لحماية البيانات (EU-GDPR)، وهي تحكم وتنظم بشكل أساسي كيفية قيام المؤسسات والشركات في المملكة المتحدة بجمع البيانات الشخصية وتخزينها واستخدامها ومعالجتها[14].

3

لوائح NIS (لوائح أمن الشبكات والمعلومات لعام ٢٠١٨)

لوائح NIS هي "لوائح الشبكات وأنظمة المعلومات لعام ٢٠١٨" والتي دخلت حيز التنفيذ في ١٠ مايو ٢٠١٨، وتهدف اللوائح إلى معالجة التهديدات التي تشكلها أنظمة الشبكات والمعلومات، وبالتالي تهدف إلى تحسين أداء الاقتصاد الرقمي[15].

4

قانون إساءة استخدام الكمبيوتر لعام ١٩٩٠

تعتبر CMA التشريع الرئيس الذي يجرم الوصول غير المصرح به وإتلاف أو تدمير أنظمة الكمبيوتر والبيانات. وقد تم إنشاء القانون بشكل أساسي للتعامل مع مسألة الوصول إلى البيانات أو تعديلها دون إذن، وكذلك لحماية سلامة وأمن أنظمة الكمبيوتر والبيانات من خلال تجريم الوصول إليها دون تصريح من مالك النظام أو البيانات. وينطبق هذا بشكل أساسي على الشركات التي لها عمليات في المملكة المتحدة[16].

5

قانون أمن الاتصالات لعام ٢٠٢١

تم سن هذا القانون بشكل أساسي لوضع أحكام تتعلق بأمن شبكات الاتصالات الإلكترونية العامة وخدمات الاتصالات الإلكترونية العامة، وهو يتناول مقدمي خدمات الاتصالات؛ لأنه يتطلب منهم اتخاذ تدابير لتحديد شبكاتهم والدفاع عنها من التهديدات السيبرانية، وكذلك الاستعداد لأي مخاطر مستقبلية، ويجب اتخاذ إجراء سريع بعد حدوث اختراق أمني للحد من الضرر ومعالجته وتخفيفه.

6

أنظمة تحديد الهوية الإلكترونية وخدمات الثقة للمعاملات الإلكترونية لعام ٢٠١٦ (UK elDAS)

تحدد هذه اللائحة قواعد الخدمات الاستئمانية في المملكة المتحدة وتضع إطارًا قانونيًّا لتوفير وتأثير التوقيعات الإلكترونية والأختام الإلكترونية والطوابع الزمنية الإلكترونية والمستندات الإلكترونية وخدمات التسليم الإلكترونية المسجلة وخدمات الشهادات لمصادقة موقع الويب[17].

7

لوائح الخصوصية والاتصالات الإلكترونية (PECR)

توجد لوائح الخصوصية والاتصالات الإلكترونية (PECR) جنبًا إلى جنب مع قانون حماية البيانات واللائحة العامة لحماية البيانات في المملكة المتحدة؛ وذلك لضمان احترام الشركات لحقوق وخصوصية عملائها المحتملين[18].

الولايات المتحدة

ينقسم تنظيم الأمن السيبراني في الولايات المتحدة في الواقع بين القوانين الفيدرالية وقوانين الولايات، وفي هذا السياق تتولى لجنة التجارة الفيدرالية (FTC) مسؤولية إنفاذ لوائح وتشريعات الأمن السيبراني على المستوى الفيدرالي، هذا بالإضافة إلى وزارة الأمن الداخلي (DHS) والمعهد الوطني للمعايير والتكنولوجيا (NIST)، اللذين لهما أيضًا أدوار في تنظيم الأمن السيبراني.

1 الأمر التنفيذي بشأن تحسين الأمن السيبراني للدولة[19]

أصدر هذا الأمر التنفيذي الرئيس بايدن في ١٢ مايو ٢٠٢١، من أجل تحسين جهود الأمن السيبراني في البلاد؛ حيث يهدف إلى تحقيق الشفافية والتواصل مع المجموعات والأنظمة الفيدرالية بمن في ذلك المقاولون.

حيث يتطلب الأمر من الوكالات تعزيز الأمن السيبراني وسلامة سلسلة توريد البرمجيات.

علاوة على ذلك، فإن النقاط الرئيسة فيه هي كما يلي:

١- إزالة العوائق التي تحول دون تهديد تبادل المعلومات بين الحكومة والقطاع الخاص.

٢- تحديث وتطبيق معايير أقوى للأمن السيبراني في الحكومة الاتحادية.

٣- تحسين أمن سلسلة توريد البرمجيات.

٤- إنشاء قواعد لعب موحدة للاستجابة لثغرات وحوادث الأمن السيبراني.

٥- تحسين قدرات التحقيق والمعالجة.

بالإضافة إلى ذلك، تجدر الإشارة إلى دور وكالة الأمن السيبراني وأمن البنية التحتية CISA؛ حيث ستعمل مع مكتب الإدارة والميزانية للتوصية بلغة العقد التي تجعل مشاركة البيانات المهمة أسهل، بما في ذلك عتبات وأطر الإبلاغ عن الانتهاك، وتتطلب تنفيذ تدابير أمنية مُحسَّنة عبر المقاولين الفيدراليين.

2

قانون خصوصية المستهلك في كاليفورنيا، بصيغته المعدلة بموجب قانون حقوق الخصوصية في كاليفورنيا (CCPA)

يمنح هذا القانون الحقوق المتعلقة بالمعلومات الشخصية ويفرض واجبات مختلفة لحماية البيانات على بعض الكيانات التي تمارس أعمالاً تجارية في كاليفورنيا؛ حيث إنه يعزز حقوق الخصوصية وحماية المستهلك لمنع إساءة استخدام بيانات المستهلك.

ينطبق قانون CCPA قانون حقوق الخصوصية على الشركات الربحية التي تمارس أعمالاً تجارية في كاليفورنيا؛ لذلك تندرج بعض العوامل ضمن لوائح قانون حقوق الخصوصية CCPA لتحديد من يجب أن يلتزم بـها، وهي:

- الحصول على دخل سنوي إجمالي الإيرادات لا يقل عن ٢٥ مليون دولار.
- شراء أو بيع أو مشاركة بيانات ١٠٠ ألف أو أكثر من المقيمين أو الأسر أو الأجهزة في كاليفورنيا.
- كسب ٥٠٪ أو أكثر من إيراداتهم السنوية من بيع المعلومات الشخصية للمقيمين في كاليفورنيا [20].

يتطلب قانون حقوق الخصوصية أيضًا من المؤسسات أن تكون شفافة بشأن ممارسات جمع البيانات واستخدامها، والاستجابة لطلبات المستهلكين، وتنفيذ إجراءات أمنية معقولة لحماية بيانات المستخدم [21].

كما أنها أنشأت العديد من أحكام الخصوصية الرئيسة التي يجب على المؤسسات الالتزام بها لحماية حقوق خصوصية البيانات، وهي:

١- الحق في معرفة أو طلب الكشف عن المعلومات الشخصية التي تجمعها الشركة عن المستهلك[22].

٢- الحق في حذف المعلومات الشخصية، والحق في إلغاء الاشتراك في بيع المعلومات الشخصية[23].

٣- الحق في إلغاء الاشتراك في بيع المعلومات الشخصية للمستهلكين[24].

٤- الحق في المعاملة غير التمييزية[25].

٥- الحق في رفع دعوى خاصة لانتهاكات البيانات[26].

3

قانون جرام ليتش بليلي (GLBA)

- هو قانون فيدرالي صدر في الولايات المتحدة يهدف إلى تعزيز خصوصية المستهلك وأمن البيانات الخاصة بالمؤسسات المالية، وهو يركز على حماية المعلومات الشخصية غير العامة (NPI) التي تحتفظ بها المؤسسات المالية.
- هذا القانون هو قانون أمن المعلومات والخصوصية، وينطبق على المؤسسات المالية التي تشمل البنوك وشركات التأمين وشركات الأوراق المالية ومقرضي الرهن العقاري غير المصرفيين، إلخ.
- يتطلب بشكل أساسي من المؤسسات المالية -الشركات التي تقدم منتجات أو خدمات مالية للمستهلكين مثل القروض، أو الاستشارات المالية أو الاستثمارية أو التأمين- شرح ممارسات مشاركة المعلومات لعملائها وحماية البيانات الحساسة[27].

3 المعهد الوطني للمعايير والتكنولوجيا (NIST)

أسس الكونجرس الأمريكي NIST في ٣ مارس ١٩٠١، NIST هو المعهد الوطني للمعايير والتكنولوجيا التابع لوزارة التجارة الأمريكية، ويحتوي على إطار عمل للأمن السيبراني يساعد الشركات من جميع الأحجام على فهم مخاطر الأمن السيبراني وإدارتها وتقليلها بشكل أفضل وحماية شبكاتها وبياناتها. إن إطار عمل المعهد طوعي؛ فهو يقدم الخطوط العريضة لأفضل الممارسات التي تساعد في تحديد مكان تركيز الوقت والمال لحماية الأمن السيبراني[28].

4 قانون لجنة التجارة الفيدرالية

يحدد قانون لجنة التجارة الفيدرالية الذي صدر عام ١٩١٤ عدة أهداف وأحكام رئيسة، وأهم هدف يتعلق بالأمن السيبراني هو حماية المستهلكين، وينطبق هذا القانون على كل مؤسسة تقريبًا في الولايات المتحدة باستثناء البنوك وشركات النقل العامة، علاوة على ذلك فإن المادة ٥ من قانون لجنة التجارة الفيدرالية (FTC) عبارة عن لائحة لأمن المعلومات (التي تتطلب تدابير مناسبة للأمن السيبراني) وقانون الخصوصية، وقد تم إنشاء لجنة التجارة الفيدرالية في ٢٦ سبتمبر ١٩١٤، وتعمل اللجنة بشكل أساسي على تطبيق قوانين حماية المستهلك الفيدرالية التي تمنع الاحتيال والخداع والممارسات التجارية غير العادلة.

5 قانون حماية خصوصية الأطفال على الإنترنت

ينطبق هذا القانون على مواقع الويب والخدمات عبر الإنترنت الموجهة للأطفال الذين تقل أعمارهم عن ١٣ عامًا، وينطبق أيضًا إذا كان لدى مشغل الموقع معرفة فعلية بأن الأطفال الذين تقل أعمارهم عن ١٣ عامًا يستخدمون موقع الويب.

وينظم القانون بشكل أساسي كيفية جمع هذه المواقع و/أو استخدامها و/أو الكشف عن المعلومات الشخصية من الأطفال وعنهم.

6 قانون حماية الاتصالات الإلكترونية (ECPA)

يُعَد قانون حماية الاتصالات الإلكترونية (ECPA) أحد قوانين الخصوصية؛ فهو ينظم بشكل أساسي الحالات التي يمكن فيها اعتراض الاتصالات الإلكترونية أو مراقبتها أو مراجعتها من قبل أطراف ثالثة؛ مما يجعل اعتراض الاتصالات الإلكترونية أو الحصول عليها جريمة ما لم ينص القانون على خلاف ذلك أو استثناء من قانون حماية الاتصالات الإلكترونية (ECPA) فهو يحمي الاتصالات السلكية والشفوية والإلكترونية في أثناء إجراء هذه الاتصالات وفي أثناء نقلها وتخزينها على أجهزة الكمبيوتر، وينطبق القانون على البريد الإلكتروني والمحادثات الهاتفية والبيانات المخزنة إلكترونيًّا.

7 القانون الفيدرالي لمكافحة الاحتيال وإساءة استخدام الكمبيوتر (CFAA)

إنه قانون اتحادي يحمي المعلومات الرقمية من الوصول غير المصرح به، ويحكم CFAA كل جهاز كمبيوتر متصل بالإنترنت وأجهزة الكمبيوتر غير المتصلة بالشبكة التي تستخدمها الحكومة الفيدرالية أو المؤسسات المالية.

وينطبق هذا بشكل أساسي على جميع الأفراد الذين يصلون عمدًا إلى جهاز كمبيوتر محمي دون الحصول على إذن مناسب أو حتى الذين يتجاوز وصولهم التفويض الممنوح لهم.

8 قانون SHIELD في نيويورك

في ٢٥ يوليو ٢٠١٩ تم سن قانون New York SHIELD في عام ٢٠١٩ لوقف الاختراقات وتحسين أمن البيانات الإلكترونية، ويعمل قانون SHIELD على تعزيز قوانين أمن البيانات في نيويورك بشكل كبير من خلال: توسيع أنواع المعلومات الخاصة التي يجب على الشركات تقديم إشعار للمستهلك بشأنها في حالة حدوث خرق مما يتطلب من الشركات تطوير وتنفيذ والحفاظ على ضمانات معقولة لحماية أمن المعلومات الخاصة وسريتها وسلامتها.

ومع ذلك، فإنه ينطبق على أي شخص أو شركة تمتلك أو ترخص البيانات المحوسبة التي تتضمن المعلومات الخاصة لأحد المقيمين في نيويورك.

9 قانون قابلية نقل التأمين الصحي والمساءلة (HIPAA)

يتطلب قانون HIPAA من الكيانات المشمولة تنفيذ العديد من الضمانات الإدارية والمادية والفنية لحماية سرية وسلامة وتوافر المعلومات الصحية المحمية إلكترونيًّا(ePHI) .

وينطبق هذا على الخطط الصحية، ومراكز تبادل المعلومات الخاصة بالرعاية الصحية، ومقدمي الرعاية الصحية الذين يقومون بإجراء بعض معاملات الرعاية الصحية إلكترونيًّا لحماية المعلومات الصحية المحمية (PHI) الموكلة إليهم.

تضع قاعدة أمان HIPAA معايير وطنية لحماية المعلومات الصحية الشخصية الإلكترونية للأفراد، والتي يتم إنشاؤها أو استلامها أو استخدامها أو الاحتفاظ بها بواسطة كيان مشمول.

10 قانون تبادل معلومات الأمن السيبراني (CISA)

قانون تبادل معلومات الأمن السيبراني CISA هو قانون اتحادي أمريكي تم سنُّه في عام ٢٠١٥ بهدف تعزيز الأمن السيبراني في الولايات المتحدة، ويهدف القانون بشكل أساسي إلى تحسين تبادل المعلومات المتعلقة بتهديدات الأمن السيبراني بين الحكومة الفيدرالية والقطاع الخاص، ويهدف إلى تحقيق ذلك من خلال تسهيل مشاركة معلومات التهديدات السيبرانية؛ مما يعزز قدرة كلا القطاعين على الوقاية من الهجمات السيبرانية والتصدي لها[29].

11 قانون الإبلاغ عن الحوادث السيبرانية للبنية التحتية الحيوية لعام ٢٠٢٢

تم سن هذا القانون من أجل تحسين الأمن السيبراني في أمريكا، ومن بين أمور أخرى فإنه يتطلب من وكالة الأمن السيبراني وأمن البنية التحتية (CISA) تطوير وتنفيذ اللوائح التي تتطلب من الكيانات المشمولة الإبلاغ عن الحوادث السيبرانية المغطاة ومدفوعات برامج الفدية إلى CISA[30].

- **هيئة الأوراق المالية والبورصات (SEC)**

توفر هيئة الأوراق المالية والبورصة (SEC) إرشادات حول الأمن السيبراني لمساعدة الوسطاء والتجار ومستشاري الاستثمار وشركات الاستثمار والبورصات وغيرهم من المشاركين في السوق على حماية عملائهم من التهديدات السيبرانية[31].

- **معيار أمن بيانات صناعة بطاقات الدفع (PCI DSS)**

تم تطوير هذا المعيار لتشجيع وتعزيز أمن بيانات حساب بطاقة الدفع وتسهيل الاعتماد الواسع النطاق لتدابير أمن البيانات المتسقة على مستوى العالم، وهي مصممة للحد من الاحتيال في بطاقات الدفع عن طريق زيادة الضوابط الأمنية حول بيانات حامل البطاقة.

الهنـــد

1

قانون تكنولوجيا المعلومات (IT) لعام ٢٠٠٠ وتعديله الأخير في عام ٢٠٢٣

تم سن قانون تكنولوجيا المعلومات لتوفير الاعتراف القانوني بالمعاملات الإلكترونية، وتسهيل الإدارة الإلكترونية، وردع الجرائم الإلكترونية، وهو يحدد الجرائم المختلفة المتعلقة بالوصول غير المصرح به، والقرصنة، وسرقة البيانات، وسرقة الهوية، والإرهاب السيبراني، والفحش في الفضاء السيبراني. وحددت التعديلات الأخرى جرائم جديدة مثل: الإرهاب السيبراني، وسرقة الهوية، والوصول غير المصرح به إلى الأنظمة المحمية. كما تم توسيع نطاق العقوبة على الجرائم المختلفة، وتناول المخاوف المتعلقة بخصوصية البيانات والأحكام المتعلقة بحماية البيانات الشخصية الحساسة والتعامل معها.[32]

أهمية القانون

تناول قانون تكنولوجيا المعلومات المستندات الإلكترونية والتوقيعات الإلكترونية والمصادقة على تلك السجلات، كما سن عقوبات على جرائم الخرق الأمني بما في ذلك إتلاف أنظمة الكمبيوتر أو ارتكاب الإرهاب السيبراني.

◈ الجمهور المستهدف

الجمهور المستهدف من قانون تكنولوجيا المعلومات هو الهند بأكملها، وباستثناء ما هو منصوص عليه بخلاف ذلك في هذا القانون، فإنه ينطبق أيضًا على أي جريمة أو مخالفة بموجب هذا القانون يرتكبها أي شخص خارج الهند.[33]

◈ مقالات مرتبطة بالأمن السيبراني

- **القسم ٤٣، ٤٣ أ:** يتناول هذا القسم الوصول غير المصرح به، وتلف الكمبيوتر، وسرقة البيانات، كما يوفر العلاجات القانونية والعقوبات للجرائم المتعلقة بالوصول غير المصرح به إلى أنظمة الكمبيوتر، وتلوث الكمبيوتر، والاستخراج غير المصرح به للبيانات، والتعويض عن الفشل في حماية البيانات.[34]
- **القسم ٦٥، ٦٦، ٦٦ أ، ٦٦ ب، ٦٦ ج، ٦٦ د، ٦٦ هـ، ٦٦ ف:** يركز هذا القسم على الجرائم الإلكترونية المختلفة، مثل: القرصنة، وسرقة الهوية، والاحتيال السيبراني، والعقوبة على إرسال رسائل مسيئة، والغش بالشخصية، والإرهاب السيبراني، كما يُمكِّن وكالات إنفاذ القانون من التحقيق مع الأفراد المتورطين في هذه الجرائم ومحاكمتهم.[35]
- **القسم ٦٩، ٦٩ أ:** يمنح هذا القسم الحكومة سلطة اعتراض المعلومات ومراقبتها وفك تشفيرها لصالح الأمن القومي، ويُمكِّن الحكومة من اتخاذ التدابير اللازمة لمنع التهديدات السيبرانية وضمان سلامة وسيادة البلاد.[36]
- **القسم ٧٠:** يتناول هذا القسم حماية البنية التحتية الحيوية للمعلومات، وينصُّ على تحديد وحماية أنظمة المعلومات الحيوية لضمان استمرارية الخدمات الأساسية وحماية المصالح الوطنية.[37]

2

قواعد تكنولوجيا المعلومات (الممارسات والإجراءات الأمنية المعقولة والبيانات أو المعلومات الشخصية الحساسة) ٢٠١١

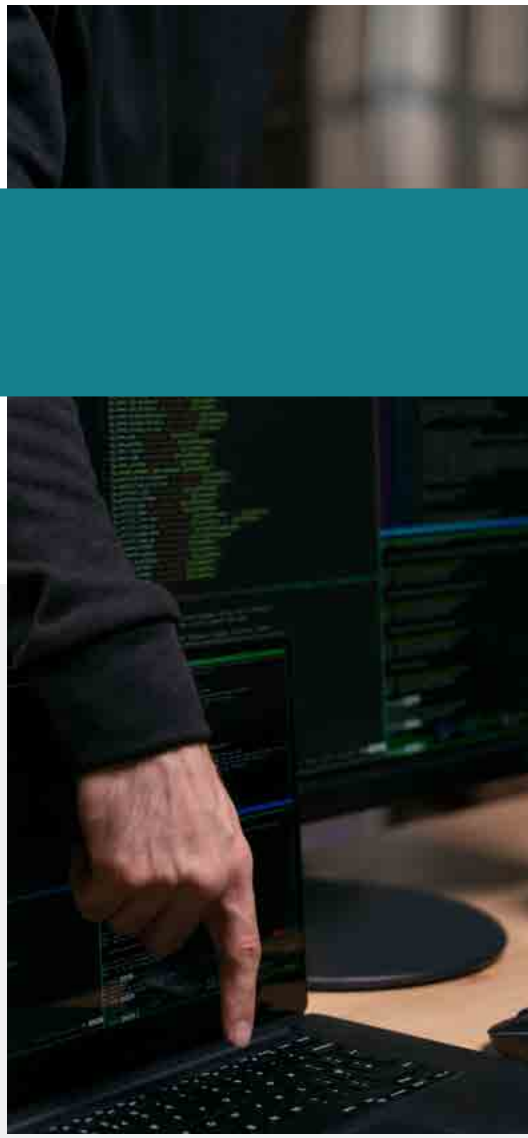
تم وضع قواعد عام ٢٠١١ بموجب المادة ٤٣ أ من قانون تكنولوجيا المعلومات لعام ٢٠٠٠ (قانون تكنولوجيا المعلومات).[38]

أهـميــة القـواعــد

يعَد كل من قانون تكنولوجيا المعلومات (ITA) وقواعد تكنولوجيا المعلومات أمرًا مهمًّا لتنظيم كيفية معالجة الكيانات والمنظمات الهندية للمعلومات الحساسة، وحماية البيانات، والاحتفاظ بالبيانات، وجمع البيانات الشخصية والمعلومات الحساسة الأخرى.

الجمهور المستهدف

- الجمهور المستهدف هنا في قواعد تكنولوجيا المعلومات هو الهند بأكملها مثل قانون تكنولوجيا المعلومات.
- قانون تكنولوجيا المعلومات مبني على القسم ٤٣A من قانون تكنولوجيا المعلومات ٢٠٠٠.



3

سياسة الأمـن السيبراني الوطني في الهنــد لعام ٢٠١٣

في عام ٢٠١٣، أصدرت وزارة الإلكترونيات وتكنولوجيا المعلومات (DeitY) السياسة الوطنية للأمن السيبراني ٢٠١٣ كإطار أمني للمؤسسات العامة والخاصة لحماية نفسها بشكل أفضل من الهجمات السيبرانية.

◈ أهمية السياسة

الهدف من السياسة الوطنية للأمن السيبراني هو إنشاء وتطوير سياسات أكثر ديناميكية لتحسين حماية النظام البيئي السيبراني في الهند، وتهدف السياسة أيضًا إلى إنشاء قوة عاملة تضم أكثر من ٥٠٠ ألف متخصص في مجال تكنولوجيا المعلومات على مدى السنوات الخمس التالية من خلال تطوير المهارات والتدريب.

◈ أهداف السياسة العامة

- إنشاء فضاء إلكتروني مرن وآمن للأفراد والمنظمات والحكومة.
- مراقبة وحماية البنية التحتية والمعلومات السيبرانية، والحد من نقاط الضعف، وتعزيز الدفاعات ضد الهجمات السيبرانية.
- إنشاء أطر وقدرات واستراتيجيات لإدارة الثغرات الأمنية لتقليل الحوادث السيبرانية والتهديدات السيبرانية أو الوقاية منها بشكل أسرع أو الاستجابة لها.
- تشجيع المؤسسات على تطوير سياسات الأمن السيبراني التي تتوافق مع الأهداف الاستراتيجية وسير العمل التجاري وأفضل الممارسات العامة.
- إنشاء الهياكل المؤسسية والأشخاص والعمليات والتكنولوجيا والتعاون بشكل متزامن لتقليل الأضرار الناجمة عن الجرائم الإلكترونية.[39]

4 الاستراتيجية الوطنية للأمن السيبراني ٢٠٢٠

أنشأ مجلس أمن البيانات الهندي (DSCI) الاستراتيجية الوطنية للأمن السيبراني في عام ٢٠٢٠، وركز البحث على ٢١ مجالاً لضمان أن يكون الفضاء الإلكتروني في الهند آمنًا وجديرًا بالثقة ومرنًا وديناميكيًا.[40]

◈ أهمية الاستراتيجية

تتمثل الأهمية الرئيسة للاستراتيجية في تحسين وضع الهند في الفضاء الإلكتروني، وكذلك زيادة التركيز على الهجمات الإلكترونية، وحماية البنية التحتية للمعلومات الحيوية.

◈ الجمهور المستهدف

- مختلف أصحاب المصلحة مثل الوكالات الحكومية
- مؤسسات القطاع الخاص
- الأفراد والجمهور العام
- معاهد البحوث
- المنظمات الدولية

5

قانون بنك الاحتياطي الهندي، ١٩٣٤ (بصيغته المعدلة بموجب قانون المالية، ٢٠٢٢)

قدم بنك الاحتياطي الهندي قانون RBI، الذي يوضح بالتفصيل إرشادات وأطر الأمن السيبراني لـ UCBs (البنوك التعاونية الحضرية) ومشغلي الدفع.[41]

◈ أهمية القانــون

يهدف قانون RBI لعام ٢٠١٨ إلى:

- إنشاء معايير تعمل على مساواة الأطر الأمنية للبنوك ومشغلي الدفع وفقًا لكيفية تكيُّفهم مع التقنيات الجديدة والتحول الرقمي.
- تكليف البنوك بإنشاء وتقديم خططها لإدارة الأزمات السيبرانية.
- تكليف البنوك بتنفيذ سياسات أمن المعلومات المعتمدة من قبل الشركات (المعتمدة من مجلس الإدارة) التي ستحدد بنجاح الاستعداد للأمن السيبراني.
- مطالبة البنوك بتنفيذ إخطارات الانتهاك الإلزامية، حيث يجب على UCBs الكشف على الفور عن حوادث الأمن السيبراني والإبلاغ عنها إلى RBI في غضون ٢-٦ ساعات من اكتشافها للاستجابة بشكل أفضل للهجمات.
- تشجيع البنوك على جدولة عمليات تدقيق تقييم التهديدات بشكل منتظم.
- مساعدة البنوك على تنفيذ نطاقات البريد الإلكتروني الخاصة بها باستخدام تكنولوجيا مكافحة التصيد الاحتيالي والبرامج الضارة، بالإضافة إلى فرض ضوابط أمان DMARC.

◈ الجمهور المستهدف

الجمهور المستهدف هو جميع البنوك الهندية التي يجب أن تتبع هذه الإرشادات لتوحيد أطر معالجة الدفع والأمن السيبراني ومكافحة التعقيدات التجارية المتزايدة باستمرار في البيئة الرقمية.

6

قانون حماية البيانات الشخصية الرقمية لعام ٢٠٢٣ (DPDP)

في ١١ أغسطس ٢٠٢٣، أقرت الحكومة المركزية الهندية قانون حماية البيانات الشخصية الرقمية (DPDP) الذي طال انتظاره، ويستعير القانون تعريفه الواسع للبيانات الشخصية من اللائحة العامة لحماية البيانات (GDPR) للاتحاد الأوروبي.[42]

◈ أهمية القانــون

يهدف قانون حماية البيانات الشخصية الرقمية إلى توفير معالجة البيانات الشخصية الرقمية بطريقة تعترف بحق الأفراد في حماية بياناتهم الشخصية والحاجة إلى معالجة هذه البيانات الشخصية لأغراض مشروعة وللمسائل المرتبطة بها أو العرضية، وتقييد أنشطة وكلاء البيانات.

◈ الجمهور المستهدف

- المواطنون الهنود
- المنظمات والشركات
- وحدات تحكم البيانات والمعالجات
- الوكالات الحكومية

7

الورقة البيضاء للجنة الخبراء بشأن إطار حماية البيانات في الهند

شكلت حكومة الهند لجنة خبراء لدراسة مختلف القضايا المتعلقة بحماية البيانات في الهند، وتقديم اقتراحات محددة بشأن المبادئ التي يقوم عليها مشروع قانون حماية البيانات وصياغة مشروع القانون هذا.[43]

◈ أهـداف الورقـة

والهدف هو "ضمان نمو الاقتصاد الرقمي مع الحفاظ على البيانات الشخصية للمواطنين آمنة ومحمية".

◈ الجمهور المستهدف

الهند كلها

بلجيكا

1

قانون التصنيف ١٩٩٨

القانون الصادر في ١١ كانون الأول/ديسمبر ١٩٩٨ بشأن التصنيف والتصاريح الأمنية والشهادات الأمنية والمشورة الأمنية ("قانون التصنيف").[44]

أهمية القانون

أهمية القانون تتمثل في ضرورة إجراء الفحوصات الأمنية وإنشاء هيئة استئنافية للتصاريح الأمنية، وضمان قدرة الشخص على ممارسة حقوق أو صلاحيات محددة دون الإضرار بالمصالح الأساسية للدولة على النحو المنصوص عليه في المادة ٢٢د من القانون.

2

قانون البنية التحتية الحيوية (CIA) لعام ٢٠١١، المعدل في ٢١ أغسطس ٢٠٢٣

قانون ١ يوليو ٢٠١١ بشأن أمن وحماية البنية التحتية الحيوية، يحتوي قانون البنية التحتية الحيوية على قواعد لتحديد مشغلي البنية التحتية الحيوية، بالإضافة إلى متطلبات اعتماد التدابير الأمنية المناسبة.[45]

◈ أهمية القانون

- وضع قواعد لحماية البنية التحتية الحيوية.
- الجهات الحكومية المعنية بحماية البنية التحتية الحيوية.

3

قانون حماية البيانات الصادر في ٣٠ يوليو ٢٠١٨ والمعدل بتاريخ ٣١ ديسمبر ٢٠٢١

قانون ٣٠ يوليو ٢٠١٨ قانون حماية البيانات المتعلق بحماية الأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية.[46]

◈ أهمية القانون

يهدف القانون إلى حماية البيانات الشخصية وحرية حركتها.

◈ الجمهور المستهدف

- وحدات التحكم
- الجهات المختصة والهيئات الإدارية

4 قانون أمن الشبكات والمعلومات NIS ٢٠١٩

هو قانون صدر في ٧ أبريل ٢٠١٩، ويضع إطارًا لأمن الشبكات وأنظمة المعلومات ذات المصلحة العامة للأمن العام.[47]

◈ أهمية القانون

يقدم قانون أمن الشبكات والمعلومات NIS مجموعة من القواعد لمشغلي الخدمات الأساسية (OESs) ومقدمي الخدمات الرقمية (DSPs). كما أنه يعدل أطر الأمن السيبراني الحالية، ويتطلب من هذه الكيانات اعتماد تدابير أمنية كافية، لمنع حوادث الأمن السيبراني. علاوة على ذلك، يفرض قانون أمن الشبكات والمعلومات بعض متطلبات الإخطار إلى السلطات المختصة.

◈ الجمهور المستهدف

مشغلو الخدمة

5 مرسوم ملكي NIS ١٢ يوليو ٢٠١٩

المرسوم الملكي المؤرخ في ١٢ يوليو ٢٠١٩ بتنفيذ القانون الصادر في ٧ أبريل ٢٠١٩ بشأن إنشاء إطار لأمن الشبكات وأنظمة المعلومات ذات المصلحة العامة للسلامة العامة، والقانون الصادر في ١ يوليو ٢٠١١ بشأن أمن وحماية البنية التحتية الحيوية.[48]

◈ أهمية المرسوم

يركز مرسوم NIS على إسناد المسؤوليات بين السلطات العامة ذات الصلة في بلجيكا، وكذلك على وضع إجراءات الامتثال لالتزامات الإخطار في حالة وقوع حادث يتعلق بالأمن السيبراني.

◈ الجمهور المستهدف

- مشغلو الخدمة
- الجهات الحكومية

الصيـــن

1 قانون الأمن السيبراني (CSL)

يعَد قانون الأمن السيبراني، الذي صدر في عام ٢٠١٧، أحد أكثر التشريعات شمولاً فيما يتعلق بالأمن السيبراني في الصين. وهو ينظم جوانب مختلفة من الأمن السيبراني، بما في ذلك حماية البيانات، وأمن البنية التحتية للمعلومات الحيوية (CII)، ومراقبة الأمن السيبراني والاستجابة لحالات الطوارئ، ومسؤوليات مشغلي الشبكة. ويفرض القانون التزامات على مشغلي الشبكات بتنفيذ التدابير الأمنية وإجراء التقييمات الأمنية والإبلاغ عن الحوادث الأمنية.[49]

2 قانون أمن البيانات (DSL)

ويهدف قانون أمن البيانات، الذي تم إقراره في عام ٢٠٢١ ومن المقرر أن يدخل حيز التنفيذ في سبتمبر من نفس العام، إلى تعزيز حوكمة البيانات وحماية أمن البيانات في الصين. فهو يحدد مواصفات جمع البيانات ومعالجتها ونقلها وتخزينها واستخدامها. ويشمل ذلك البيانات الحساسة المتعلقة بالمصالح العامة والأمن القومي بالإضافة إلى المعلومات الخاصة. يُطلب من معالجي البيانات بموجب القانون تنفيذ التدابير الأمنية وإجراء تقييمات المخاطر وإخطار الأطراف الثالثة بانتهاكات البيانات.

3 قانون الاستخبارات الوطني

صدر قانون الاستخبارات الوطني في عام ٢٠١٧، وهو يمكّن وكالات الاستخبارات الصينية من إجبار المنظمات والأفراد على التعاون مع العمل الاستخباراتي والحفاظ على سرية المعلومات الحساسة. ويقول المنتقدون إن هذا القانون قد يتطلب من الشركات الصينية مساعدة الحكومة في الأنشطة الاستخباراتية؛ مما يثير المخاوف بشأن الخصوصية وأمن البيانات.

4 نظام الحماية متعدد المستويات (MLPS)

نظام الحماية متعدد المستويات هو نظام لإصدار شهادات الأمن السيبراني قدمته الحكومة الصينية لتقييم وتصنيف مستوى الأمان لأنظمة وشبكات المعلومات. ويتطلب الأمر من المؤسسات، وخاصة مشغلي CII، الخضوع لتقييمات أمنية والحصول على شهادة بناءً على مستوى المخاطر لديها.

5 لوائح البنية التحتية الحيوية الحاسمة (CIIS)

- تحدد لوائح البنية التحتية الحيوية الحاسمة CIIS الصادرة عن إدارة الفضاء الإلكتروني الصينية (CAC) المتطلبات الأمنية لمشغلي البنية التحتية الحيوية للمعلومات، كقطاعات الطاقة، والنقل، والتمويل، والاتصالات.
- يخضع مشغلو البنية التحتية الحيوية الحاسمة CIIS لالتزامات صارمة تتعلق بالأمن السيبراني، بما في ذلك متطلبات توطين البيانات، والتقييمات الأمنية، والامتثال للمعايير الوطنية.

6 لوائح إدارة محتوى الإنترنت

تحكم هذه اللوائح، التي تشرف عليها إدارة الفضاء الإلكتروني الصينية (CAC)، المحتوى عبر الإنترنت وتفرض إجراءات رقابة ومراقبة للتحكم في نشر المعلومات على الإنترنت. كما يُطلب من موفري الخدمات عبر الإنترنت مراقبة المحتوى وتصفيته، والامتثال لقيود المحتوى، والإبلاغ عن الأنشطة غير القانونية إلى السلطات.

7 اللجنة المركزية لشؤون الفضاء السيبراني

في إطار اللجنة المركزية للحزب الشيوعي الصيني، تم إنشاء اللجنة المركزية لشؤون الفضاء الإلكتروني لتطوير وتنفيذ السياسات المتعلقة بالإنترنت. ويُعتقد أن هذا يغطي المشكلات المتعلقة بأمن الإنترنت، ونمو الخدمات عبر الإنترنت، والسلطة الواسعة على لوائح الرقابة على الإنترنت.[50]

اليابـــان

1 قانون حماية المعلومات الشخصية (APPI)

تم إقرار قانون حماية المعلومات الشخصية APPI في عام ٢٠٠٥ والذي تم تعديله في عام ٢٠١٥، ويحكم كيفية استخدام الشركات والمنظمات الحكومية للبيانات الشخصية، ويجب على المؤسسات اتخاذ التدابير الأمنية اللازمة للحماية من الوصول غير المصرح به للبيانات الشخصية والكشف عنها وتعديلها وتدميرها.[51]

2

القانون الأساسي للأمن السيبراني (BAC)

ويضع هذا القانون الذي صدر في عام ٢٠١٤ إطارًا أساسيًّا لتدابير الأمن السيبراني في اليابان، ويؤكد أهمية الشراكات بين القطاعين العام والخاص وتبادل المعلومات والتعاون لمعالجة تهديدات الأمن السيبراني بشكل فعال.[52]

3

إرشادات أمان الشبكة

تصدر الحكومة اليابانية إرشادات أمان الشبكات لمؤسسات القطاعين العام والخاص، توفر هذه الإرشادات التوصيات وأفضل الممارسات لتأمين أنظمة المعلومات، ومنع الهجمات السيبرانية، والاستجابة للحوادث الأمنية.

4 حماية البنية التحتية الحيوية

تحدد اليابان قطاعات معينة مثل الطاقة والتمويل والنقل والاتصالات باعتبارها بنية تحتية حيوية تتطلب حماية معززة للأمن السيبراني، وتعمل الحكومة بشكل وثيق مع الصناعات ذات الصلة لتطوير وتنفيذ تدابير الأمن السيبراني لحماية البنية التحتية الحيوية من التهديدات السيبرانية.

5 استراتيجية الأمن السيبراني

- طورت اليابان استراتيجية وطنية للأمن السيبراني لتعزيز قدرات الأمن السيبراني في البلاد وقدرتها على مواجهة التهديدات السيبرانية، وتتضمن هذه الاستراتيجية مبادرات مثل: تعزيز التعليم والتوعية بالأمن السيبراني، وتعزيز التعاون الدولي، وتحسين قدرات الاستجابة للحوادث.
- استراتيجية الأمن السيبراني الحالية الصادرة في سبتمبر ٢٠٢١ هي الاستراتيجية الثالثة بموجب القانون الأساسي للأمن السيبراني. توضح استراتيجية الأمن السيبراني موقفًا أساسيًّا من سياسة الأمن السيبراني وأهدافها وتنفيذها لمدة ٣ سنوات محليًّا ودوليًّا.[53]

6 المركز الوطني للاستعداد للحوادث واستراتيجية الأمن السيبراني (NISC)

تم تأسيسه منذ عام ٢٠١٥، وكان يسمى سابقًا المركز الوطني لأمن المعلومات منذ عام ٢٠٠٥، تحت الاختصار نفسه "NISC"، كأمانة لمقر استراتيجية الأمن السيبراني، ويعمل جنبًا إلى جنب مع القطاعين العام والخاص في مجموعة متنوعة من الأنشطة لإنشاء "الفضاء السيبراني الحر العادل والآمن"، ويلعب المركز الوطني للاستعداد للحوادث واستراتيجية الأمن السيبراني دوره الرائد كنقطة محورية في تنسيق التعاون داخل الحكومة وتعزيز الشراكات بين الصناعة والأوساط الأكاديمية والقطاعين العام والخاص.[54]

7 مركز الأمن السيبراني الياباني (JCSIRT)

يقوم مركز الأمن السيبراني الياباني، الذي يديره المركز الوطني للاستعداد للحوادث واستراتيجية الأمن السيبراني (NISC)، بتنسيق أنشطة الاستجابة لحوادث الأمن السيبراني، ويوفر المعلومات والإرشادات حول تهديدات الأمن السيبراني، ويساعد المؤسسات في تحسين وضع الأمن السيبراني لديها.

8 قانون أعمال الاتصالات (TBA)

تنص المادة ٤ من TBA على أنه (١) لا يجوز انتهاك سرية الاتصالات التي تتعامل معها شركة اتصالات، و(٢) لا يجوز لأي شخص يشارك في أعمال الاتصالات أن يكشف الأسرار التي تم الحصول عليها في أثناء وجوده في منصبه.[55]

كوريـا

1 قانون حماية المعلومات الشخصية لعام ٢٠١١ (بصيغته المعدلة في عام ٢٠٢٠) (PIPA)

ينظم قانون حماية المعلومات الشخصية جمع البيانات الشخصية واستخدامها والإفصاح عنها ومعالجتها من قبل الكيانات الحكومية والخاصة، ويتم تطبيقه بالاشتراك مع قانون الشبكة على جميع حوادث انتهاك خصوصية البيانات، بما في ذلك الهجمات الإلكترونية وتسريب البيانات.

أهمية القانون

الغرض من هذا القانون هو حماية حرية الأفراد وحقوقهم، وكذلك تحقيق كرامة الأفراد وقيمتهم، من خلال وصف معالجة المعلومات الشخصية وحمايتها.

الجمهور المستهدف

- معالجات البيانات
- كيانات القطاع العام والخاص
- المنظمات الأجنبية التي تتعامل مع المعلومات الشخصية للمواطنين الكوريين[56]

2 قانون تعزيز استخدام شبكة المعلومات والاتصالات وحماية المعلومات (قانون الشبكة)

القانون الذي يغطي الأمن السيبراني في كوريا الجنوبية، ويفرض تدابير أمنية لشبكات المعلومات والاتصالات، ويتطلب الإبلاغ عن الحوادث، ويحدد العقوبات المفروضة على انتهاكات البيانات والفشل الأمني.

◈ أهمية القانون

تكمن أهمية قانون الشبكات في تعزيز استخدام شبكات المعلومات والاتصالات، وحماية المعلومات الشخصية للمستخدمين الذين يستخدمون خدمات المعلومات والاتصالات، وبناء بيئة آمنة وسليمة لشبكات المعلومات والاتصالات من أجل تحسين حياة المواطن.

◈ الجمهور المستهدف

- مقدمو ومستخدمو خدمات المعلومات والاتصالات
- الحكومة
- المنظمات
- هيئة الاتصالات الكورية[57]

3 قانون حماية المعلومات والبنية التحتية للاتصالات

يهدف هذا القانون إلى تشغيل البنية التحتية الحيوية للمعلومات والاتصالات بطريقة مستقرة من خلال صياغة وتنفيذ التدابير المتعلقة بحماية هذه البنية التحتية، استعداداً للاختراق بالوسائل الإلكترونية، وبالتالي المساهمة في سلامة الأمة واستقرار حياة الناس.

◈ أهمية القانون

يسعى القانون إلى تسهيل المزيد من تبادل معلومات البنية التحتية الحيوية بين مالكي ومشغلي البنى التحتية الحيوية والكيانات الحكومية التي تتحمل مسؤوليات حماية البنية التحتية، وبالتالي تقليل تعرض الدولة للإرهاب.

◈ الجمهور المستهدف

- وزير العلوم وتكنولوجيا المعلومات والاتصالات
- مدير جهاز المخابرات الوطني
- المنظمات الأمنية للدولة [58]

4 قانون العقوبات وتعزيز السياسات على كوريا الشمالية لعام ٢٠١٦

وفقًا للقانون، يجب على الحكومة المركزية والمحلية الكورية والبلديات وضع وتنفيذ سياسات لتشجيع صناعة الأمن السيبراني وإعداد التدابير لتخصيص الميزانيات لتحقيق تلك السياسات.

◈ أهمية القانون

- استخدام وسائل غير عسكرية لمعالجة الأزمة الموصوفة في القسم الفرعي (أ).
- توفير النفوذ الدبلوماسي للتفاوض بشأن التغييرات الضرورية في سلوك حكومة كوريا الشمالية.
- تخفيف معاناة شعب كوريا الشمالية.

◈ الجمهور المستهدف

حكومة كوريا الشمالية

5 قانون جهاز المخابرات الوطنية

هو قانون يتعلق بمجلس الأمن القومي، وينص على إنشاء مجالس أمن إقليمية لتحديد وتنسيق أنشطة الوكالات المسؤولة عن أمن الدولة وحماية والحفاظ على وحدة الدولة واستقرارها.

◈ أهمية القانون

يهدف هذا القانون إلى تسهيل مشروعات تجسيد الحكومة الإلكترونية، وتحسين الإنتاجية والشفافية والديمقراطية للوكالات الإدارية، وفي نهاية المطاف تحسين نوعية حياة المواطنين في عصر المعلومات المعرفية من خلال توفير المبادئ والإجراءات الأساسية وطرق الترويج وغيرها من المسائل ذات الصلة بالمعالجة الإلكترونية للأعمال الإدارية، والأداء الفعال لواجبات الأمن القومي.

◈ الجمهور المستهدف

الحكومة [59]

6 الاستراتيجية الوطنية للأمن السيبراني ٢٠١٩

في عام ٢٠١٩، أصدر مكتب الأمن القومي الرئاسي استراتيجية الأمن السيبراني الوطنية التي حددت تصميم شبكات الجيل الخامس ونشرها وإجراءات مكافحة الطائرات بدون طيار باعتبارها المجالات الأكثر أهمية لتركيز الحكومة، وكلاهما قضيتان جديدتان للتركيز على الأولوية في الأمن السيبراني والأمن القومي الكوري، وأدت هذه الاستراتيجية إلى مضاعفة الجهود لتعزيز مرونة البنية التحتية الرقمية في كوريا.

◈ أهمية الاستراتيجية

- تتمثل أهداف استراتيجية ٢٠١٩ في ضمان عمليات مستقرة للدولة، والرد على الهجمات السيبرانية، وبناء أساس قوي للأمن السيبراني في كوريا، كما تحدد الاستراتيجية ثلاثة مبادئ أساسية:
- تحقيق التوازن بين الحقوق الفردية والحاجة إلى تحسين الأمن السيبراني.
- القيام بالأنشطة الأمنية على أساس سيادة القانون.
- بناء نظام للمشاركة والتعاون بين أصحاب المصلحة المحليين ونظرائهم الأجانب.
- وتتمحور الاستراتيجية حول ست ركائز استراتيجية: البنية التحتية الحيوية الوطنية الآمنة، وتعزيز القدرات الدفاعية ضد الهجمات السيبرانية، والحوكمة القائمة على الثقة والتعاون، ونمو صناعة الأمن السيبراني، وتعزيز ثقافة الأمن السيبراني، وتعزيز التعاون الدولي.

◈ الجمهور المستهدف

- الحكومة
- الشركات
- المواطنون [60]

إستونيا

التواصل مع الاستراتيجيات الأخرى

- قام أصحاب المصلحة في مجال الأمن السيبراني في إستونيا، والذين يضمون الوكالات الحكومية والمؤسسات الأكاديمية ومراكز الفكر وقطاع الشركات، بإنشاء استراتيجية الأمن السيبراني، وهي وثيقة أفقية، تسعى إلى توفير صورة واسعة النطاق، والقضاء على الازدواجية، وضمان تطبيق المفاهيم من خلال الاستفادة من مجموعة متنوعة من اللاعبين والإجراءات. وتركز الاستراتيجية على القضايا التي تحتاج إلى التعاون بين أصحاب المصلحة ولها تأثير على الدولة والمجتمع. وتشمل مسؤولياتها الحفاظ على إطار عمل للأمن السيبراني، وتسهيل التواصل المثمر بين الصناعة والحكومة والأوساط الأكاديمية، وتعزيز مناخ الأعمال الصحي، وحماية الأمن القومي.
- **تتعامل الأجندة الرقمية ٢٠٢٠ لإستونيا** مع الأهداف المتعلقة بتطوير الدولة الإلكترونية، وضمان اتصالات البيانات والمهارات العامة لتكنولوجيا المعلومات والاتصالات ويتم تخطيط محتواها كعملية موحدة مع استراتيجية الأمن السيبراني[61].

- **وثيقة التخطيط الأساسية للدفاع الوطني هي خطة تطوير الدفاع الوطني ٢٠١٧ - ٢٠٢٦،** وتهدف إلى تحديد تطورات القدرات غير العسكرية والعسكرية المطلوبة والمتسقة مع قدرات الدولة للسنوات العشر القادمة، بناءً على سيناريوهات التهديد الحالية.

- ويعَد إنشاء قيادة إلكترونية و"التجنيد الإلكتروني" بالإضافة إلى نظرة عامة واسعة النطاق لتتبع الأحداث في الفضاء الإلكتروني في الوقت الفعلي، من أهم الأولويات السيبرانية في خطة تطوير الدفاع الوطني[62].

- **تهدف خطة تطوير الأمن الداخلي ٢٠١٥ - ٢٠٢٠** إلى تطوير قدرات مكافحة الجرائم الإلكترونية وتحديد الهجمات التي تهدد الأمن الداخلي لإستونيا، كما تتوافق مع استراتيجية الأمن السيبراني ٢٠١٤ - ٢٠١٧ وخطة تطوير الأمن الداخلي ٢٠٢١ - ٢٠٣٠، وتشمل مجالاتها الرئيسة تعزيز الكشف عن الجرائم الإلكترونية والتحقيق والاستعداد للتهديدات المستقبلية وتعزيز التعاون وتبادل المعلومات بين المؤسسات ونشر المعلومات وتحليل مواقف الجرائم الإلكترونية ومكافحة المبيعات غير القانونية عبر الإنترنت وتخفيف المخاطر المتعلقة بالإقامة الإلكترونية والهوية الرقمية[63].

- تم تحديد الأهداف طويلة المدى لسياسة العدالة الجنائية في مجالات تطوير سياسة العدالة الجنائية حتى عام ٢٠٣٠، وهي وثيقة تشمل مجالات أولوياتها مكافحة الجرائم الإلكترونية، والتقليل إلى أدنى حد من التسلط عبر الإنترنت[64].

- تهدف خطة تطوير السياسة الخارجية لإستونيا ٢٠٣٠ إلى ضمان الأمن السيبراني والاستجابة السريعة للتهديدات السيبرانية من خلال زيادة الوعي بموضوعات القانون الدولي، وتعزيز التعاون الإنمائي، والمشاركة بنشاط في شبكة المساعدة السيبرانية التابعة للاتحاد الأوروبي، وتؤكد الخطة أيضًا الحاجة إلى الثقة في الفضاء الإلكتروني.

- **تدعم خطة إستونيا للتعاون الإنمائي والمساعدات الإنسانية للفترة ٢٠١٦ - ٢٠٢٠** اعتماد حلول تكنولوجيا المعلومات والاتصالات والدولة الإلكترونية في البلدان النامية، وزيادة الوعي بإمكاناتها وضمان القدرة على مواجهة التهديدات السيبرانية[65].

- تضمن سياسة الأمن السيبراني في إستونيا استمرار الخدمات الأساسية والتعاون التشغيلي من خلال التوافق مع أهداف الاتحاد الأوروبي وحلف شمال الأطلسي. ومن خلال إعطاء الأولوية لمنع الحوادث وحلها، تتوافق سياسات الأمن السيبراني الإستونية مع حزمة الأمن السيبراني لعام ٢٠١٧ للاتحاد الأوروبي. كما أنه ومن خلال الانضمام إلى تعهد الدفاع السيبراني، تعهدت إستونيا وحلفاؤها بحماية الشبكات والبنية التحتية الوطنية مع تعزيز الأمن السيبراني لحلف شمال الأطلسي بشكل عام[66].

التنظيم والتنسيق الوطني لإدارة الأمن السيبراني

- تقوم وزارة الشؤون الاقتصادية والاتصالات بتنسيق تخطيط وتنفيذ سياسة الأمن السيبراني في إستونيا؛ مما يضمن التعاون مع الحكومة والمجتمع. ويتم تنفيذ أهداف استراتيجية الأمن السيبراني من خلال مجلس الأمن السيبراني التابع لحكومة الجمهورية، والذي يعمل مع المؤسسات الحكومية لتطوير السياسة. وتدير الوزارة إعداد وتنفيذ استراتيجية الأمن السيبراني كجزء من استراتيجية مجتمع المعلومات، وتعمل مع هيئة نظام معلومات الدولة (RIA) لتطوير المرونة التكنولوجية، وإدارة الأزمات، وتطوير المؤسسات في قطاع الأمن السيبراني، وتوجيه البحوث. كما تشمل الوكالات الأخرى المساهِمة في الأمن السيبراني الإستوني كلًّا من: هيئة المراقبة الفنية (TJA)، ومؤسسة الإنترنت الإستونية (EIS)، ومؤسسة اتصالات المعلومات الحكومية (RIKS)، ومؤسسة الإنترنت الإستونية (EIS)، ومؤسسة اتصالات المعلومات الحكومية (RIA)، ومؤسسة المشروعات الإستونية (EAS)، والشركات الناشئة الإستونية (SUE)، التي تدعم المشروعات والابتكار في هذا القطاع[68].

- تركز وزارة التعليم والبحث العلمي على استراتيجيات التعلم مدى الحياة لتزويد الخريجين بالمعرفة الأساسية لمكافحة التهديدات السيبرانية. وتدعم مؤسسة تكنولوجيا المعلومات للتعليم (HITSA) ذلك من خلال تنسيق برنامج Targalt Internetis وبرنامج أكاديمية تكنولوجيا المعلومات. وتتعاون وزارة العدل مع مكتب المدعي العام لتخطيط سياسة العدالة القضائية والجنائية واستراتيجيات الوقاية من العنف. وتشمل مؤسسات الأمن السيبراني الرئيسة مفتشية حماية البيانات (AKI)، والمعهد الإستوني لعلوم الطب الشرعي (EKEI)، ومركز السجلات ونظم المعلومات(RIK) . هذا، وتقوم وزارة الدفاع، بالتعاون مع قوات الدفاع ورابطة الدفاع وجهاز المخابرات الأجنبية، بتنفيذ أنشطة الدفاع العسكري، وتساهم في آليات التعاون والتنسيق عبر القطاعات[68].

- تتولى وزارة الداخلية، بالتعاون مع هيئة الشرطة وحرس الحدود وجهاز الأمن الداخلي، مسؤولية منع الجرائم الإلكترونية ومكافحتها واكتشافها. وهي تنفذ خطط تطوير الأمن الداخلي وتساهم في التعاون بين القطاعات. كما يقوم مركز تكنولوجيا المعلومات والتنمية (SMIT) بإدارة أنظمة المعلومات الأمنية المحلية. في حين تقوم وزارة الخارجية بتوجيه أنشطة التعاون الدولي. وتساهم وزارة المالية في تطوير الاستراتيجية؛ مما يضمن الاستدامة والتكامل مع عمليات التخطيط الأخرى. وتشرف هيئة الرقابة المالية على المؤسسات المالية، في حين يقوم بنك إستونيا بدمج الأمن السيبراني في وثائق التخطيط الدفاعي الوطني[70].

- تركز إستونيا على تعزيز أمنها السيبراني من خلال التعاون الوثيق مع مراكز الكفاءة ومراكز الفكر والجامعات ومؤسسات البحث وشركاء القطاع الخاص. وتستخدم الدولة مؤسسات الفكر والرأي كشركاء استراتيجيين لتطوير الكفاءة القطاعية والتعاون الدولي. تعمل إستونيا أيضًا على تعزيز تطوير مركز التميز للدفاع السيبراني التعاوني التابع لمنظمة حلف شمال الأطلسي (CCD COE) كمنظمة دولية. كما تدعم أكاديمية الحوكمة الإلكترونية (EGA) التبني الدولي للحلول الرقمية في إستونيا. ويستخدم المركز الدولي للدفاع والأمن (RKK) خبرة الخبراء الإستونيين في مجال الدفاع السيبراني لتطوير دفاع وطني شامل. كما يهدف مركز TalTech للطب الشرعي الرقمي والأمن السيبراني إلى زيادة كفاءة الأمن السيبراني في إستونيا من خلال التعليم والبحث والتطوير[71].

مصـــــر


مصر العربية

التعريف بالجرائم الإلكترونية وأنواعها

عرَّف مؤتمر الأمم المتحدة العاشر لمنع الجريمة السيبرانية ومعاقبة المجرمين "الجريمة السيبرانية" بأنها "أي جريمة يمكن ارتكابها عن طريق نظام حاسوبي أو شبكة حاسوبية، وتشمل تلك الجريمة، من حيث المبدأ، جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية"[72].

وبحسب التعريفات، فإن الجريمة الإلكترونية هي "أي فعل يستخدم أجهزة الكمبيوتر وأدوات الاتصال المعاصرة، مثل شبكة الإنترنت، لإلحاق ضرر جسيم بالأفراد أو الجماعات أو المؤسسات، بهدف ابتزاز الضحية وتشويه سمعتها من أجل تحقيق مكاسب مادية أو خدمة أهداف سياسية"[73].

ومن المؤكد أن هناك العديد من أنواع الجرائم الإلكترونية الأخرى التي تستهدف الأشخاص والمنظمات والدول والمجموعات، وتنقسم فئات هذه الجرائم بشكل تفصيلي على النحو التالي:

١- **الجرائم التي تستهدف الأفراد:** تنطوي على الحصول على معلومات حساسة من حساباتهم، مثل حسابات البنك أو الإنترنت، لتحقيق مكاسب مادية أو تشويه سمعتهم أو تعطيل العلاقات. ويمكن أن تنطوي هذه الجرائم على أنشطة غير قانونية مثل الدعارة وتهريب المخدرات وغسل الأموال والجرائم الإلكترونية الأخرى[74].

٢- **الجرائم التي تستهدف المؤسسات:** تتسبب الجرائم الإلكترونية في خسائر كبيرة للمؤسسات والشركات، وتتمثل في خسائر مادية وأنظمة، منها:

أ- اختراق الأنظمة والوصول غير المصرح به إلى شبكات الشركة، والحصول على معلومات قيمة، واستخدامها لتحقيق مكاسب شخصية، وسرقة الأموال، وتدمير أنظمة الإدارة؛ مما يؤدي إلى خسائر كبيرة[75].

ب- اختراق المواقع الإلكترونية والسيطرة عليها، ومن ثَمَّ استخدامها لخدمة مصالح جهات خطيرة تهدف إلى زعزعة أمن البلاد والسيطرة على عقول الشباب وتحريضهم على القيام بأعمال غير مشروعة[76].

ت- غالبًا ما يكون تدمير النظام بسبب الفيروسات الإلكترونية؛ مما يسبب الفوضى ويؤدي إلى خسائر كبيرة في الملفات وأهميتها في إدارة وتنظيم الشركة[77].

ا- **الجرائم التي تستهدف المال:**

أ- الاستيلاء على الحسابات المصرفية: وهي جرائم تهدف إلى الاستيلاء على الأموال والممتلكات عن طريق اختراق الحسابات المصرفية والحسابات المتعلقة بمؤسسات الدولة والمؤسسات الخاصة الأخرى[78].

ب- انتهاك حقوق الملكية الفكرية والأدبية: وهي صناعة نسخ غير أصلية من البرامج وملفات الوسائط المتعددة ونشرها عبر شبكة الإنترنت، وهذا يسبب خسائر فادحة في مؤسسات تصنيع البرمجيات والصوتيات[78].

ا- **الجرائم التي تمس الأمن القومي:** هذه هي جرائم المعلومات؛ حيث تكون الدولة هي الضحية، وقد تمكَّن الجاني من الوصول إلى حساب خاص، أو موقع ويب أو بريد إلكتروني أو نظام معلومات خاص أو اختراقه إما ليديره هو أو لصالح الدولة أو لكيان قانوني عام أو متصل به. ومن أمثلة هذه الجرائم التجسس والتحريض على الإرهاب ضد مصالح البلاد باستخدام بيانات مأخوذة من ملفات أجهزة الدولة[80].

الأبعاد القانونية للأمن السيبراني في مصر

- مصر تحتل المركز التاسع في مؤشر الأمن السيبراني العالمي٢٠٢٠ (GCI)[81]، استناداً إلى جدول أعمال الأمن السيبراني العالمي للاتحاد الدولي للاتصالات (GCA)، وهو إطار للتعاون الدولي يهدف إلى تعزيز الثقة والأمن في مجتمع المعلومات. يصنف مؤشر الأمن السيبراني العالمي GCI قدرات الأمن السيبراني للدول في خمس فئات: التدابير القانونية، والتدابير الفنية، والتدابير التنظيمية، وبناء القدرات والتعاون. ويهدف GCI إلى تعزيز استراتيجيات الحكومة الوطنية، ودفع جهود التنفيذ، ودمج الأمن في التقدم التكنولوجي، وتعزيز ثقافة الأمن السيبراني العالمية[82].

١- الإطار القانوني والكيانات التشريعية

- **المجلس الأعلى المصري للأمن السيبراني ٢٠١٤ (ESCC)**

أسسه مجلس الوزراء المصري في ديسمبر ٢٠١٤؛ لحماية معلومات وبيانات السلطات، وضمان تمويل أنظمة الأمن السيبراني، وتوضيح الإطار التشريعي، ويضم المجلس وزير الاتصالات وتكنولوجيا المعلومات رئيسًا وممثلين عن الوزارات المختلفة. وفي عام ٢٠١٥ تمت إضافة ممثلين عن وزارة المالية والتخطيط والمتابعة والإصلاح الإداري. وفي عام ٢٠١٦، تم تعيين ممثل عن رئاسة الجمهورية لوضع استراتيجية لمواجهة التهديدات السيبرانية والإشراف على تنفيذها. في مايو ٢٠١٧، نُشر قرار يلزم جميع الجهات الحكومية وشركات قطاع الأعمال العام بتنفيذ قرارات المجلس وتوصياته بشأن تأمين البنية التحتية الحيوية لتكنولوجيا المعلومات والاتصالات وتنفيذ استراتيجية الأمن الوطني[83].

- **الاستراتيجية الوطنية للأمن السيبراني ٢٠١٧ – ٢٠٢١**

هي وثيقة أعدتها الحكومة المصرية لدعم الأمن القومي وتنمية المجتمع، وتهدف إلى رصد ومواجهة التهديدات والتحديات الناشئة في الفضاء السيبراني والمجتمع الرقمي. وقد تم تطوير الاستراتيجية استجابةً لإنشاء المجلس الأعلى للأمن السيبراني في مصر (ESCC)، الذي تم تكليفه بوضع استراتيجية شاملة لحماية البنية التحتية لتكنولوجيا المعلومات والاتصالات. وتتضمن الاستراتيجية برامج تدعم الأهداف الاستراتيجية للأمن السيبراني، وتسلط الضوء على أدوار الجهات الحكومية والقطاع الخاص ومؤسسات الأعمال والمجتمع المدني، وقد تضمنت خطة عمل للأعوام ٢٠١٧ - ٢٠٢١، مع التأكيد على أهمية الشراكة بين هذه الجهات. إن تحقيق هذه الأهداف سيمهد

الطريق أمام اقتصاد رقمي متكامل، يلبي تطلعات المواطنين في التنمية الاجتماعية والاقتصادية، ويحمي رفاهية الفرد، ويساهم في تقدم البلاد وازدهارها[84].

المركز المصري للاستجابة لطوارئ الكمبيوتر (EG-CERT)

تم إنشاء المركز المصري للاستجابة لطوارئ الكمبيوتر (CERT) في عام ٢٠٠٩ من قبل الجهاز القومي لتنظيم الاتصالات (NTRA) لتقديم الدعم الفني على مدار ٢٤ ساعة لحماية البنية التحتية الحيوية للمعلومات. ومنذ عام ٢٠١٢، يدعم المركز مختلف القطاعات، بما في ذلك تكنولوجيا المعلومات والاتصالات، والخدمات المصرفية، والحكومة، لمكافحة تهديدات الأمن السيبراني، بما في ذلك هجمات الحرمان من الخدمة. ويتكون المركز من أربعة أقسام رئيسة: مراقبة المخاطر، وتحليل الأدلة السيبرانية، وتحليل البرمجيات الخبيثة، وفحص نقاط الضعف، واختبار الاختراق. وتتمثل مهمته في توفير نظام إنذار مبكر ضد البرمجيات الخبيثة واسعة النطاق والهجمات الإلكترونية على البنية التحتية الحيوية للمعلومات في مصر. كما يهدف المركز إلى تطوير الإطار التشريعي للأمن السيبراني، وإنشاء البنية التحتية للتعاملات الإلكترونية وحماية الهوية الرقمية، وجمع وتحليل معلومات الحوادث الأمنية، والتنسيق والتوسط بين الأطراف، والتعاون مع فرق دولية[85].

البنية التحتية للمعلومات الحيوية المصرية

تركز إدارة حماية البنية التحتية للمعلومات الحيوية وخطط الطوارئ على حماية المعلومات في القطاعات الحيوية من خلال دراسة احتياجاتها وتنفيذ معايير الأمن السيبراني، وتقوم بتطوير استراتيجيات وأطر الحماية من خلال الشراكات. كما تهدف إدارة التوعية السيبرانية إلى رفع مستوى الوعي حول الأمن السيبراني وأمن المعلومات، بمشاركة الوزارات والجهات الحكومية والشركات والبنوك وقطاعات الاستثمار وفئات المجتمع. هذا، وتشمل الحملات التوعوية جلسات ودورات تدريبية ومنشورات وفيديوهات وإعلانات والمشاركة في الأنشطة المدرسية والجامعية[86].

وزارة الاتصالات وتكنولوجيا المعلومات (MCIT)

تعمل وزارة الاتصالات وتكنولوجيا المعلومات (MCIT) على بناء بنية تحتية رقمية آمنة وموثوقة ويمكن الوصول إليها في مصر. وهي تعطي الأولوية للحفاظ على بنية تحتية قوية، وتطوير التقنيات، وحماية الإطار التنظيمي لنمو قطاع تكنولوجيا المعلومات والاتصالات. الجهاز القومي لتنظيم الاتصالات (NTRA) هو هيئة تنظيمية مستقلة تشرف على قطاع الاتصالات وتحسين الخدمات وتوسيع الاستخدام[87].

تكنولوجيا المعلومات والاتصالات (ICT)

شهد قطاع تكنولوجيا المعلومات والاتصالات في مصر نموًّا بنسبة ١٦٪ في العام المالي ٢٠٢٠/٢٠٢١، ليساهم بنسبة ٥٪ من الناتج المحلي الإجمالي للبلاد. وتقوم الحكومة بتنفيذ استراتيجية تكنولوجيا المعلومات والاتصالات ٢٠٣٠، مع التركيز على بناء القدرات، وتصميم الإلكترونيات، والتصنيع، ومجمعات التكنولوجيا. وتقوم وزارة الاتصالات وتكنولوجيا المعلومات بتدريب ١٠٠ ألف شاب مصري وتطوير مهارات تكنولوجيا المعلومات والاتصالات لديهم[88].

٢- **تنفيذ القوانين وفعالية التشريعات**

1 قانـــون مكافحـــة الجرائـــم الإلكترونية وجرائـــم تكنولوجيـــا المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨

الغرض من هذا القانون هو تنظيم أنشطة الإنترنت واستكمال قوانين الإعلام والصحافة في مصر. وقد أكد هذا القانون بشكل عميق على أنشطة وسائل الإعلام والصحافة، لا سيما معاقبة إنتاج الأخبار المزيفة، والأنشطة غير المرخصة عبر الإنترنت، وما إلى ذلك.

نظرة عامة على القانون[88]

يتكون القانون من ٤٥ مادة، ويتولى القانون الهيئة القومية لتنظيم الاتصالات في مصر، والوزير المختص هو وزير الاتصالات وتكنولوجيا المعلومات في مصر.

فالقانون موجه إلى:

١- الأشخاص الطبيعيين والاعتباريين

٢- مديري الأشخاص الاعتباريين

٣- مقدمي خدمات الإنترنت

٤- مسؤولي الويب

٥- مسؤولي الدولة

يعاقب القانون على جرائم مختلفة مثل الجرائم المتعلقة بـ:

١- تجاوز حق الوصول

٢- التعدي على أمن الشبكات وأنظمة وتقنيات المعلومات

٣- التعدي على تصميم المواقع

٤- التعدي على نظم معلومات الدولة

٥- التعرض لسلامة شبكة المعلومات

٦- انتهاك الخصوصية، ومحتوى المعلومات غير القانوني[80]

- **التعدي على أمن شبكات وأنظمة وتقنيات المعلومات:** أقرت المادة ١٣ من الفصل الأول جريمة الانتفاع بغير حق من خدمات الاتصالات والمعلومات؛ فإذا أساء شخص استخدام أنظمة الشبكات أو تكنولوجيا المعلومات في الاتصالات أو البث المسموع أو المرئي، فيمكن أن يواجه الحبس لمدة تصل إلى ثلاثة أشهر وغرامة تتراوح من عشرة آلاف جنيه مصري إلى خمسين ألف جنيه مصري، حسب الجريمة.
- **جرائم الغش والتعدي على نظم وتقنيات المعلومات:** تحدد المادة ٢٣ من الفصل الثاني من قانون العقوبات المصري عقوبات الجرائم الواقعة على بطاقات الائتمان والخدمات وأدوات الدفع الإلكتروني. سيواجه الأفراد المخالفون الذين يصلون إلى بيانات الاعتماد المصرفية أو طرق الدفع الإلكتروني السجن لمدة تصل إلى ثلاثة أشهر وغرامة تتراوح بين ٣٠ ألفًا إلى ٥٠ ألف جنيه مصري. وإذا ارتكبت الجريمة للحصول على أموال أو خدمات من طرف ثالث، يمكن الحكم بالسجن لمدة ستة أشهر وغرامة من ٥٠ ألفًا إلى ١٠٠ ألف جنيه مصري. وإذا استولى الشخص على أموال أو خدمات من طرف ثالث، فسيواجه السجن لمدة عام وغرامة قدرها ١٠٠ ألف جنيه مصري[81].
- **الجرائم المتعلقة بانتهاك الخصوصية والمحتوى غير القانوني:** تحدد المادة ٢٥ من الفصل الثالث من قانون مكافحة الجرائم الإلكترونية المصري عقوبات انتهاك المبادئ الأسرية، أو بيع البيانات الخاصة دون موافقة، أو إرسال رسائل بريد إلكتروني دون موافقة، أو نشر معلومات أو صور شخصية دون علم. وتتراوح العقوبات من الحبس لمدة عام إلى الغرامة من ٥٠ ألف جنيه إلى ٢٠٠ ألف جنيه. وإذا ارتكبت ضد شخص اعتباري عام، يمكن أن تكون العقوبة مزيجًا من الاثنين معًا. تعتبر هذه الجرائم حاسمة في قانون مكافحة الجرائم الإلكترونية المصري، الذي يعتبرها جرائم كبيرة.
- **زيادة مسؤولية مسؤولي ومديري الويب:** يحدد القانون مسؤولية مسؤولي الويب ومديري النطاق عن الجرائم التي يرتكبونها. وتتناول المادة ٢٧ الجرائم التي يرتكبها القائمون على الموقع، ومعاقبتهم بالحبس لمدة تصل إلى سنتين وغرامة تتراوح بين ٥٠ ألف جنيه مصري إلى ٣٠ ألف جنيه مصري. وتنص المادة ٢٩ على أنه في حالة تعرض موقع إلكتروني أو حساب خاص لجريمة، يمكن أن يواجه الشخص الحبس لمدة تصل إلى سنة وغرامة تتراوح من ٢٠ ألف جنيه مصري إلى ٢٠٠ ألف جنيه مصري. وفي حالة الإهمال، يمكن أن يواجه الشخص السجن لمدة تصل إلى ستة أشهر وغرامة تتراوح من ١٠ آلاف إلى ٢٠٠ ألف جنيه مصري. وتحدد المادة ٣٥ المسؤولية الجنائية للأشخاص الاعتباريين، ومعاقبتهم إذا علموا بوقوع جريمة ولم يبلغوا السلطة المختصة. وإذا كان المدير على علم بالجريمة أو قام بتسهيلها لتحقيق مكاسب شخصية أو طرف ثالث، فسوف يواجه عقوبة مماثلة لمرتكب الجريمة الأصلي.
- وقد أثارت الأحكام كما ذكرنا النقاش العام وكان سؤالهم هو: هل سيواجه مديرو أو مالكو أي موقع مسؤولية جنائية عن أي جريمة يرتكبها المستخدمون؟

وفقًا لبعض الناس، يمكن أن يحاكمهم القانون. ومع ذلك، يمكن القول إن المادة ٢٧ تعطي نطاقًا واسعًا جدًّا لجرائم الدولة. وبالتالي، فإن الكثير من الأفعال تقع ضمن نطاق هذه الجريمة، على الرغم من أنه من منظور عام، لا يمكن التعامل معها على أنها جريمة جنائية. على الرغم من ذلك، يمكن أن يؤدي النطاق الواسع للمادة ٢٧ أيضًا إلى تحميل مسؤولي الويب المسؤولية عن مثل هذه الأفعال التي تكون خارجة عن سيطرة الشخص من الناحية الفنية[82].

2 قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠

يهدف قانون حماية البيانات المصري إلى تنظيم التعامل مع البيانات الشخصية وإدارتها، باستثناء تلك التي يتعامل معها البنك المركزي المصري والجهات التابعة له. دخل القانون حيز التنفيذ في ١٥ أكتوبر ٢٠٢٠، مع فترة سماح مدتها ٢١ شهرًا للشركات للامتثال له. ويجب على الشركات تعيين مسؤول لحماية البيانات أو دفع غرامة قدرها ٢ مليون جنيه مصري (حوالي ١٢٥ ألف دولار). كما يتطلب القانون الحصول على ترخيص لمعالجة البيانات والتحكم فيها والتعامل مع البيانات الحساسة والتسويق الإلكتروني ونقل البيانات عبر الحدود. يمكن أن تؤدي الانتهاكات إلى فرض غرامات شديدة على مراقبي البيانات ومعالجيها، بمن في ذلك المواطنون المصريون والمواطنون الأجانب والأجانب المقيمون في مصر. وهناك أربعة أعمال تؤدي إلى السجن تشمل: خرق شروط نقل البيانات عبر الحدود، والتعامل مع البيانات الحساسة دون موافقة، وخرق القانون من قبل معالجي البيانات، ومنع ممثلي مراكز حماية البيانات من أداء واجباتهم.

3 قانون تنظيم الاتصالات القومي رقم ١٠ لسنة ٢٠٠٣ (الجهاز القومي لتنظيم الاتصالات)

يهدف الجهاز القومي لتنظيم الاتصالات إلى تنظيم قطاع الاتصالات وتطوير ونشر جميع خدماته بما يواكب أحدث التقنيات ويلبي جميع احتياجات المستخدمين بأنسب الأسعار، ويشجع الاستثمار الوطني والدولي في هذا المجال في إطار حرية الوصول[83].

ويمكن تلخيص الأهداف الرئيسة للهيئة فيما يلي:

١- التأكد من وصول خدمات الاتصالات إلى جميع مناطق الجمهورية.

٢- حماية الأمن الوطني والمصالح العليا للدولة.

٣- ضمان الاستخدام الأمثل للطيف الترددي وتعظيم إنتاجه.

٤- التأكد من الالتزام بأحكام الاتفاقيات الدولية النافذة والقرارات الصادرة عن المنظمات الدولية والإقليمية المعتمدة لدى الدولة.

٥- مراقبة تحقيق برامج الكفاءة الفنية والدراسات الاقتصادية لخدمات الاتصالات المختلفة[84].

اختصاصات الهيئة:

١- وضع الخطط واللوائح والقواعد اللازمة لإدارة سوق الاتصالات وتنظيم العلاقة بين أصحاب المصلحة في القطاع.

٢- منح التصاريح والتراخيص اللازمة للمشغلين لتقديم خدمات الاتصالات.

٣- تحديد معايير جودة الخدمة التي يجب أن يتوافر فيها المستخدم المصري.

٤- مراقبة السوق للتأكد من تطبيق معايير المنافسة العادلة وجودة الخدمات والحفاظ على حقوق المستخدمين.

٥- التحكيم وحل المنازعات التي قد تنشأ بين مشغلي الاتصالات، أو بينهم وبين المستخدمين.

٦- التأكد من مراعاة المعايير الصحية والبيئية في التقنيات المطبقة والمستخدمة في السوق المصرية[85].

4 قرار رئيس مجلس الوزراء رقم ٩٩٤ لسنة ٢٠١٧

كلف المجلس الأعلى للأمن السيبراني جميع الجهات الحكومية والشركات العامة بتنفيذ قراراته وتوصياته بشأن تأمين البنية التحتية الحيوية للاتصالات وتكنولوجيا المعلومات. ويتولى وزير الاتصالات وتقنية المعلومات وضع قواعد وإجراءات تأمين قطاعات الدولة وتنفيذ توصيات المجلس. وقد تؤدي انتهاكات هذه القرارات إلى عقوبات جنائية، وقد يواجه الموظفون أو العمال الذين ينتهكون هذه الإرشادات إجراءات تأديبية. ويعَد هذا الالتزام بالأمن السيبراني أمرًا بالغ الأهمية لمنع المخاطر والهجمات السيبرانية[86].

5 قانون تنظيم التوقيع الإلكتروني وإنشاء هيئة صناعة تكنولوجيا المعلومات رقم ١٥ لسنة ٢٠٠٤

يعَد قانون تنظيم التوقيع الإلكتروني أول تشريع في مصر ينظم المعاملات الإلكترونية، بما يضمن حقوق العملاء ومصداقيتهم، فهو يسمح للوسائل الإلكترونية بتحرير المستندات وتبادلها وحفظها مع الحفاظ على الشرعية، وأنشأ القانون هيئة تنمية صناعة تكنولوجيا المعلومات لإحداث نقلة نوعية في صناعة تكنولوجيا المعلومات في مصر وبناء القدرة التنافسية لتصدير تكنولوجيا المعلومات وتطبيقاتها. في السابق، لم تكن الكتابة والتوقيعات الإلكترونية دليلاً صحيحًا أمام القضاء.

6 قانون رقم ٩٤ لسنة ٢٠١٥ لمكافحة الإرهاب

يتناول القانون مسألة مغادرة الإرهابيين أوطانهم للقتال إلى جانب الجماعات الإرهابية، وتوسيع نطاق التجريم لتسهيل الانضمام أو التعاون أو عبور الآخرين خارج البلاد. كما تعمل على الترويج لارتكاب الجرائم والأفكار الإرهابية وتجريم العنف والتصدي للإرهاب السيبراني بما يتماشى مع قرار مجلس الأمن رقم ٢١٧٨ لسنة ٢٠١٤[87].

٣- الاتفاقيات والمعاهدات

اتفاقية الاتحاد الإفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية | اتفاقية مالابو

تعَد اتفاقية مالابو، التي اعتمدها الاتحاد الإفريقي في عام ٢٠١٤، بمثابة إطار قانوني لمكافحة الجرائم الإلكترونية وحماية البيانات في إفريقيا؛ فهو يجرم الأنشطة السيبرانية مثل القرصنة والاحتيال وسرقة الهوية، ويضع إجراءات التحقيق والملاحقة القضائية، ويفوض سلطات حماية البيانات. وتؤكد الاتفاقية على التعاون الدولي في مكافحة الجرائم الإلكترونية وحماية البيانات الشخصية. كما أنها تحدد الأحكام الجنائية المتعلقة بهجمات أنظمة الكمبيوتر، وانتهاكات البيانات، والجرائم المتعلقة بالمحتوى، والتدابير الأمنية للرسائل الإلكترونية. هذا، ويمكن أن يؤدي عدم الامتثال لهذه الضوابط إلى فرض عقوبات وغرامات على تكنولوجيا المعلومات والاتصالات. وفي هذا الإطار، فإنه يجب تثقيف الموظفين حول حماية البيانات ومراقبتهم بانتظام بحثًا عن الجرائم الإلكترونية وانتهاكات البيانات. إن فهم اتفاقية مالابو يمكن أن يساعد الشركات والأفراد على حماية بياناتهم وأنظمتهم ضد التهديدات السيبرانية[88].

خـــاتمـــة

يعتمد النهج الذي تتبناه مصر في مكافحة الإرهاب السيبراني على مناهج أمنية وتعليمية ومؤسسية وثقافية برعاية رئاسية. ودعا الرئيس السيسي إلى تبني منظور إصلاحي شامل لحماية الشباب من الإرهاب السيبراني واعتماد ركيزة ثقافية، حيث أطلق مبادرة تتعلق بجرائم تقنية المعلومات ووجه لاتفاقيات إقليمية ودولية. ونظرًا للتهديدات السيبرانية العديدة، قامت مصر بتوسيع قوانين مكافحة الإرهاب، وإنشاء مؤسسات وطنية وإقليمية متخصصة في الأمن السيبراني، وأجرت برامج تدريبية لرفع مستوى الوعي بين موظفي الحكومة والأطفال والنساء والأشخاص ذوي الإعاقة. وسيتم تشكيل فرق لتحليل الأدلة الرقمية من الأجهزة الإلكترونية، وسيتم إنشاء وحدات للأمن السيبراني في كل جهة حكومية. ويعَد التعاون الدولي عنصرًا أساسيًّا في جهود مصر، خاصة مع التطورات التكنولوجية السريعة وتأثير التكنولوجيات مثل: الذكاء الاصطناعي، وإنترنت الأشياء، والجيل الخامس.

التوصيات

١- تحسين قدرات الاستفادة من التقنيات الجديدة والناشئة في مكافحة الجرائم الإلكترونية، وتحسين فعالية الاستخبارات مفتوحة المصدر (OSINT) والتحقيقات الجنائية الرقمية، وتعزيز قدرات الهيئات التنفيذية والمؤسسية لمنع استغلال التكنولوجيات الجديدة. والتكنولوجيات الناشئة لأغراض إرهابية.

٢- تعزيز قدرة الدول المصرية على وقف الهجمات الإلكترونية التي تشنها الجماعات الإرهابية على البنية التحتية الحيوية، وتقليل آثار تلك الهجمات في حالة حدوثها، واستعادة الأنظمة المتضررة.

٣- الاستخدام المكثف لوسائل التواصل الاجتماعي لجمع البيانات مفتوحة المصدر والأدلة الرقمية لمكافحة التطرف العنيف والإرهاب والابتزاز والعنف وسرقة المعلومات أو انتهاكات حقوق الملكية الفكرية، مع ضمان الالتزام الكامل بالمعايير القانونية وحقوق الإنسان عند وضع مختلف التدابير المضادة، واستراتيجيات الجرائم السيبرانية في مكانها الصحيح.

٤- تعزيز تدابير الدفاع السيبراني من خلال توسيع قدرات الإنذار المبكر من خلال شبكات واسعة النطاق من نقاط المراقبة وأجهزة الاستشعار، فمن ناحية تفعيل عمليات مراقبة الشبكة الحاسمة وتقييم نقاط القوة والضعف فيها، ومن ناحية أخرى، المشاركة في تدريبات عربية وإقليمية مكثفة لتحسين فعالية فرق الدفاع السيبراني والاستجابة السريعة وتبادل الخبرات.

٥- إنشاء "مجمع استخبارات إلكتروني" لجمع وتبادل البيانات الاستخباراتية مع الدول الأخرى في الوقت الحقيقي. وهذا قد يشمل أكثر من مجرد تتبع المواقع الإرهابية وجمع البيانات الاستخبارية؛ إذ إنه سيشمل جمع الأدلة الإلكترونية حول الهجمات والتهديدات الإلكترونية المحتملة.

٦- رفع القدرات المطلوبة لإنشاء وتنفيذ الاستراتيجيات المصرية المرتبطة بمواجهة الجرائم الإلكترونية، وكذلك رفع مستوى الوعي بالتهديد الذي يشكله الأمن السيبراني وسبل مواجهته باستخدام التقنيات المتطورة.

٧- نشر أحدث التصحيحات الأمنية وتحديث مجموعة متنوعة من الأنظمة والتطبيقات بشكل منتظم لمنع المتسللين ومجرمي الإنترنت والجماعات الإرهابية من استخدام العيوب الأمنية المعروفة للوصول إلى الأنظمة.

المراجـــــع

1 - The Legal Landscape of Cybersecurity: Protecting Digital Frontiers - Aditya Kumar Mishra – September 27,2023 – retrieved from https://www.linkedin.com/pulse/legal-landscape-cybersecurity-protecting-digital/

2 - What is Cyber Security? Definition and Best Practices – law review - retrieved from https://www.itgovernance.co.uk/what-is-cybersecurity

3 - DEFINITION cybersecurity – by Sharon shea Executive Editor – Alexander S. Gillis, technical writer and editor – Tech Accelerator – retrieved from https://www.techtarget.com/searchsecurity/definition/cybersecurity

4 - The AFRICAN UNION CONVENTION ON CYBERSECURITY : A REGIONAL RESPONSE TOWARDS CYBER STABILITY ? – by UCHENNA JEROME ORJI – September 2018 – masaryk university journal of law and technology – retrieved from https://www.researchgate.net/publication/327986841_The_African_Union_Convention_on_Cybersecurity_A_Regional_Response_Towards_Cyber_Stability

5 - "The information which can be accessed any time whenever authorized users want. There are primarily two dangers to the accessibility of the system which are as per the following: Denial of Service, Loss of Data Processing Capabilities"

6 - "The maintaining of consistency, accuracy, and completeness of the information is known as Integrity. Information cannot be modified in an unapproved way. For example, in an information break that compromises the integrity, a programmer might hold onto information and adjust it prior to sending it on to the planned beneficiary. Some security controls intended to keep up with the integrity of information include Encryption, Controls of Client access, Records Control, Reinforcement, recovery methodology, and Detecting the error".

7 - "The protection of information of authorized clients which allows them to access sensitive information is known as Confidentiality. For example, assuming we say X has a password for my Facebook account yet somebody saw while X was doing a login into the Facebook account. All things considered, my password has been compromised and Confidentiality has been penetrated"

8 - Network Security Strategies: There are numerous strategies to further develop network security and the most well-known network security parts are as per following: Firewalls, Antivirus, Email Security, Web Security, Wireless Security.

9 - Network Security Software: There are different types of tools that can shield a computer network like Network firewall, Cloud application firewall, Web application firewall, etc.

10 - What are the five elements of a good cyber security culture? – September 5,2023- the security company (international) limited – retrieved from https://www.linkedin.com/pulse/what-five-elements-good-cyber-security-culture-thesecurityco/

11 - Elements of cybersecurity – greeksforgreeks – retrieved from https://www.geeksforgeeks.org/elements-of-cybersecurity/

12 - Cyber resiliency, NIST Computer security resource center, CSRC, retrieved from - https://csrc.nist.gov/glossary/term/cyber_resiliency

13 - About International Telecommunication Union (ITU), ITU UN Agency website, retrieved from - https://www.itu.int/en/about/Pages/default.aspx

14 - Service GD, 'Data Protection' (GOV.UK, 16 September 2015) https://www.gov.uk/data-protection#:~:text=The%20Data%20Protection%20Act%202018%20is%20the%20UK's%20implementation%20of, used%20fairly%2C%20lawfully%20and%20transparently, accessed 9 April 2024.

15 - Service GD, 'Data Protection' (GOV.UK, 16 September 2015) https://www.gov.uk/data-protection#:~:text=The%20Data%20Protection%20Act%202018%20is%20the%20UK's%20implementation%20of, used%20fairly%2C%20lawfully%20and%20transparently, accessed 9 April 2024.

16 - 'The Network and Information Systems Regulations 2018' (Legislation.gov.uk) https://www.legislation.gov.uk/uksi/2018/506/contents/made, accessed 9 April 2024

17 - 'Review of the Computer Misuse Act 1990: Consultation and Response to Call for Information (Accessible)' (GOV.UK) https://www.gov.uk/government/consultations/review-of-the-computer-misuse-act-1990/review-of-the-computer-misuse-act-1990-consultation-and-response-to-call-for-information-accessible, accessed 9 April 2024

18 - https://ico.org.uk/for-organisations/guide-to-eidas/what-is-the-eidas-regulation/#:~:text=The%20UK%20eIDAS%20Regulations%20set,certificate%20services%20for%20website%20authentication.

19 - 'What Are PECR?' (ICO) https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guide-to-pecr/what-are-pecr/, accessed 9 April 2024

20 - 'Executive Order on Improving the Nation's Cybersecurity' (The White House, 12 May 2021) https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/, accessed 29 February 2024

21 - 1798.140. "(c) (A) Has annual gross revenues in excess of twenty-five million dollars ($25,000,000), as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185. (B) Alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices. (C) Derives 50 percent or more of its annual revenues from selling consumers' personal information".

22 - Cal. Civ. Code § 1798.100. "(e) A business that collects a consumer's personal information shall implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure in accordance with Section 1798.81.5."

23 - 1798.100. "(a) A consumer shall have the right to request that a business that collects a consumer's personal information disclose to that consumer the categories and specific pieces of personal information the business has collected".

24 - 1798.105. "(a) A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer".

25 - 1798.120. "(a) A consumer shall have the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information. This right may be referred to as the right to opt-out".

26 - 1798.125. "(a) (1) A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this title, including, but not limited to, by: (A) Denying goods or services to the consumer....."

27 - 1798.150" (a) (1) Any consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following: (A) To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater (b)....."

28 - Technology FO of, 'Gramm-Leach-Bliley Act' (Federal Trade Commission, 5 February 2024) <https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act> accessed 9 April 2024

29 - ——, 'Gramm-Leach-Bliley Act' (Federal Trade Commission, 5 February 2024) <https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act> accessed 9 April 2024.

30 - 'Cybersecurity and Infrastructure Security Agency: CISA' (Cybersecurity and Infrastructure Security Agency CISA, 19 April 2024) https://www.cisa.gov/news-events/alerts/2018/11/19/cybersecurity-and-infrastructure-security-agency, accessed10 April 2024

31 - "Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA): CISA' (Cybersecurity and Infrastructure Security Agency CISA) <https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber- incident-reporting-critical-infrastructure-act-2022-circia#: -:text-Enactment%20of%20CIRCIA%20marked%20an,and%20ransomware%20payments%20to%20CISA

32 - 'Cybersecurity' (SEC Emblem, 24 April 2017) <https://www.sec.gov/securities-topics/cybersecurity> accessed 8 April 2024

33 - THE INFORMATION TECHNOLOGY ACT, 2000 ACT NO. 21 OF 2000 - India – retrieved from https://www.indiacode.nic.in/bitstream/123456789/1999/1/A2000-21%20%281%29.pdf

34 - Chapter 1 point 2, page 5, THE INFORMATION TECHNOLOGY ACT, 2000 ACT NO. 21 OF 2000 - India – retrieved from https://www.indiacode.nic.in/bitstream/123456789/1999/1/A2000-21%20%281%29.pdf

35 - Chapter 9 (PENALTIES, COMPENSATION AND ADJUDICATION), section 43, 43A, page 19,20, THE INFORMATION TECHNOLOGY ACT, 2000 ACT NO. 21 OF 2000 - India – retrieved from https://www.indiacode.nic.in/bitstream/123456789/1999/1/A2000-21%20%281%29.pdf

36 - Chapter 11 (OFFENCES), section 65, 66, 66A, 66B, 66C, 66D, 66E, 66F, page 23,24,25, THE INFORMATION TECHNOLOGY ACT, 2000 ACT NO. 21 OF 2000 - India – retrieved from https://www.indiacode.nic.in/bitstream/123456789/1999/1/A2000-21%20%281%29.pdf

37 - Chapter 11 (OFFENCES), section 69, 69A, page 26,27, THE INFORMATION TECHNOLOGY ACT, 2000 ACT NO. 21 OF 2000 - India – retrieved from https://www.indiacode.nic.in/bitstream/123456789/1999/1/A2000-21%20%281%29.pdf

38 - Chapter 11 (OFFENCES), section 70, page 27, THE INFORMATION TECHNOLOGY ACT, 2000 ACT NO. 21 OF 2000 - India – retrieved from https://www.indiacode.nic.in/bitstream/123456789/1999/1/A2000-21%20%281%29.pdf

39 - The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information), 2011 (Rules), NO. 11 April 2011 – India - retrieved from - https://www.dataguidance.com/sites/default/files/in098en.pdf

40 - The INDIA'S NATIONAL CYBER SECURITY POLICY, 2013 – India - retrieved from - https://www.meity.gov.in/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf

41 - The National Cyber Security Strategy, 2020 – India - retrieved from - https://www.dsci.in/files/content/knowledge-centre/2023/National-Cyber-Security-Strategy-2020-DSCI-submission.pdf

42 - The Reserve Bank of India Act, 1934, Amended by The Finance act, 2022, - India – retrieved from - https://rbidocs.rbi.org.in/rdocs/Publications/PDFs/RBIA1934170510.PDF

43 - THE DIGITAL PERSONAL DATA PROTECTION ACT, NO. 22 OF 2023, 11th August, 2023, India - retrieved from - https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

44 - THE WHITE PAPER OF THE COMMITTEE OF EXPERTS ON A DATA PROTECTION FRAMEWORK FOR INDIA, India - retrieved from - https://www.meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf

45 - The "Classification Act", 1998, 11 December 1998, last updated 28-2-2024, Belgium, retrieved from - https://www.ejustice.just.fgov.be/img_l/pdf/1998/12/11/1999007004_N.pdf

46 - The Critical Infrastructures Act, 2011, amended on 21 – 8 – 2023, Belgium, retrieved from - https://www.ejustice.just.fgov.be/mopdf/2011/07/15_2.pdf#Page6

47 - The Data protection act, 30 July 2018, amended on 31-12-2021, Belgium, retrieved from - https://www.ejustice.just.fgov.be/mopdf/2018/09/05_1.pdf#Page10

48 - The NIS Act, 2019, amended on 15– 12 -2022, Belgium, retrieved from - https://www.ejustice.just.fgov.be/mopdf/2019/05/03_1.pdf#Page15

49 - The NIS Royal Decree, 12 July 2019, Belgium, retrieved from - https://www.ejustice.just.fgov.be/mopdf/2019/07/18_2.pdf#Page9

50 - Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017) –Rogier CreemersGraham Webster Paul Triolo - June 29, 2018 - Standford University – retrieved from https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/ Behind the Facade of China's Cyber Super-Regulator - What we think we know—and what we don't—about the Cyberspace Administration of China - Jamie P. Horsley - August 8, 2022 – retrieved from https://digichina.stanford.edu/work/behind-the-facade-of-chinas-cyber-super-regulator/ Act on the Protection of Personal Information

51 - Act No. 57 of (2003) – retrieved from https://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf

52 - The Cybersecurity Policy for CIP is revised to designate Ports and Harbours as a critical infrastructure sector – National center of Incident readiness and Strategy For Cybersecurity retrieved from https://www.nisc.go.jp/eng/index.html#sec2

53 - The Cybersecurity Policy for CIP is revised to designate Ports and Harbours as a critical infrastructure sector – National center of Incident readiness and Strategy For Cybersecurity retrieved from https://www.nisc.go.jp/eng/index.html#sec2

54 - The Cybersecurity Policy for CIP is revised to designate Ports and Harbours as a critical infrastructure sector – National center of Incident readiness and Strategy for Cybersecurity retrieved from https://www.nisc.go.jp/eng/index.html#sec2

55 - Cybersecurity Laws and Regulations Japan 2024- Hiromi Hayashi, Masaki yukawa, Daisuke Tsuta – retrieved from https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/japan

56 - The Personal Information Protection Act (PIPA), 2011, amended in 2020, Korea – retrieved from file:///C:/Users/j/Downloads/PERSONAL%20INFORMATION%20PROTECTION%20ACT.pdf

57 - The Act on Promotion of Information and Communications Network Utilization and Information Protection, last updated jun. 10, 2022, Korea – retrieved from https://elaw.klri.re.kr/kor_service/lawView.do?hseq=60899&lang=ENG

58 - The ACT ON THE PROTECTION OF INFORMATION AND COMMUNICATIONS INFRASTRUCTURE, Act No. 6383, Jan. 26, 2001, last updated, Act No. 11690, Mar. 23, 2013, Korea – retrieved from https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=28812&type=part&key=43

59 - Electronic Government Act, Act No. 6439, 28-3-2001, last updated by Act No. 9705, 22 May 2009, Korea – retrieved from https://elaw.klri.re.kr/kor_service/lawView.do?hseq=45844&lang=ENG

60 - The National Cybersecurity Strategy, 2019, Korea – retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/National%20Cybersecurity%20Strategy_South%20Korea.pdf

61 - Ministry of Economic Affairs and Communications – DIGITAL AGENDA 2020 FOR ESTONIA – retrieved from https://wp.itl.ee/files/DigitalAgenda2020_Estonia_ENG.pdf

62 - National defence development plan 2017 – 2026 – Republic of Estonia Ministry of Defense retrieved from https://www.kaitseministeerium.ee/riigikaitse2026/arengukava/eng/

63 - CYBERSECURITY STRATEGY Republic of Estonia 2019 – 2022 retrieved from file:///C:/Users/win10/Downloads/kyberturvalisuse_strateegia_2022_eng%20(2).pdf

64 - CYBERSECURITY STRATEGY Republic of Estonia 2019 – 2022 retrieved from file:///C:/Users/win10/Downloads/kyberturvalisuse_strateegia_2022_eng%20(2).pdf

65 - CYBERSECURITY STRATEGY Republic of Estonia 2019 – 2022 retrieved from file:///C:/Users/win10/Downloads/kyberturvalisuse_strateegia_2022_eng%20(2).pdf

66 - Cyber Defence Pledge – NORTH ATLANTIC TREATY ORGANIZATION – RETERIVED FROM https://www.nato.int/cps/su/natohq/official_texts_133177.htm

٦٧ - The abbreviation for "Estonian Government Information Communications Agency" is often referred to as "RIA," which stands for "Riigi Infosüsteemi Amet" in Estonian. - غالبًا ما يُشار إلى اختصار "وكالة اتصالات المعلومات الحكومية الإستونية" باسم "RIA"، والذي يرمز إلى "Riigi Infosüsteemi Amet" باللغة الإستونية.

68 - CYBERSECURITY STRATEGY Republic of Estonia 2019 – 2022 retrieved from file:///C:/Users/win10/Downloads/kyberturvalisuse_strateegia_2022_eng%20(2).pdf

69 - CYBERSECURITY STRATEGY Republic of Estonia 2019 – 2022 retrieved from file:///C:/Users/win10/Downloads/kyberturvalisuse_strateegia_2022_eng%20(2).pdf

70 - CYBERSECURITY STRATEGY Republic of Estonia 2019 – 2022 retrieved from file:///C:/Users/win10/Downloads/kyberturvalisuse_strateegia_2022_eng%20(2).pdf

71 - CYBERSECURITY STRATEGY Republic of Estonia 2019 – 2022 retrieved from file:///C:/Users/win10/Downloads/kyberturvalisuse_strateegia_2022_eng%20(2).pdf

72 - Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders Vienna, 10-17 April 2000 – United Nations – retrieved from https://digitallibrary.un.org/record/432663/files/A_CONF.187_15-EN.pdf

73 - Cyber Blackmail between Threats and Protection: A Study of the Egyptian and American Legislations – Mohamed Hassan Mekkawi PHD Candidate , Cairo University – retrieved from file:///C:/Users/win10/Downloads/Cyber+Blackmail+between+Threats+and+Protection_+A+Study+of+the+Egyptian+and+American+Legislations.pdf

74 - What is cyber crime? Types Examples, and Prevention – cyber talents – retrieved from https://cybertalents.com/blog/what-is-cyber-crime-types-examples-and-prevention

75 - 5 Types of Cyber Crime: How Cybersecurity Professionals Prevent Attacks- NORWICH UNIVERSITY – retrieved from https://online.norwich.edu/5-types-cyber-crime-how-cybersecurity-professionals-prevent-attacks

76 - 5 Types of Cyber Crime: How Cybersecurity Professionals Prevent Attacks- NORWICH UNIVERSITY – retrieved from https://online.norwich.edu/5-types-cyber-crime-how-cybersecurity-professionals-prevent-attacks

77 - 5 Types of Cyber Crime: How Cybersecurity Professionals Prevent Attacks- NORWICH UNIVERSITY – retrieved from https://online.norwich.edu/5-types-cyber-crime-how-cybersecurity-professionals-prevent-attacks

78 - Concept of Cybercrime in the Banking Sector by Adv. Rupa K.N – ezy legal – retrieved from https://www.ezylegal.in/blogs/concept-of-cybercrime-in-the-banking-sector

79 - What is Intellectual Property – WIPO – retrieved from https://www.wipo.int/about-ip/en/

80 - Anti-Cyber and Information Technology Crimes Law "EGYPT" Law No. 175 of 2018 - (Chapter Six) Aggravating Circumstances of the Crime Article (34) - Mohamed CHAWKI, Ph.D. Chairman, International Association of Cybercrime Prevention (AILCC) Paris – France 2020 – retrieved from https://cybercrime-fr.org/wp-content/uploads/2020/04/Egyptian-cybercrime-law-.pdf

81 - The Global Cybersecurity Index (GCI) is a trusted reference that measures the commitment of countries to cybersecurity at a global level – to raise awareness of the importance and different dimensions of the issue. As cybersecurity has a broad field of application, cutting across many industries and various sectors, each country's level of development or engagement is assessed along five pillars – (i) Legal Measures, (ii) Technical Measures, (iii) Organizational Measures, (iv) Capacity Development, and (v) Cooperation – and then aggregated into an overall score. Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

82 - Egypt ranked ninth at global cybersecurity index – ITU – retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Egypt-Ranked-Ninth-at-Global-Cybersecurity-Index.aspx

83 - National Cybersecurity Strategy – 12 march, 2024 – STATE INFORMATION SERVIVE – retrieved from https://beta.sis.gov.eg/en/media-center/strategies/national-cybersecurity-strategy/

84 - National Cybersecurity Strategy1 2017-2021 - The Arab Republic of Egypt Cabinet of Ministers Egyptian Supreme Cybersecurity Council (ESCC) – retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/EgyptNational%20Cybersecurity%20Strategy-English%20version-18%20Nov%202018.pdf

85 - National Cybersecurity Strategy – 12 march, 2024 – STATE INFORMATION SERVIVE – retrieved from https://beta.sis.gov.eg/en/media-center/strategies/national-cybersecurity-strategy/

86 - Cyber Security – Ministry of Communications and Information Technology – retrieved from https://mcit.gov.eg/en/TeleCommunications/Industry/Cyber_Security

87 - Telecommunications – ministry of communications and information technology – retrieved from https://mcit.gov.eg/en/TeleCommunications/Consumers

88 - Egypt - Information and Communications Technology; and Digital Economy – INTERNATIONAL TRADE ADMINISTRATION – DEPARTMENT OF COMMERCE UNITED STATES OF AMERICA – retrieved from https://www.trade.gov/country-commercial-guides/egypt-information-and-communications-technology-and-digital-economy

89 - Critical analysis of Egypt's new cyber law December 2, 2021 – Smaranika Sen from Kolkata Police Law Institute. This article deals with Egypt's cybercrime laws- retrieved from https://blog.ipleaders.in/critical-analysis-of-egypts-new-cyber-law/

90 - Critical analysis of Egypt's new cyber law December 2, 2021 – Smaranika Sen from Kolkata Police Law Institute. This article deals with Egypt's cybercrime laws- retrieved from https://blog.ipleaders.in/critical-analysis-of-egypts-new-cyber-law/

91 - Critical analysis of Egypt's new cyber law December 2, 2021 – Smaranika Sen from Kolkata Police Law Institute. This article deals with Egypt's cybercrime laws- retrieved from https://blog.ipleaders.in/critical-analysis-of-egypts-new-cyber-law/

92 - Critical analysis of Egypt's new cyber law December 2, 2021 – Smaranika Sen from Kolkata Police Law Institute. This article deals with Egypt's cybercrime laws- retrieved from https://blog.ipleaders.in/critical-analysis-of-egypts-new-cyber-law/

93 - National Telecom Regulatory Authority (NTRA) – STATE INFORMATION SEVICE - 28,March,2024- retrieved from https://beta.sis.gov.eg/en/egypt/political-system/regulatory-authorities/national-telecom-regulatory-authority-ntra/#:~:text=The%20NTRA%20aims%20to%20regulate,the%20framework%20of%20free%20competition.

94 - National Telecom Regulatory Authority (NTRA) – STATE INFORMATION SEVICE - 28,March,2024- retrieved from https://beta.sis.gov.eg/en/egypt/political-system/regulatory-authorities/national-telecom-regulatory-authority-ntra/#:~:text=The%20NTRA%20aims%20to%20regulate,the%20framework%20of%20free%20competition.

95 - National Telecom Regulatory Authority (NTRA) – STATE INFORMATION SEVICE - 28,March,2024- retrieved from https://beta.sis.gov.eg/en/egypt/political-system/regulatory-authorities/national-telecom-regulatory-authority-ntra/#:~:text=The%20NTRA%20aims%20to%20regulate,the%20framework%20of%20free%20competition.

٩٦ - قرار رئيس مجلس الوزراء رقم ٩٩٤ لسنة ٢٠١٧ - الجريدة الرسمية - العدد ١٧ مكرر (ب) - السنة الستون ٥ شعبان ١٤٣٨هـ، الموافق ٢ مايو سنة ٢٠١٧م https://www.laweg.net/framePlain.aspx?action=ViewActivePages&Ite - mID=108151&Type=6&NID=134058

٩٧ - التجربة المصرية في مكافحة الإرهاب السيبراني: رؤية تحليلية - د. رغدة البهي مدرس العلوم السياسية، كلية الاقتصاد والعلوم السياسية، جامعة القاهرة – مركز الاهرام للدارسات السياسية والاستراتيجية - https://acpss.ahram.org.eg/News/٢١٠٧٤.aspx

98 - African Union Convention on Cyber Security and Personal Data Protection – African Union – retrieved from https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

مجلس الوزراء
مركز المعلومات ودعم اتخاذ القرار

الحـــي الحكومـــي – العاصمـــة الإداريـــة الجـديـــدة – مصـــر

رقم بريدي: ٤٨٢٩٩٠٢ ص.ب: ١٩١ الحي السكني R3

تليفون: ٤-٣-٢-١-٢٠٥٤٦٦٠٠ (٢٠٢+) فاكس: ٢٠٥٣٢١١٥ (٢٠٢+)

info@idsc.gov.eg www.idsc.gov.eg