تحديات الأمن السيبراني في ضوء تطور تقنيات الذكاء الاصطناعي

د. البشير محمدين حامد البشير

جامعة المنصورة- مصر

ملخص البحث:

يعد الأمن الركيزة الأساسية للمجتمع لا يمكن تصور نمو أي نشاط بعيدا عن تحققه على المستوى التقني أو القانوني لاسيما مع بروز مجتمع المعلومات والفضاء السيبرانى كأحد أهم القطاعات الخدمية التي تشكل قيمة مضافة ودعامة أساسية لأنشطة الحكومات والأفراد. فقد أفرز التطور العلمي والتكنولوجي ثورة في الاتصالات والمعلومات ذات تأثير على الأنظمة والعناصر المكونة له والتي أصبحت في تقدم تقني متزايد تعدى تطوره التقدم في الاتصالات والمعلوماتية الأجزاء الزمنية الصغيرة من بينها الذكاء الاصطناعي الذي أصبح جزءا منها مع توقعات بفرض هيمنة كبيرة خلال الفترة القادمة لاسيما مع الانتشار الواسع للتطبيقات التكنولوجية الحديثة على الهاتف المحمول أو الحاسب الآلي وازدياد أساليب التواصل الاجتماعي والآلاف من البرامج الالكترونية. وفى العصر الحالي تتسارع التقنية والتحول الرقمي وأصبح الأمن السيبرانى أكثر القضايا أهمية لما يمثله من حماية أساسية للأنظمة والشبكات وبات الاجرام السيبرانى أحد أهم المسائل الجنائية التي تلقى اهتماما ملحوظا على المستويين الوطني والدولي مما دعا الدول إلى العمل على إيجاد آليات لمواجهة تحديات الأمن السيبرانى في ضوء تطور تقنيات الذكاء الاصطناعى بما يحقق طموحات المواطنين في تنمية اجتماعية واقتصادية شاملة ويحمى مصالحهم ويحافظ على مصالح الدولة العليا ويسهم في نهضتها وازدهارها.

الكلمات المفتاحية: الأمن السيبرانى، الذكاء الاصطناعى، التحول الرقمى، الأنظمة والبيانات، الجرائم الالكترونية

Cybersecurity Challenges considering The Development of Artificial Intelligence Technologies

Dr. El-Bashir Mohamedein Hamed El-Bashir

Abstract

Security is the fundamental pillar of society. It is impossible to imagine any activity growing without its technical or legal realization, especially with the emergence of the information society and cyberspace as one of the most important service sectors, constituting value for the activities of governments and individuals. Scientific and technological developments have produced a revolution in communications and information. These systems have witnessed increasing technical progress, with their development going beyond small timescales. Artificial intelligence, among these advances, is now an integral part of this, with expectations of significant dominance in coming period, especially with the widespread use of modern technological applications on mobile phones and computers, the increase in social communication methods, and thousands of electronic programs. Currently, technology and digital transformation are accelerating, and cybersecurity has become a more important issue due to its fundamental protection of systems and networks. This has prompted countries to work and develop mechanisms to address cybersecurity challenges through the development of artificial intelligence technologies. This will achieve citizens' aspirations for comprehensive social and economic development, protect their interests, safeguard the state's supreme interests, and contribute to its progress and prosperity.

Keywords

Cybersecurity, Artificial Intelligence, Digital Transformation, Systems and Data, Cybercrime

المقدمة.

ارتبط الذكاء بالعقل البشـرى، ومع تطور التكنولوجيا، ودخول الحاسـب الآلى كافة المجالاتLakshminath)، A. & Sarda ، 2012 .M ، (3 P أصـبح الذكاء الاصطناعي جزءا منها، مع توقعات بفرض هيمنة كبيرة خلال الفترة القادمة (عبد العليم، م. 2024. ص 1276 وما بعدها)، (على، هـــ. 2022، ص 10 وما بعدها) ؛ فقد أفرز التطور العلمي والتكنولوجى تصنيع الإنسان آلة تساعده على إنجاز المهام بشكل أكثر دقة، وسرعة، ومرونة إكتسـبت صـفة الذكاء التي يتمتع بها الإنسـان أطلق عليها الذكاء الاصـطناعي. (علام، م. 2024، ص. 13) كما أسـهمت الجهود المتواترة خلال العقد الماضى في إحداث تطورات بارزة في هذا المجال، والتقنيات التكنولوجية المرتبطة به كالحوسـبة الكمية، والبيانات الضـخمة، وإنترنت الأشـياء، والروبوتات، والأنظمة ذاتية التشغيل، وغيرها، والوصول بها خلال فترات زمنية قصيرة إلى مستويات فاقت توقعات الخبراء والمتخصصين (منصور، أ. 2024، ص11).

لذا بات ينظر إلى الذكاء الاصـطناعي على أنه قاطرة التطور البشـرى، وأعلاها منزلة في العصر الراهن (حسـكر، م. 2022، ص 188)، لما يقدمه من خدمات جليلة على كافة المسـتويات الشـخصـية، والطبية، والصـناعية، والعسـكرية، والتجارية، والتي تهدف إلى رفاهية البشر، وحمايتهم، والمحافظة على أرواحهم. ورغم ذلك هناك العديد من التداعيات الأخلاقية السلبية المترتبة على تصاعد الإعتماد على مثل هذه التقنية، سواء كانت أمنية، أو اقتصـادية، أو اجتماعية، مما يقتضى ضرورة وضـع ضـوابط للتعامل معها (إبراهيم، م. 2022، ص 7 وما بعدها).

ومع دخول البشـرية مرحلة جديدة تتطلب ضرورة وضـع إطار قانوني حاكم لإستخدامات تقنيات الذكاء الاصـطناعي (دهشـان، ي. 2022، ص 701 وما بعدها)، وتأثير ذلك على السـلوك الإنسـانى، والإجتماعى للإنسـان، والمصـالح القانونية المختلفة الجديرة بالحماية القانونية (القاضى، ر. 2021، ص 875)، وهو الأمر الذي باتت معه مثل هذه التقنيات أحد أهم الموضـوعات بالنسـبة لفقهاء القانون الجنائي، بالنظر إلى كونه علم

يرتكز على تصميم آلات تشارك الإنسان في سلوكيات توصف بأنها ذكية (Khan، C. 2024، 277 P)، ومن ثم تبرز الحاجة إلى إرساء قواعد قانونية تتناسب مع طبيعة هذه التقنية التي من المتوقع لها أن تسود العالم أجمع (سعيد، و. 2022، ص 5).

كما أفرز التطور العلمي والتكنولوجي ثورة في الإتصالات والمعلومات، ذات تأثير على الأنظمة والعناصر المكونة، والتي أصبحت في تقدم تقنى متزايد، تعدى تطوره التقدم في الاتصالات والمعلوماتية الأجزاء الزمنية الصغيرة (عطية، ط. 2009، ص 11)، من بينها الحاسب الآلي (Lerner)، K. & Lerner ، B. 2004 ، 106 P ، الذي يعد أحد أهم ركائز الوثائق الالكترونية وأمنها، ويشغل كثيرا من المسئولين ويؤرقهم. (Moatti، D. 1998، 33-30 P) فضلا عن انتشار تطبيقات التكنولوجيا الحديثة للاتصال بشكل واسع، سواء على الهاتف المحمول أو الحاسب الآلى ؛ إذ أنها تشهد تزايدا واقبالا بسبب تطور التقنية، وازدياد أساليب التواصل كالفيسبوك، الواتس آب، الايميل، الانستغرام، الفايبر، تويتر... الخ، ناهيك عن الآلاف من البرامج الالكترونية التي أصبحت تتحكم في أساليب إدارة الحياة العصرية، ونتيجة لذلك أصبحت تخصصات البرمجة مرغوبة وبكثرة، بسبب تزايد الأفكار، والحاجة إلى تطبيقها بصورة رقمية ومبرمجة (لخضر، ح. 2023، ص 507).

في المقابل من ذلك لاسيما وأننا نعيش اليوم في عصر التقنية الرقمية، والذي تغيرت فيه الكثير من المفاهيم والمعتقدات والسلوكيات، وظهرت أنماط أخرى، ومصطلحات جديدة بدلا من القديمة، كالمواطن الرقمي والحياة الرقمية، وفرضت واقعا جديدا، وسمة تطبع القرن الحادى والعشرين، كون معظم سكان العالم مرتبطين بالانترنت، فضلا عن إتاحة التقنيات الحديثة للجميع، وبات يستفيد منها المواطن العادى ونخبة المثقفين والسياسيين، وجميع القادة في العالم، بل أكثر من ذلك أصبحت التقنية الرقمية مصدرا للمعلومات، ومصدرا للدخل، وقوة بعض الدول، وهو ما يجعلنا أمام عصر رقمى، ونظام عالمى جديد فيه للتقنية دور ونطاق، وفاعلية في رسم خطوط المستقبل (ملال، س. & ادعمى، س. https: //caus.org.lb، 9 / 8 / 2025).

كما يعد الأمن الركيزة الأساسية للمجتمع، بحيث لا يمكن تصور نمو أي نشاط بعيدا عن تحققه، سواء كان ذلك على المستويين التقني والقانوني، والذي تحول مع بروز مجتمع المعلومات والفضاء السيبراني إلى أحد أهم القطاعات الخدمية التي تشكل قيمة مضافة، ودعامة أساسية لأنشطة الحكومات والأفراد على حد السواء. (آل خليفة، م. 2012، ص 2) وفي هذا الصدد تنص المادة (31) من الدستور المصري الصادر عام 2014 على أن " أمن الفضاء المعلوماتي جزء أساسي من منظومة الاقتصاد والأمن القومي، وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه، على النحو الذي ينظمه القانون ".

وتحظى سياسات الأمن السيبراني في القطاع الحكومي بأهمية خاصة، للحاجة إليها، وللصرامة في تطبيقها داخل المؤسسات والمرافق الحيوية ذات الطابع القومي أو السيادي، كالمطارات، والموانئ، ومفاعلات الطاقة النووية، والمنشآت الطبية، والمؤسسات والأسواق المالية، والمنشآت الأمنية والعسكرية... إلخ. (أحمد، ط. 2023، ص 137 وما بعدها) فالمعلومات والبيانات مثلها مثل أي سلعة ذات قيمة مادية، أو غير مادية عالية عرضة للجريمة كالاحتيال، والسرقة ،... إلخ، خاصة مع تباين العلاقات بين الدول، بسبب سرقة معلومات تتعلق بتقنيات متقدمة، كما هو الحال بين الولايات المتحدة والصين وكندا (البداينة، ذ. 2006، ص 16)، وحيث تدل المؤشرات على أن حجم الخسائر العالية الناتجة عن الهجمات السيبرانية يصل إلى تريليون جنيه سنويا، مقابل 80 مليار دولار حجم الإنفاق على أمن المعلومات. (السيد، هـ. https://www.youm7.com/story/2024/7/22، 26 / 7 / 2025)

ويعد الاجرام السيبراني من بين أهم المسائل الجنائية التي باتت تلقى اهتماما، سواء على المستوى الوطني أو الدولي، لانتشارها الكبير (المزروعي، ن. 2024. ص 129)، فضلا عن آثارها الهائلة التي تصيب الدول، والأفراد على حد السواء (Champy)، G. 1992، P5 . كما يظهر الاجرام السيبراني من خلال الهجوم السيبراني الذي يحدث باستخدام وسائل غير مشروعة لاختراق خصوصية الأفراد، أو المؤسسات، أو الشركات، أو المنظمات، أو الحكومات، بهدف الاستيلاء على المعلومات، والسيطرة على البيانات

الخاصـــة بالجهة التي يســـتهدف اختراقها، بغرض الابتزاز المالى، أو الحاق الأذى بالجهة المســـتهدفة، أو بغرض عمليات التجســـس، أو بهدف عمليات السرـــقة، ســـواء لسرـــقة الاختراعات، والابتكارات، والحسابات البنكية والأموال (حمودة، أ. 2022، ص 970).

أولا: موضوع الدراسة.

يحظى موضـوع تحديات الأمن السـيبراني في ضـوء تطور تكنولوجيا الذكاء الاصـطناعي بأهمية خاصـة ؛ ففي عصر تتسـارع فيه التقنية والتحول الرقمي الذي نعيشـه اليوم، أصـبح الأمن السيبراني أحد أهم القضايا، لما يمثله من حماية أساسية للأنظمة والشبكات (العالمية، أ. https://aljazeeraacademy.com، 24 / 7 / 2025)، بهـدف حمـايـة البيانات والمعلومات الحساسة من الوصول غير المصرح به، والهجمات السيبرانية المحتملة (المزروعى، ن. 2024، ص 128). فضـــلا عن تزايد الاعتماد على التكنولوجيا الرقمية في جميع جوانب الحياة من الأعمال التجارية إلى الخدمات الحكومية، مع ارتفاع نســـبة المخاطر المرتبطة بالهجمات الســـيبرانية، وتنوع التهديدات بين الفيروســـات، والبرمجيات الخبيثة إلى هجمات حجب الخدمة، مما يفرض على مؤســـســـات الدولة حماية بيانتها وأصـــولها (لينك، س. https://sumer-link.com ، 24 / 7 / 2025)، لذا تسعى الدول النشطة رقميا جاهدة من أجل توفير الأمن لمختلف البرامج والتطبيقات (Vdovichena، 2024 .O، 1558 P ، وكذا الأجهزة الالكترونية المســـتخدمة، والأنظمة والشـــبكات المعمول بها، بهدف حماية البيانات من أية اختراقات، أو تجاوزات، أو قرصـــنة رقمية محتملة (جربوعة، ع. & بوطمين، ع. 2023، ص 454).

ثانيا: أهمية الدراسة.

ينظر إلى الأنظمة والبيانات المحفوظة لدى أي جهاز أو مؤســـســـة من الأمور الحيوية التي يلزم الحفاظ على سريتها، لما يترتب على افشاءها من أضرارا تصيب الصالح العام، وهو ما يقتضىـ ضرورة اتخاذ كافة التدابير الوقائية لمنع تسرـبها. ونظرا لأهمية الأنظمة والبيانات والاعتماد عليها في تسيير كافة النشاطات الانسانية أصبح الحصول عليها بالطرق المقبولة وغير المقبولة عملية هامة، نجم عنها التفكير في حمايتها، خاصـــة ذات القيمة الأمنية

والاقتصادية والعسكرية، الأمر الذي دعا الحكومات إلى توفير السبل الكفيلة بحماية الأمن السيبراني، والعمل على تقسيم المعلومات إلى درجات سرية، وفق أهميتها، وكيفية تقدير وضع هذه الدرجات وتغييرها، طبقا للظروف والمتغيرات.

ثالثا: أهداف الدراسة.

تهدف الدراسة إلى العمل على تطوير الوسائل، والسبل، والتطبيقات المرتبطة بالذكاء الاصطناعي، واكتسابها أهمية بالغة، خاصة فيما يتعلق بالإعتماد على تقنية المعلومات في عملية تشغيل العديد من مرافق البنية الأساسية كمحطات المياة، والطاقة، وقطاعات أخرى كالدفاع والأمن وغيرها، مما زاد من أهمية وحيوية الحفاظ على الأمن السيبراني، ليس فقط للحفاظ على عمليات تشغيل وتطوير هذا القطاع الحيوى بجوانبه المختلفة، ولكن أيضا لحمايته من محاولة الاختراق، سواء من قبل قراصنة محترفين، أو من خلال هجمات فيروسية وغير ذلك (مهدى، ط. 2023، ص 67).

رابعا: مشكلة الدراسة.

تكمن مشكلة الدراسة في أن تحقيق الأمن السيبراني ليس بالعملية السهلة والبسيطة ؛ إذ يواجه كل يوم بتحديات، وتهديدات عديدة، ومتنوعة، وسريعة، لاسيما في مجال الحفاظ على خصوصية الأفراد، والأمن القومي للدولة، مما يتطلب ضرورة اليقظة، والسرعة، والاستجابة الفعالة، والواعية، والتحديث التكنولوجي المستمر، والقيام بالعمل المطلوب على أعلى مستوى، لمواجهة مثل هذه التحديات والتهديدات، خاصة مع تزايد الانفاق الهائل والمستمر لمواجهة الأضرار التي تنتج عن تهديد الأمن السيبراني أو تعرضه للخطر.

خامسا: تساؤلات الدراسة.

تثير الدراسة العديد من التساؤلات بشأن تحديات الأمن السيبراني في ضوء تطور تقنيات الذكاء الاصطناعي، وتتمثل في الآتي:

ما هو مفهوم الأمن السيبراني وخصائصه وأهدافه؟

ما هي صور تحديات الأمن السيبراني في ضوء تطور تقنيات الذكاء الاصطناعي؟

ما هي آليات مواجهة تحديات الامن السيبراني في ضوء تطور تقنيات الذكاء الاصطناعي وموقف المشرع المصري منها؟

سادسا: منهج الدراسة.

اعتمد الباحث على المنهج الوصفي التحليلي بشأن دور التحول الرقمي في حماية الأنظمة والبيانات من التهديدات السيبرانية، كما وردت في المؤلفات العلمية، باستعراض النصوص التشريعية ذات الصلة، والقاء الضوء على السياسات المتبعة في ذلك، والأحكام القضائية الصادرة، مع الاعتماد على بعض النتائج الهامة، والتوصيات التي انتهي إليها الباحث، للوصول إلى رؤية واضحة، تضمن مواجهة تحديات الأمن السيبراني في ضوء تطور تكنولوجيا الذكاء الاصطناعي، بما يكفل في النهاية الحفاظ على أمن الأنظمة والبيانات من التهديدات السيبرانية.

سابعا: تقسيم الدراسة.

المبحث الأول: مفهوم الأمن السيبراني وتحدياته في ضوء تطور تقنيات الذكاء الاصطناعي.

المبحث الثاني: آليات مواجهة تحديات الأمن السيبراني في ضوء تطور تقنيات الذكاء الاصطناعي وموقف المشرع المصري.

المبحث الأول

مفهوم الأمن السيبراني وتحدياته في ضوء تطور تقنيات الذكاء الاصطناعي

تمهيد

أظهرت ثورة تكنولوجيا المعلومات والاتصالات تولد قلق متزايد نتيجة الخلل في سرية المعلومات المحفوظة والمتداولة الكترونيا، وأثارت محاولات التلصص، أو الاطلاع غير المقبول وغير المشروع على المعلومات، أو الأنظمة من قبل أشخاص غير مصرح لهم بذلك، بحيث أصبحت الحرب السيبرانية أحد أحدث أنواع الحروب في العقود الأخيرة في ظل تجنب الدول الكبرى الدخول في المواجهات العسكرية المباشرة (الرفاتى، أ. https://www.almayadeen.net/articles، 7 / 8 / 2025). وتعد الثورة التكنولوجية أكبر انقلاب علمي وحضاري في توجيه العقل الإنساني نحو التفكير

العميق، والتدبير في شـئون الحياة (جاد، ر. 2023، ص 6) ؛ حيث تؤدى دورا هاما ليس فقط في تسـهيل المعيشـة اليومية للبشر، ولكن كأداة فعالة في تعزيز التنمية في المجتمع، وكعنصر فعال في حماية المصالح العامة، خاصة بعد دخول العالم العصر الرقمي، والذي أصبح معيار التقدم لأي دولة بالعالم (العامري، هـ. 2024، ص 10).

تقسيم...

المطلب الأول: تعريف الأمن السيبراني وأهدافه.

المطلب الثاني: صور تحديات الأمن السيبراني.

المطلب الأول

تعريف الأمن السيبراني وأهدافه

أولا: مضمون الأمن السيبراني.

تضمنت الفقرة التاسعة من المادة الأولى من القانون رقم 5 لسنة 2022 بإصدار قانون تنظيم وتنمية اسـتخدام التكنولوجيا المالية في الأنشـطة المالية غير المصرـفية على تعريف الأمن السـيبراني على أنه " إجراءات وعمليات تقنية وتنظيمية من شـأنها الحفاظ على خصوصية البيانات، وسريتها، وسلامتها، ووحدتها، وتكاملها فيما بينها ". ويتضمن ذلك على العديد من الجوانب مثل أمن الشبكات، أمن التطبيقات، أمن المعلومات، والتعافي من الكوارث، التوعية والتدريب، وإدارة الهوية والوصـول. ومن خلال الاسـتراتيجيات التي تعتمدها الدول يمكن للأفراد، والمؤسـسـات حماية أنفسـهم من التهديدات السـيبرانية المتزايدة (المزروعى، ن. 2024. ص 130).

كما يشـير مصـطلح الأمن السـيبراني إلى مجموعة الوسـائل التقنية، والتنظيمية، والإدارية التي يتم اسـتخدامها، لمنع الاسـتخدام غير المصرـح به، وسـوء الاسـتغلال، واسـتعادة المعلومات الالكترونية، ونظم الاتصـالات والمعلومات التي تحتويها (عبود، ق. 2017، ص 97 وما بعدها)، بهدف ضـمان توافر، واسـتمرارية عمل نظم المعلومات، وتعزيز حماية سرية المعلومات، وخصـوصـية البيانات الشـخصـية، وإتخاذ جميع التدابير اللازمة لحماية المواطنين، والمستهلكين من المخاطر في الفضاء السيبراني (Metin، B. & özhan ، F.

Wynn &، M. 2024 ، (P 1 . ومن هنا تبلورت السياسة السيبرانية وتم توظيفها، للتعبير عن العمليات الآلية، والعلاقات بين الأجهزة الالكترونية والإنسان (برغوث، ل. 2023، ص 446).

ثانيا: خصائص وأهداف الأمن السيبراني.

يتميز الأمن السيبراني بالعديد من الخصائص أهمها شبكة خالية من الحجم، وذو طابع متعدد التخصصات الاجتماعية والتقنية، وعلى درجة عالية من التغيير والترابط وسرعة التفاعل (عدلى، هـ. 2023، ص 190). ويهدف الأمن السيبراني إلى ضمان توافر استمرارية عمل النظم المعلوماتية، وحماية الأنظمة التشغيلية من أي محاولات، للولوج غير المسموح به لأهداف غير سليمة، وحماية مصالح الدولة وأمنها الوطني، والبنى التحتية الحساسة فيها، وإتخاذ جميع التدابير اللازمة، لحماية المواطنين والمستهلكين على حد سواء من المخاطر المحتملة في مجالات استخدام الانترنت المختلفة، فضلا عن تعزيز حماية الشبكات، وحماية، وسرية، وخصوصية البيانات الشخصية، وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات (بسيونى، آ. 2022، ص 254).

وفي حال الاخلال بأهداف وخصائص الأمن السيبراني يؤدى ذلك إلى ظهور الجرائم السيبرانية، والتي تعرف على أنها " كل فعل غير مشروع يستهدف تغيير البيانات، أو المعلومات بالحذف، أو الاضافة، أو المعالجة، أو السرقة، أو تحويل المعلومات، أو تعديلها لغايات غير مشروعة بواسطة الكمبيوتر، أو أي وسيلة تكنولوجية أخرى " (محمد، ا. 2024، ص 17). ومن هذا التعريف يتضح أن الجريمة السيبرانية، لا تعنى فقط بالجرائم التي تستهدف البيانات الموجودة على أنظمة الحاسب الآلي، وإنما تمتد لتشمل كافة الأنشطة الاجرامية التي يستخدم فيها الحاسب الآلي والانترنت، ومختلف التقنيات المتطورة كالذكاء الاصطناعي، وتقنيات الجيل الخامس (برغوث، ل. 2023. ص 448). ونظرا للطبيعة الخاصة لهذه الجرائم، فإنها تتميز عن الجرائم التقليدية بالعديد من الخصائص أهمها تتم عبر التقنيات التكنولوجية الحديثة، وتستهدف الأنظمة المعلوماتية، لذا تعد من الجرائم

الناعمة، فضلا عن صعوبة اكتشافها، وضبط وتوصيف الجرائم السيبرانية، والطابع الدولي لها، وامتناع المجنى عليه عن التبليغ (الهدى، ق. 2023، ص 2023).

وجدير بالذكر أن وكالات الاستخبارات في جميع أنحاء العالم تسخر قوة الذكاء الاصطناعي لتعزيز قدراتها بطرق مختلفة (Osoba، A. & Welser، W. P 6، https: / /www.rand.org /pubs /perspectives /PE237.html، (2025 / 8 / 11، حيث تنقب خوارزميات الذكاء الاصطناعي في مجموعة بيانات ضخمة لحركة الاتصالات العالمية، وصور الأقمار الصناعية، ومنشورات مواقع التواصل الاجتماعي، لتحديد تهديدات الأمن السيبراني والأنشطة الارهابية، والتطورات الجيوسياسية (الكتبى، ع. 2023، ص 62 وما بعدها). ويمكن من خلال هذه التحليلات التنبؤية مساعد أجهزة الأمن على احباط الهجمات الالكترونية بشكل استباقي، ومنع الأعمال الارهابية، والاستجابة بفاعلية أكبر للأزمات الجيوسياسية الناشئة في مجال الأمن السيبراني، حيث تراقب الأنظمة المدعومة بالذكاء الاصطناعي الشبكات باستمرار، وتكشف الهجمات الالكترونية، وتستجيب لها بسرعة، من خلال الأنظمة ذاتية التشغيل القادرة على تنفيذ مهام المراقبة والاستطلاع (University، V. https: //onlinewilder-vcu-edu.، 2025 / 8 / 8).

وفي هذا السياق قامت وكالات الأمن السيبراني والاستخبارات بالدول الأعضاء في العيون الخمس Five Eyes، وهو تحالف استخباراتي يشمل كل من الولايات المتحدة والمملكة المتحدة وكندا واستراليا ونيوزيلندا من خلال عملية منسقة أطلق عليها عملية MEDUSA بتدمير البنية التحتية المستخدمة، من قبل برنامج Snake للتجسس الإلكتروني، والذي تستهدف الحكومات والسفارات، ومنشآت البحث ويديره جهاز الأمن الفيدرالي الروسي FSB عبر تطوير أدوات الذكاء الاصطناعي، لفك تشفير شبكة التجسس والاتصالات (الارهاب والاستخبارات، ال. https: //www.europarabct.com، 8 / 8 / 2025). كما أعلنت شركة سيلوبريكر عن خططها لإطلاق سيلوبريكر للذكاء الاصطناعي، وهي أداة ذكاء

اصـطناعى توليدية، مصـممة لمسـاعدة فرق اسـتخبارات التهديدات على جمع، وتحليل، واعداد التقارير حول متطلباتها الاسـتخباراتية، مما يمكن المؤسـسـات من تقييم المخاطر الجيوسـياسـية والسـيبرانية والمادية من التخفيف من حدتها بكفاءة (Silobreaker، https: //www-silobreaker-com، 2025 8 / 8 ،).

المطلب الثاني

صور تحديات الأمن السيبراني

أولا: الهجمات المعادية على أنظمة الذكاء الاصطناعي.

وتشـمل التهديدات التي تلحق بمكونات الذكاء الاصـطناعي المادية، مثل وحدات الادخال والاخراج والتخزين، والمكونات المعنوية كالبيانات والمعلومات، التي تتسبب في الحاق الضرـر بأجهزة الذكاء الاصـطناعي، ومن ثم تدميرها كليا أو جزئيا (محمد، ال. 2024. ص 20)، لما لشـبكة الانترنت العالمية من تأثير على أوضـاع الأمن الاقتصـادي، والاجتماعي، والثقافي، والعسـكري للدول والمجتمعات، واسـتخدامها من جانب بعض العصـابات الإجرامية، والتنظيمات الإرهابية في تنفيذ عملياتها، وإحباط مخططات الحكومات، وأجهزة الأمن المضادة (محمد، ال. 1998، ص 25).

ثانيا: استخدام الذكاء الاصطناعي في الهجمات السيبرانية.

نتيجة التطورات البارزة في مجال الذكاء الاصـطناعي، والتقنيات التكنولوجية المرتبطة به، يسـتخدم منفذي الهجمات السـيبرانية الذكاء الاصـطناعي كوسـيلة للوصـول إلى المعلومات والبيانات الخاصـة بالهيئات والمؤسـسـات والشرـكات، ذات القيمة العالية، لتحقيق مكاسب مادية على حساب هذه الشركات (الخبيزى، ب. 2023، ص 245). كما تم اسـتخدام تقنيات الذكاء الاصـطناعي من قبل الجماعات والتنظيمات الارهابية، والتي طورت قدراتها التكنولوجية، بما يسـمح لها باسـتخدام بيانات ضـخمة، وتحليلها عبر الانترنت، بغرض تسهيل عملياتها الارهابية (مهدى، ط. 2023. ص 11).

ثالثا: تحديات الثغرات الأمنية في الذكاء الاصطناعي.

مع تزايد الاعتماد على تقنيات الذكاء الاصطناعي ظهرت تهديدات أمنية متقدمة تتطلب الحذر واليقظة من بينها الاختراق السيبراني للأنظمة الذكية، وسرقة البيانات الشخصية، وهجمات التصيد الاحتيالي المتطورة التي يصعب اكتشافها، والتزييف العميق (DeepFake)، بإنشاء مقاطع فيديو وصوت مزيفة لأغراض خبيثة، والتحكم غير المصرح به في الأجهزة، والذي قد يؤدى إلى تعطيل أنظمة حيوية، أو توجيهها لأغراض ضارة (الاصطناعي، ق.https: //www.fada2-ai.com ، 18 / 8 / 2025).

رابعا: تحديات التكاليف والموارد.

تشكل قيود الموارد والحدود في الميزانية تحديات كبيرة للمنظمات التي تسعى إلى تنفيذ تدابير الأمن السيبراني الشاملة، وتعزيز دفاعاتها الرقمية. ففي ظل بيئة الأمن السيبراني المعقدة تتطور التهديدات باستمرار، وتزداد تعقيدا، تعد الحاجة إلى موارد كافية أمرا بالغ الأهمية، مما يتعين معه على المؤسسات العمل على تحديد أولوياتها الاستراتيجية، لتخصيص مواردها المحدودة، ومعالجة نقاط الضعف في بنيتها التحتية، والحماية من الهجمات السيبرانية المحتملة. ويتطلب هذا تخطيطا دقيقا، وفهما عميقا، لمشهد المخاطر السيبرانية، وتحتاج المؤسسات إلى استكشاف حلول أمنية فعالة من حيث التكلفة، دون المساس بفاعلية دفاعاتها (DataGuard، https: //www-dataguard-com18 / 8 / 2025 ،).

خامسا: تحديات إدارة الهوية والوصول.

يمكن للقراصنة الاستفادة من الذكاء الاصطناعي لتطوير هجمات أكثر تعقيدا واستهدافا وأتمتة مراحل مختلفة من عملياتهم، لذا سعى المجرمين والخارجين عن القانون في الفضاء السيبراني – سواء أكانوا من الهواة أم معتادي الاجرام – على مواكبة التطورات التقنية في المجال المعلوماتي، وخاصة فيما يتعلق بالأمن السيبراني، الأمر الذي يصعب معه تحديد هوية مرتكبي انتهاكات الأمن السيبراني أو الوصول إليهم (أحمد، ط. 2023. ص 138 وما بعدها).

سادسا: تحديات اكتشاف الهجمات.

تتسم هذه الجرائم بصعوبة اثباتها، حيث أن وسيلة ارتكابها ليست مادية، لذا تسمى بالجريمة الناعمة، لاعتمادها على أنشطة الكترونية يمكن الغائها، أو تدميرها، أو تغييرها، وليس سهلا إثبات مصدرها، إلا من قبل متخصصين، وتقتضي إجراءات محاكمتها لقضاة مؤهلين علميا وتقنيا (محمد، ال. 2024. ص 19).

سابعا: تحديات الخصوصية.

أدى الاتصال الجماعي والتشارك في استعمال التطبيقات المختلفة التي أتاحتها التكنولوجيا والبرمجيات عبر الانترنت إلى تراجع مبدأ السرية والخصوصية الشخصية، فأصبح من الممكن الاطلاع على أسرار الغير، من خلال نشر الفضائح، والأسرار الشخصية، أو عن طريق الاختراق (لخضر، ح. 2023. ص 509). وفي هذا السياق أدى استخدام تقنيات الذكاء الاصطناعي للبيانات والمعلومات المرفوعة على الانترنت، وتداولها، وتتبع السلوكيات الرقمية للبشر لحظة بلحظة، ومراقبة العملاء، والموظفين، والمستهلكين بطريقة فاعلة، والتعرف على سلوكياتهم، والاطلاع على أسرارهم مما يمثل خرقا لخصوصياتهم وبياناتهم (جمعة، ط. 2023. ص 48).

وفي هذا الصدد قضت محكمة النقض المصرية بأنه " لما كان الحكم المطعون فيه بعد أن بين واقعة الدعوى بما تتوافر به العناصر القانونية، لجرائم هتك عرض طفلة، والتقاط صور لها في مكان خاص، ونشرها، وتهديدها كتابة بإفشاء أمور خادشة للحياء، لحملها على القيام بعمل التي دان المطعون ضده بها، وأورد على ثبوتها في حقه أدلة سائغة... لما كان ذلك وكان البند الأخير من المادة 309 مكررا من قانون العقوبات التي دين بها المطعون ضده بها، ينص على أنه " ويحكم في جميع الأحوال بمصادرة الأجهزة، وغيرها مما يكون قد استخدم في الجريمة، أو تحصل عنها، كما يحكم بمحو التسجيلات المتحصلة عنها، أو اعدامها ". ولما كانت عقوبة محو التسجيلات المتحصلة عن الجريمة هي عقوبة نوعية مراعى فيها طبيعة الجريمة. ولذلك يجب توقيعها مهما تكن العقوبة المقررة، لما ترتبط به هذه الجريمة من جرائم أخرى، والحكم بها مع عقوبة الجريمة الأشد. لما كان ما تقدم، فإن

الحكم المطعون فيه إذا أغفل القضاء بمحو التسجيلات المتحصلة عن الجريمة إعمالا لنص البند الأخير من المادة 309 مكررا من القانون المشار إليه يكون قد خالف القانون، بما يتعين معه تصحيحه بإضافة عقوبة محو التسجيلات المتحصلة عن الجريمة إلى العقوبة المقضى- بها " (نقض جنائى، الطعن رقم 3224 لسنة 90 قضائية، جلسة 5 سبتمبر سنة 2021).

ثامنا: تحديات أخرى للأمن السيبراني.

يواجه الأمن السيبراني العديد من التحديات الأخرى بشأن صعوبة وتعقيد عمليات إدارة المخاطر السيبرانية بشكل عام – سواء في القطاع الحكومي، أو غيره من القطاعات الأخرى – نتيجة التطور التقني المتسارع في النظم الرقمية، والتطبيقات المعلوماتية، وتعقد القيود والالتزامات القانونية المرتبطة بها. وتعد ثقافة إدارة الخطر السيبراني هي الأقل انتشارا حتى في الدول المتقدمة، ومن ثم يظل العنصر- البشرى أحد أكبر التحديات التي تواجه الأمن السيبراني. وعجز بعض المؤسسات العلمية لدى الدولة عن وضع سياسة أمن سيبراني متكاملة، وفعالة، وسهلة التطبيق (أحمد، ط. 2023. ص 138 وما بعدها). فضلا عن قصور التشريعات في ملاحقة التطورات المستمرة لمثل هذا النوع من الجرائم، والاعتماد الكبير على الأجهزة والبرامج المستوردة، واستخدامها في العديد من القطاعات الحيوية، الأمر الذي يترتب عليه الحاق أضرار بالأمن القومي للبلاد (الخبيزى، ب. 2023. ص 246).

المبحث الثاني
آليات مواجهة تحديات الأمن السيبراني
في ضوء تطور تقنيات الذكاء الاصطناعي وموقف المشرع المصري

تمهيد...

تنبع أهمية الاختيار الواعي لسياسات الأمن السيبراني المتبعة من قبل الجهة، أو الحكومات القائمة على حماية المنظومة الرقمية للحكومة الالكترونية من عدم الفعالية الكاملة لنظم إدارة الخطر السيبراني، والوقاية منه (أحمد، ط. 2023. ص 137). وفي هذا

الصـدد أصـدر المشـرع المصـري العديد من التشـريعات، والقرارات ذات الصـلة، بما يدعم التحول نحو اقتصـــاد رقمي متكـامـل، يحقق طموحـات المواطنين في تنميـة اجتماعيـة واقتصادية شاملة، ويحمى مصالحهم، ويحافظ على مصالح الدولة العليا، ويسهم في نهضتها وازدهارها (الوزراء، م. 2017-2021. ص 1 وما بعدها).

تقسيم...

المطلب الأول: آليات مواجهة تحديات الأمن السيبراني.

المطلب الثاني: موقف المشرع المصري لمواجهة تحديات الأمن السيبراني.

المطلب الأول

آليات مواجهة تحديات الأمن السيبراني

أولا: تطوير استراتيجيات شاملة للأمن السيبراني.

تولى الحكومات الأولوية القصوى للأمن السيبراني، ضمن الاستراتيجية الوطنية للأمن السـيبراني، من حيث تسـخير التدابير اللازمة التي من شـأنها توفير أكبر درجة حماية لبنيتها المعلوماتية التحتية، وتحقيق أمنا سـيبرانيا مناسـبا للتحولات الرقمية الجارية، وعملية عصرـنة قطاعات الدولة، والتي تفرض تحديات كبيرة أمام تحقيق الأمن اللازم لمختلف أجهزة الدولة ومواطنيها (برغوث، ل. 2023. ص 452). وفي هذا السياق تسعى الدول إلى القيام بإعادة شـاملة، وعامة لنظم حفظ، وتداول المعلومات، والبيانات، وأسـس وقواعد السرـية، بما يتناسـب مع المسـتجدات التي أوجدتها العولمة، وثورة المعلومات والاتصـالات، وطبيعة التهديدات الجديدة التي فرضـتها، بهدف الوصـول إلى تحديد دقيق إلى كيف، ولماذا تكون المعلومات سرية، ومتى يمكن إطلاق هذه المعلومات، وإزالة طابع السرية عنها (العسافي، غ. 27501/elsada.net//:http، 7 / 8 / 2025).

ثانيا: الاستثمار في تدريب وتوعية الموظفين.

يعد الخطأ البشرـى أبرز نقاط الضـعف في الأمن السـيبراني (SwntinelOne، 18 / 8 / 2025 https://www-sentinelone-com18، ، لذا يتعين العمل على عقد دورات تدريبية للموظفين في مجال الأمن السـيبراني تتناول مفاهيم وأهداف

وأهمية وفوائد، وأنواع الأمن السيبراني، والتحديات التي تواجهه وكيفية التغلب عليها. فضلا عن عقد ورش عمل حول إجراءات الحماية ضد تحديات وتهديدات ومخاطر الأمن السيبراني تحت اشراف مدربين متخصصين في الأمن السيبراني. كما يجب على الموظفين فهم المبادئ الاساسية لأمن البيانات والمعلومات والامتثال اليها مثل اختيار كلمات مرور قوية والحذر من المرفقات الموجودة ضمن البريد الإلكتروني والنسخ الاحتياطي للبيانات (الخبيزى، ب. 2023. ص 247).

ثالثا: تدابير إرساء الأمن الفكري والإعلامي.

تعزى العديد من مظاهر الجريمة وأسبابها إلى المواد الاعلامية المنكشفة، والميسرة لكافة فئات المجتمع، لاسيما المراهقين منهم عن طريق الانترنت، أو القنوات الاعلامية، وأفلام الاكشن والدراما والمواقع الارهابية والاباحية... الخ، والتي تعمل على التوجيه اللاإرادي لوعى وسلوك المشاهدين نحو طباع العنف وسلوك الاجرام، من خلال ترويض النفوس على صور القتل والدم والمخدرات والعلاقات الجنسية، الأمر الذي يقتضي ضرورة وضع قواعد ومبادئ واضحة لميثاق أخلاقيات الاعلام الوطني، وبيان موضوعه وغايته، وطبيعته ومجاله ورسالته، والالتزام بالدفاع عنها، باستخدام التكنولوجيا الحديثة للمعلومات والاتصالات (لخضر، ح. 2023. ص 516 وما بعدها).

وفي هذا الصدد قضت محكمة النقض المصرية بأنه " لما كان الحكم المطعون فيه قد حصّل واقعة الدعوى بما مؤداه قيام المتهمين – في الفترة. – ...من الأول وحتى الثلاثين بالتخابر مع التنظيم الدولي للإخوان المسلمين وحركة المقاومة الإسلامية ".... " واشتراك المتهمين الأربعة التالين لهم في هذه الجريمة، وذلك بغية إشاعة الفوضى والعنف ونشر الشائعات، بما يؤدي إلى إسقاط نظام الحكم واعتلائهم محله، ولتحقيق ذلك المسعى تولى المتهمون من الأول وحتى الثامن ومن الحادي والثلاثين حتى الرابع والثلاثين قيادة جماعة أُسست على خلاف القانون الغرض منها الدعوة إلى تعطيل أحكام الدستور والقوانين وعرقلة عمل مؤسسات الدولة، وسلطاتها العامة، والعصف بحريات المواطنين والمساس بالحقوق العامة والوحدة الوطنية والسلام الاجتماعي مبتغية من وراء ذلك المسلك الآثم قفزًا على

السـلطة بالقوة على حسـاب دماء بريئة ذكية وأموال عامة اسـتهدفوها حيث اتخذوا من الإرهاب مطية لهم وسبيلًا لتحقيق مبتغاهم مستعينين في ذلك بأسلحة وأموال أمدهم بها المتهمون الأول والثاني والعاشر والرابع والثلاثين وهم على بينه من ذلك المسعى ومبتغين تحقيقه منضمًا إليهم في جمعهم هذا المتهمون من التاسع وحتى الثالث عشر ومن الخامس عشر حتى الثلاثين، وكذا الأخيرين وهم أيضًا على بينة من أمر هذه الجماعة ومسعاها، وفي سبيل ذلك انتهجوا تنسيقًا وتحالفًا مع جهتي التخابر وغيرها من المنظمات والأحزاب التي التقت معها في هذا المسعى كحزب الله والحرس الثوري. ...انطوى على دعم مادي وعسكري وتأهيل إعلامي وتبادل للمعلومات وتلقٍ للتوجيهات والتحاق للمتهمين الخامس عشر والحادي والعشرين والثاني والعشرين ومن الخامس والعشرين حتى الثلاثين بمنظمة إرهابية خارج البلاد بغية تأهيلهم عسكريًا ثم تسللهم بطريقة غير شرعية إلى داخل البلاد بعد أن أتموا مبتغاهم وكان من نتاج كل هذا السبيل إشاعة الفوضى والعنف والإرهاب داخل البلاد وإتيان عديد من الأعمال الماسة باستقلال البلاد وسلامتها من قبل المتهمين عدا الأخيرين منهم بما أدى إلى إراقة الدماء البريئة الذكية والاعتداء على ممتلكات ومؤسسات عدة للدولة أفلح معه مسعاهم الآثم وامتطوا الحكم على أنقاض وطن ودماء أبنائه ولم ينسوا وقد بلغوا المأمول من أعانهم على بلوغه فقام المتهمون الثالث – بصفته رئيسًا للجمهورية حينها والعاشر والحادي عشر والواحد والثلاثين والأخيرين – حال كونهم من موظفي الرئاسة حينها – بتسليم الحرس الثوري.... سرًا من أسرار الدفاع عن البلاد يتعلق بأنشطة غير مشروعة رصدتها أجهزة الأمن القومي بشأن عناصر موالية ل.... تبتغى المساس بأمن واستقرار البلاد. كما أفشوا مضمون خمس تقارير سرية أعدتها الأجهزة – آنفة الذكر – للعرض على المتهم الثالث، وساق الحكم برهانًا على ثبوت تلك الجرائم بحق الطاعنين أدلة استقاها من أقوال شهود الإثبات، وما ثبت من تحريات الأمن الوطني، وأقوال مجريها وتحريات الأمن القومي، وما أرفق بهما، وما ثبت من الاطلاع على بعض القضايا والأحكام والوثائق ورسائل هاتفيه، وما قرر به المتهم الرابع بتحقيقات النيابة العامة، وما ثبت من الاطلاع على شهادة اللواء.... في القضية رقم.... لسنة....

جنايات..... وحيث إن الشـارع يوجب في المادة ٣١٠ من قانون الإجراءات الجنائية أن يشتمل كل حكم بالإدانة على بيان الواقعة المستوجبة للعقوبة بيانًا تتحقق به أركان الجريمة والظروف التي وقعت فيها، والأدلة التي اسـتخلصـت منها المحكمة ثبوت وقوعها من المتهم وأن تلتزم بإيراد مؤدى الأدلة التي اسـتخلصـت منها الإدانة، حتى يتضـح وجه اسـتدلالها بها، وسـلامة مأخذها، وإلَّا كان الحكم قاصرًا... " (نقض جنائي، الطعن رقم 50733 لسنة 85 قضائية، جلسة 22 / 11 / 2016).

رابعا: التعاون وتبادل المعلومات.

أدى ظهور الجرائم السـيبرانية كنمط جديد من أنماط الجريمة، وما تتميز به من خاصـية عابرة للحدود الاقليمية للدول، ضرورة توجه المجتمع الدولي نحو التعاون من أجل تصد فعال لتلك الجرائم، والتي لها بالغ الآثار السـلبية، إذا ما تركت على الأمن القومي للدول في جميع النواحي الاقتصـادية والعسـكرية والأمنية وفق ما ورد بنص المادة الرابعة من القانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات.، لذا سعت دول العالم التقدمة والنامية نحو اتخاذ إجراءات مشتركة للتصدي لتلك الجرائم، من خلال إبرام الاتفاقيات والمعاهدات الدولية، لمواجهة مثل هذه النوع من الجرائم، والعمل على مكافحتها (محمد، ال. 2024. ص 16).

فعلى الصـعيد الدولي أصـدر مجلس أوروبا اتفاقية بودابسـت 2001 بشـأن الجرائم الالكترونية، لتصـبح أول معاهدة دولية تركز صراحة على الجرائم الالكترونية (https://rm.coe.int/budapest-convention-in-arabic/1680739173، 31 / 7 / 2025)، وتهدف إلى موائمة القوانين الوطنية المتعلقة بالجرائم الالكترونية، ودعم التحقيق في هذه الجرائم، وتعزيز التعاون الدولي في مكافحة الجرائم الالكترونية. وتلزم المعاهدة الدول المشاركة بإعتماد تشريعات تجرم جرائم الكترونية محددة، وصـياغة قواعد محددة لجمع الأدلة، عندما لا تمتلك الدول المعنية بطلب المساعدة القانونية المتبادلة (MLAT)، بشأن الحفظ السريع للبيانات المخزنة (داسكال، ج. & مايو، د. https://www-crossborderdataforum-org، 3 / 7 /

2025). كما اعتمدت الجمعية العامة للأمم المتحدة في عام 2024 اتفاقية مكافحة الجرائم الالكترونية، بهدف منع ومكافحة الجرائم الالكترونية بكفاءة وفعالية أكبر، والعمل على تعزيز التعاون الدولي، وتقديم المساعدة الفنية، ودعم وبناء القدرات، وخاصة للدول النامية، ولتصبح منصة غير مسبوقة للتعاون في تبادل الأدلة الالكترونية، وحماية الضحايا، واتخاذ التدابير الوقائية لضمان حقوق الإنسان على الانترنت (الجمعية العامة، https://news.un.org/ar/story، 31 / 7 / 2025). كما أصدر الاتحاد الأوروبي اللائحة العامة لحماية البيانات GDPR، باعتبارها قانون لحماية خصوصية، وبيانات مواطني الاتحاد الأوروبي، بهدف ردع الشركات عن إساءة استخدام بيانات العملاء، وتعد وثيقة أساسية من حيث حماية البيانات، وبالتالي فهي جزء لا يتجزأ من الأمن السيبراني (GDPR، 2025 / 7 / 31) https://www-gdpreu، org ،

خامسا: سياسة تشفير البيانات.

أدى التقدم التقني الهائل في عالم الاتصالات، وما استتبعه بالضرورة من قيام تهديدات، واستغلال لتلك الشبكة (Catala) ، 1983 .P ، 37 P ، نحو إيجاد وسائل تأمين، لمواجهة المخاطر والتهديدات السيبرانية (عبد الحفيظ، أ. 2002، ص 429)، مما دفع عدد من الخبراء المعنيين نحو البحث عن حلول مناسبة، يتم استخدامها في أمن وحماية المعلومات، وقواعد البيانات أهمها تشفير الأنظمة والبيانات الحساسة (أحمد، أ. 2014، ص 49). ويعد التشفير أهم حجر في بناء أمن المعلومات، وأكثر الوسائل فعالية (Juliana de Groot، https://www.digitalguardian.com ، / 29 / 7 / 2025)، بمقتضاه يتم تحوير صورة البيانات على نحو غير مفهوم لمن يتلصص عليها، ومنع الأشخاص غير المرخص لهم من الاطلاع عليها (سالم، ص. 2003، ص 157). كما يهدف تشفير المعلومات إلى إخفاء البيانات والمعلومات (أحمد، ن. 2009، ص 276)، والعمل على حمايتها، والمحافظة على سريتها عن طريق تحويلها إلى رموز معينة غير مقروءة (على، ر. 2009، ص 276). ومن خلال هذا المفهوم لا يستطيع أي شخص تلقى الرسائل بوضوح، أو فهم مضمونها، إلا من خلال استعمال أجهزة فك الشفرة (طنطاوي،

إ. 2003، ص 235). ويستخدم التشفير كأساس لبعض البروتوكولات أثناء تنفيذ مهمة معينة، لضمان إتاحة الموارد لمن يحتاج إليها (داود، ح. 2000، ص 176)، وكأحد وسائل حماية أمن المعلومات ضد أعمال القرصنة، وبث الفيروسات، والإعتداء على المعلومات الاسمية، وبيانات بطاقات الائتمان الممغنطة (عطية، ط. ص 586).

ويطلق الفقه على التشفير مصطلح تكويد المعلومات (غيطاس، ج. 2007، ص 168)، ويعنى نقل المعلومات من حالتها الواضحة المفهومة التي تتيح لمن يطالعها، أو يحصل عليها معرفة ما تحمله من معنى، أو مغزى إلى حالة شديدة الغموض غير مفهومة أو واضحة، يجعل الفهم، أو المعرفة، أو الاستيعاب، وهو بذلك يختلف عن مصطلح الرمز أو الكود عن الشفرة (الشهري، ح. 2012، ص 20 وما بعدها) ؛ إذ أن ما تحمله من معنى يجعلها معلومات عديمة الفائدة، أو عديمة الجدوى لمن يطالعها، أو يحصل عليها بدون وجه حق (علام، م. 2014، ص 128). ويتميز كمال المعلومات بخاصيتين (الأولى) القدرة على تجميع، ومعالجة، واختزان، وتوزيع المعلومات بصورة دقيقة، وكاملة في الوقت المناسب. و(الثانية) القدرة على التصدي لأي ضعف، أو انتهاك لكمال المعلومات عارضا، أو متعمدا (بيكر، هـ. 1998، ص 25). وقد تطورت وسائل التكويد والتشفير عبر عقود طويلة من الزمن بدءا من الرسائل، والمكاتبات المشفرة المكتوبة باليد، وبالأحبار السرية، وغيرها، وانتهاء بالنظم المعقدة التي تقوم لحظيا بتشفير، وتكويد تيارات متصلة من البيانات، والمعلومات التي تبث عبر شبكات الاتصالات، والمعلومات العملاقة التي تلف كوكبنا الأرضي، وسماء الفضاء الخارجي (غيطاس، ج. 2007. ص 168). كما يقوم تشفير GSM A5 بعمل حماية وتشفير البيانات المرسلة بين الأجهزة المحمولة، ومحطة الاستقبال، ويرسل المعلومات في حوزة تمثل محادثة صوتية، أو رسالة SMS، أو فاكس، أو غيرها، وهو ما حدث ابان تفجير المركز التجاري الدولي في نيويورك بالولايات المتحدة الأمريكية عام 1994، وطائرة مانيليه (البداينة، ذ. 2006. ص 143). وتستخدم GSM في الهواتف المحمولة، والانترنت اللاسلكي، وبرامج تحديد المواقع، وغيرها (العازمي، ف. 2012، ص 90). كما تستخدم المفاتيح في تشفير الرسالة (Encryption)، وفك

تشفيرها (Decryption)، وتستند هذه المفاتيح إلى صيغ رياضية معقدة (خوارزميات)، وتعتمد على قوة، وفعاليات التشفير على عاملين أساسيين الخوارزمية، وطول المفتاح مقدرا بالبايت (Bits) (الشهرى، ح. 2012. ص 22).

وينقسم التشفير بصفة عامة إلى نوعين أساسيين (الأول) وهو التشفير المتماثل، والذي يتم باستخدام مفتاح شفرة واحد لكل من عمليتي التشفير، وفك الشفرة. أما النوع (الثاني) فهو التشفير غير المتماثل، والذي يستخدم فيه مفتاحان للشفرة أحدهما يستخدم خلال عملية التشفير، والآخر يستخدم لفك الشفرة (رزق، ك. 2016، ص 416 وما بعدها). كما تتعدد أساليب تشفير البيانات، إما باستخدام المفتاح السري " شفرة قيصر "، أو نظام (Data Encryption Standard DES) للتشفير، أو التشفير باستخدام المفتاح العلني، أو التشفير بنظام (Shamir & Adleman RSA ،Rivest) للتشفير، وكذلك أيضا أسلوب التشفير المودع (ESS) (داود، ح. ص 177 وما بعدها). وللتشفير أساليب يتم من خلالها عملية التشفير ذاتها من ذلك شفرة الإحلال، وشفرة الاستبدال، وشفرة الإنتاج، والشفرة الاسمية، وشفرة حقيبة الظهر (عبد الحفيظ، أ. 2002. ص 470 وما بعدها).

ونظرا لأهمية التشفير في حماية أمن البيانات والمعلومات تنص المادة (64) من القانون رقم 10 لسنة 2003 بشأن إصدار قانون تنظيم الاتصالات على أنه " يلتزم مقدمو ومشغلو خدمة الاتصالات والتابعون لهم وكذلك مستخدمو هذه الخدمات بعدم استخدام أية أجهزة لتشفير أجهزة الاتصالات، إلا بعد الحصول على موافقة من كل من الجهاز، والقوات المسلحة، وأجهزة الأمن القومي، ولا يسرى ذلك على أجهزة التشفير الخاصة بالبث الإذاعي والتليفزيوني. ومع مراعاة حرمة الحياة الخاصة للمواطنين التي يحميها القانون يلتزم كل مشغل، أو مقدم خدمة أن يوفر على نفقته داخل شبكة الاتصالات المرخص له بها كافة الإمكانيات الفنية من معدات، ونظم، وبرامج، واتصالات داخل شبكة الاتصالات التي تتيح للقوات المسلحة، وأجهزة الأمن القومي ممارسة اختصاصاتها في حدود القانون، على أن يتزامن تقديم الخدمة مع توفير الإمكانيات الفنية المطلوبة، كما

يلتزم مقدمو، ومشغلو خدمات الاتصالات، ووكلائهم المنوط بهم تسويق تلك الخدمات بالحصول على معلومات، وبيانات دقيقة عن مستخدميها من المواطنين، ومن الجهات المختلفة بالدولة ".

كما تضمنت الفقرة التاسعة من المادة الأولى من قرار وزير الاتصالات وتكنولوجيا المعلومات رقم 109 لسنة 2005 بإصدار اللائحة التنفيذية لقانون التوقيع الالكتروني، وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات على التشفير كمنظومة تقنية حسابية تستخدم مفاتيح خاصة لمعالجة، وتحويل البيانات، والمعلومات المقروءة الكترونيا، بحيث تمنع استخلاص هذه البيانات والمعلومات، إلا عن طريق استخدام مفتاح، أو مفاتيح فك الشفرة. كما تضمنت الفقرة العاشرة من المادة الأولى على تقنية شفرة المفتاحين العام، والخاص المعروفة باسم تقنية شفرة المفتاح العام باعتبارها منظمة تسمح لكل شخص طبيعي، أو معنوي بأن يكون لديه مفتاحين متفردين أحدهما عام متاح الكترونيا، والثاني خاص يحتفظ به الشخص، ويحفظه على درجة عالية من السرية.

وتلجأ جميع أجهزة ومؤسسات الدولة العسكرية والمدنية إتباع سياسة تشفير الوثائق والمعلومات السرية على النحو الذي يحول وصولها إلى الأعداء (عطيات، ع. 2004، ص 146). كما قدمت منظمة التطوير والتعاون الاقتصادي (OECD) عام 1996 خطوطا عامة لسياسة التشفير آخذة بالحسبان المستوى الوطني، والدولي اللازم للتعاون في هذا المجال، ويتفرع عن هذه الإرشادات العديد من المبادئ التي تتمثل في الثقة بشأن طرق التشفير، والاختيار من طرق التشفير، والتطوير السوقي لطرق التشفير، والمعايير المستخدمة لطرق التشفير، وحماية خصوصية البيانات، والوصول القانوني، والحماية القانونية، والتعاون الدولي. وفي بعض الدول كالولايات المتحدة الأمريكية يعد تصدير تكنولوجيا التشفير مقيد بتنظيمات مستنتجة من خلال قانون ضبط التصدير العسكري (Arms Export Control Act) لعام 1949، وقانون إدارة التصدير (Export Administration Act)، والذي يغطى المواد ذات الاستخدام المزدوج المدني والعسكري (البداينة، ذ. 2006. ص 344 وما بعدها).

سادسا: تطوير التشريعات والأنظمة الخاصة بالأمن السيبراني.

يضيف الأمن السيبراني إلى البعد المادي والتكنولوجي لأمن المعلومات بعدين آخرين، أحدهما قانوني يتعلق بوسائل الحماية القانونية لكل ما من شأنه أن يشكل جريمة، والآخر سيأسى يندرج ضمن إطار السياسة الأمنية الداخلية والخارجية، وما تتطلبه من تعزيز وسائل، وأدوات الدفاع من جهة، وتعاون بين الدولة والقطاع الخاص والمحيط الإقليمي من جهة أخرى (جيلانى، ج. & يعقوب، ب. 2021، ص 537). وجدير بالذكر أن هناك سباق مستمر بين شركات تطوير التطبيقات، وبين شركات تقديم أدوات كسر الحماية، وكشف كلمات السر، فشركات تطوير التطبيقات تسعى دائما إلى رفع مستوى أمن التطبيقات، بحيث يصبح كسر حماية ملفاتها في الإصدارات الجديدة أكثر صعوبة عما كان عليه مع ملفات الإصدارات الأقدم، تقابلها شركات كسر الحماية بابتكار طرق، وأدوات اختراق جديدة بعد فترة قصيرة (موسى، م. 2009، ص 316 وما بعدها).

المطلب الثاني

موقف المشرع المصري لمواجهة تحديات الأمن السيبراني

أولا: المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات.

تم تشكيل المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات (EG-CERT) بالجهاز القومي لتنظيم الاتصالات في إبريل 2009، ويتم العمل على مدار الساعة طوال أيام الأسبوع. ويقدم المركز الدعم اللازم لحماية البنية التحتية المعلوماتية الحرجة. ويضم فريق عمل من المتخصصين على أعلى المستويات الفنية، يتولون على مدار الساعة مراقبة الأمن السيبراني، والاستجابة للحوادث، وتحليل الأدلة الرقمية، البرمجيات الخبيثة والهندسة العكسية. ويتمثل الهدف الرئيس للمركز في تعزيز أمن البنية التحتية المصرية للاتصالات والمعلومات، من خلال اتخاذ إجراءات استباقية، وجمع وتحليل المعلومات الخاصة بالحوادث الأمنية، والتنسيق بين الأطراف المعنية في ايجاد الحلول المناسبة للحوادث الأمنية، والتعاون الدولي مع غيرها من فرق الاستجابة لطوارئ الحاسبات والشبكات في الدول الأخرى. وجدير بالذكر أن جهود نيابة الأمن السيبراني بشتى قطاعاتها المتمثلة في (

المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات EG-CERT، وقطاع الحوكمة وإدارة المخاطر GRC، وقطاع تنمية صناعة الأمن السيبراني) ساهمت في تصدر مصر للنسخة الخامسة من المؤشر العالمي للأمن السيبراني (GCI) الصادر عن الاتحاد الدولي للاتصالات (ITU) في سبتمبر 2024، والذي يقيس مستوى الأمن السيبراني في 194 دولة على مستوى العالم ؛ حيث حصلت مصر على العلامة الكاملة في المحاور الخمسة للأمن السيبراني (التقني، التنظيمي، بناء القدرات، التعاون الدولي، التشريعي) محققة 100 نقطة بالتساوي مع 11 دولة أخرى (NTRA، https://egcert.eg/ar / 28 / 8 / 2025).

ثانيا: إصدار العديد من التشريعات لتحقيق الأمن السيبراني.

مع تعاظم أهمية الأمن السيبراني بالتوازي مع جهود الدولة المصرية لتسريع التحول الرقمي وتحقيق رؤية مصر 2030، يبرز تقرير الآفاق العالمية للأمن السيبراني 2025 – الصادر عن المنتدى الاقتصادي العالمي بالتعاون مع أكسنتشر – ضرورة تكاتف الجهود لتعزيز القدرات السيبرانية، سواء على مستوى الجهات الحكومية، أو المؤسسات الخاصة، وترسيخ ثقافة الأمن على كافة المستويات (24 / 7 / 2025 ، https://encc-eg.org/pressroom/press.aspx?id=267). وفي هذا السياق أصدر المشرع المصري العديد من التشريعات، بهدف تطبيق التحول الرقمي في أجهزة ومؤسسات الدولة المختلفة من بينها القانون رقم 15 لسنة 2004 بتنظيم التوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات (الجريدة الرسمية العدد 17 تابع (د) في 22 ابريل سنة 2004)، والقانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات (الجريدة الرسمية العدد 32 مكرر (ج) في 14 أغسطس سنة 2018)، والقانون رقم 151 لسنة 2020 بإصدار قانون حماية البيانات الشخصية (الجريدة الرسمية العدد 28 مكرر (هـ) في 15 يولية سنة 2020)، رغم عدم كفاية وفعالية القواعد القانونية الواردة بها، لمواكبة التطورات التكنولوجية الحديثة (إبراهيم، خ. ص 109). وتهدف هذه التشريعات في مجملها نحو تجريم بعض الأفعال الضارة بالأنظمة الالكترونية المملوكة

للدولة، أو بالشبكة المعلوماتية بوجه عام، والتي تؤثر بشكل مباشر على مرفق الاتصالات الرقمي، ومن ثم الأمن السيبراني داخل الدولة المصرية، وعلى الثقة المفروضة في هذا المرفق، وثقة المواطنين في أجهزة ومؤسسات الدولة المختلفة (أحمد، ط. 2023. ص141).

وقد تضمنت نصوص المواد (12 – 14) من القانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات إضفاء مزيد من الحماية على الأنظمة والبيانات الالكترونية، سواء كانت هذه المعلومات ماسة بالدولة وأجهزتها، أو ماسة بالأفراد. وفي هذا الصدد تنص المادة الثانية من القانون المشار إليه على أنه " **أولا:** مع عدم الإخلال بالأحكام الواردة بهذا القانون، وقانون تنظيم الاتصالات الصادر بالقانون رقم 10 لسنة 2003 يلتزم مقدمو الخدمة بما يأتي (1) حفظ وتخزين سجل النظام المعلوماتي، أو أي وسيلة لتقنية المعلومات، لمدة مائة وثمانين يوما متصلة، وتتمثل البيانات الواجب حفظها وتخزينها فيما يأتي (أ) البيانات التي تمكن من التعرف على مستخدم الخدمة. (ب) البيانات المتعلقة بمحتوى ومضمون النظام المعلوماتي المتعامل فيه، متى كانت تحت سيطرة مقدم الخدمة. (جـ) البيانات المتعلقة بحركة الاتصال. (د) البيانات المتعلقة بالأجهزة الطرفية للاتصال. (هـ) أي بيانات أخرى يصدر بتحديدها قرار من مجلس إدارة الجهاز. (2) المحافظة على سرية البيانات التي تم حفظها وتخزينها، وعدم إفشائها أو الإفصاح عنها بغير أمر مسبب من إحدى الجهات القضائية المختصة، ويشمل ذلك البيانات الشخصية لأي من مستخدمي خدمته، أو أي بيانات أو معلومات متعلقة بالمواقع، والحسابات الخاصة التي يدخل عليها هؤلاء المستخدمون، أو الأشخاص والجهات التي يتواصلون معها. (3) تأمين البيانات والمعلومات، بما يحافظ على سريتها، وعدم اختراقها أو تلفها.

ثانيا: مع عدم الإخلال بأحكام قانون حماية المستهلك، يجب على مقدم الخدمة أن يوفر لمستخدمي خدماته، ولأي جهة حكومية مختصة، بالشكل والطريقة التي يمكن الوصول إليها بصورة ميسرة، ومباشرة، ومستمرة البيانات والمعلومات الآتية (1) اسم مقدم الخدمة وعنوانه. (2) معلومات الاتصال المتعلقة بمقدم الخدمة، بما في ذلك عنوان الاتصال

الالكتروني. (3) بيانات الترخيص لتحديد هوية مقدم الخدمة، وتحديد الجهة المختصة التي يخضع لإشرافها. (4) أي معلومات أخرى يقدر الجهاز أهميتها، لحماية مستخدمي الخدمة، ويصدر بتحديدها قرار من الوزير المختص. **ثالثا:** مع مراعاة حرمة الحياة الخاصة التي يكفلها الدستور، يلتزم مقدمو الخدمة والتابعون لهم، أن يوفروا حال طلب جهات الأمن القومي، ووفق لاحتياجاتها كافة الإمكانيات الفنية التي تتيح لتلك الجهات ممارسة اختصاصاتها وفقا للقانون. **رابعا:** يلتزم مقدمو خدمات تقنيات المعلومات ووكلاؤهم وموزعوهم التابعون لهم المنوط بهم تسويق تلك الخدمات بالحصول على بيانات المستخدمين، ويحظر على غيرهم القيام بذلك ".

ثالثا: إنشاء المجلس الأعلى للأمن السيبراني في مصر.

أصدر رئيس مجلس الوزراء القرار رقم 2259 لسنة 2014 متضمنا على انشاء مجلس أعلى لأمن البنى التحتية للاتصالات وتكنولوجيا المعلومات (https://www.escc.gov.eg/2014.pdf، 27 / 7 / 2025)، يتبع رئاسة مجلس الوزراء يسمى المجلس الأعلى للأمن السيبراني، ويشكل برئاسة وزير الاتصالات وتكنولوجيا المعلومات، وعضوية ممثلي وزارات (الدفاع، الخارجية، الداخلية، البترول والثروة المعدنية، الكهرباء والطاقة المتجددة، الصحة والسكان، الموارد المائية والري، التموين والتجارة الداخلية، الاتصالات وتكنولوجيا المعلومات)، وجهاز المخابرات العامة، والبنك المركزي المصري، عدد ثلاثة من ذوى الخبرة في الجهات البحثية والقطاع الخاص، يرشحهم المجلس، ويصدر بتعيينهم قرار من وزير الاتصالات وتكنولوجيا المعلومات (المادة الأولى). ويختص المجلس بوضع استراتيجية وطنية لمواجهة الأخطار والهجمات السيبرانية، والاشراف على تنفيذ تلك الاستراتيجية، وتحديثها تمشيا مع التطورات التقنية المتلاحقة (المادة الثانية). ويقوم أعضاء المجلس بمراجعة مهامه، وتشكيل أمانة فنية تنفيذية تابعة له، وما يتبعها من إدارات ومراكز في جلساته الأولى، ويصدر بتشكيلها وتحديد اختصاصاتها ومعاملاتها المالية قرار من رئيس مجلس الوزراء (المادة الثالثة).

كما أصدر رئيس مجلس الوزراء القرار رقم 994 لسنة 2017 (الجريدة الرسمية العدد 17 مكرر (ب) في 2 مايو سنة 2017) ونص في مادته الأولى على ضرورة التزام كافة الجهات الحكومية بكافة مستوياتها، وشركات قطاع الأعمال العام بتنفيذ قرارات وتوصيات المجلس الأعلى للأمن السيبراني فيما يتعلق بتأمين البنية التحتية الحرجة للاتصالات وتكنولوجيا المعلومات الخاصة بها، واتخاذ كافة الاجراءات الفنية والادارية لمواجهة الأخطار والهجمات السيبرانية، وتنفيذ الاستراتيجية الوطنية للأمن السيبراني. كما تضمنت المادة الثانية بالنص على أن يتولى وزير الاتصالات وتكنولوجيا المعلومات وضع وتحديد قواعد وإجراءات تأمين البنية المعلوماتية الحرجة لقطاعات الدولة، ومتابعة تنفيذ قرارات وتوصيات المجلس الأعلى للأمن السيبراني وتطبيق أحكام هذا القرار. وتضمنت المادة الثالثة بالنص على أنه مع عدم الاخلال بأي عقوبات جنائية قد تنشأ نتيجة وقوع أضرار جسيمة تتعلق بعدم الالتزام بتأمين البنية التحتية الحرجة للاتصالات وتكنولوجيا المعلومات، يسأل تاديبيا كل موظف أو عامل يخالف قرار المجلس الأعلى للأمن السيبراني.

رابعا: قرار بتحديد اختصاصات المجلس الأعلى للأمن السيبراني.

يختص المجلس الأعلى للأمن السيبراني طبقا لنص المادة الأولى من قرار رئيس مجلس الوزراء رقم 1630 لسنة 2016 (https://www.escc.gov.eg/2016.pdf، 25 / 7 / 2025) بالمهام التالية 1- اعتماد البنى التحتية للاتصالات والمعلومات الحرجة في كافة قطاعات الدولة بالتنسيق مع الجهات المسئولة والأجهزة المنظمة للقطاعات المختلفة. 2- اعتماد أطر واستراتيجيات وسياسات تأمين البنى التحتية للاتصالات والمعلومات الحرجة لكافة قطاعات الدولة، وآليات متابعة تنفيذها بالتنسيق مع الجهات المسئولة والأجهزة المنظمة للقطاعات المختلفة. 3- وضع أطر تقييم ومتابعة تأمين البنى التحتية للاتصالات والمعلومات الحرجة في القطاعات المختلفة. 4- وضع خطط وبرامج تنمية صناعة الأمن السيبراني والتنمية البشرية، وإعداد الكوادر اللازمة، لمواجهة التحديات المتزايدة، والمخاطر السيبرانية، وآليات لتنفيذ برامج الحماية والتأمين في شتى القطاعات. 5- وضع إطار للبحث العلمي والتطوير والابتكار في مجال الأمن السيبراني،

وآليات تنفيذه، بالتنسيق مع الجهات ذات الصلة، للمساهمة في تأمين منظومة الأمن السيبراني المصري. 6- التعاون والتنسيق اقليميا ودوليا مع الجهات ذات الصلة في مجال الأمن السيبراني، وتأمين البنى التحتية الحرجة للاتصالات والمعلومات، سواء الجهات الحكومية وغير الحكومية، ومؤسسات الأعمال، لتبادل الخبرات والمعارف، وخاصة للتنسيق، وتبادل المعلومات، لمواجهة الهجمات السيبرانية والتصدي لها.

7- إعداد توصيات بأية تدخلات تشريعية لازمة لتأمين البنى التحتية للاتصالات والمعلومات وللأمن السيبراني، والمشاركة في اللجان الوطنية ذات الصلة. 8- وضع المعايير الملزمة لكافة الجهات كحد أدنى لتأمين البنى التحتية للاتصالات والمعلومات الحرجة، والزامها بإعداد خطط الطوارئ، واستمرار الأعمال، لمواجهة الهجمات السيبرانية، والتصدي لها مع التدريب على تفعيل تلك الخطط بصورة دورية، وإفادة المجلس الأعلى عنها. 9- وضع آليات رصد المخاطر والمتابعة الدورية للهجمات السيبرانية، وتوزيع الأدوار على المستوى الوطني، واخطار ومتابعة قيام الجهات المستهدفة بالاستعداد، والتصدي لتلك المخاطر (وحدة الانذار المبكر، والتدخل مع المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات " السيرت المصري ". 10- وضع وتفعيل معايير وآليات لتحديد الاعتماديات البينية الموجودة بين عناصر البنية الأساسية الحرجة، والقائمين عليها، وما يقع خارجها، بحيث يتم تجنب التأثيرات المتتالية. 11- إقرار مواصفات الأمن السيبراني القياسية للأنظمة والأجهزة والتطبيقات في مختلف القطاعات، وإضافة معايير الجودة السيبرانية بالتنسيق مع الجهات ذات الصلة. 12- اعتماد توصيف التقويم الأمنى للقائمين على تشغيل البنى التحتية للاتصالات والمعلومات الحرجة. 13- وضع آلية لمتابعة وتأمين، وحماية الموافقة الحكومية الرسمية على الانترنت.

ويشكل المكتب التنفيذي للمجلس الأعلى للأمن السيبراني طبقا لنص المادة الثانية برئاسة... عضو المجلس الأعلى للأمن السيبراني وعضوية أعضاء المجلس ممثلي الوزارات والجهات الآتية: (وزارة الدفاع، وزارة الخارجية، وزارة الداخلية، وزارة الاتصالات وتكنولوجيا المعلومات، جهاز المخابرات العامة). ويختص المكتب التنفيذي بالآتى 1-

الاشراف العام على تنفيذ أعمال المجلس والخطط التي يقرها في ضوء الاستراتيجيات والسياسات المحددة. 2- أعمال المتابعة واعداد توصيات ومقترحات وخطط تنفيذية فيما يتعلق بمهام المجلس. 3- التنسيق مع مختلف القطاعات والجهات ذات الصلة – داخليا وخارجيا – لتنفيذ قرارات وتوجيهات المجلس. 4- دراسة التقارير والطلبات المقدمة إلى المجلس وإعداد التوصيات الملائمة بشأنها. 5- عمل الدراسة اللازمة للهيكل التنظيمي للمجلس وإدارته التنفيذية واعداد موازنته المالية 6- القيام بأي أعمال أخرى يقرها المجلس الأعلى للأمن السيبراني.

وطبقا للمادة الثالثة تشكل الأمانة الفنية للمجلس الأعلى للأمن السيبراني برئاسة... المدير التنفيذي للمركز الوطني للاستعداد لطوارئ الحاسبات والشبكات (EG CERT)، وعضوية ممثلي الوزارات والجهات التالية: (وزارة الدفاع، وزارة الداخلية، وزارة الاتصالات وتكنولوجيا المعلومات، جهاز المخابرات العامة). وتتولى الأمانة الفنية القيام بالآتي 1- القيام بالأعمال والدراسات الفنية التي يطلبها المجلس ومكتبه التنفيذي وإعداد التقارير الفنية الدورية للمجلس. 2- تشكيل إدارة لنظم المعلومات والبرمجيات القومية في مجال الأمن السيبراني. 3- تشكيل إدارة للأزمات الخاصة بنظم الاتصالات والمعلومات الحرجة. 4- تشكيل لجنة فنية لمتابعة تأمين المواقع الحكومية على الانترنت. 5- تنظيم وإطلاق حملات وطنية دورية للتعريف بمخاطر الاختراقات السيبرانية لنظم التحكم الصناعية في مختلف القطاعات وخاصة في قطاع الطاقة والمرافق العامة. 6- تنظيم ورش عمل ودورات للتوعية بالأمن السيبراني على المستوى القطاعي وخاصة للمسئولين من الصف الثاني والثالث، مع التركيز على أهمية التوازن بين تحقيق الاستمرارية ورفع مستوى التأمين.

خامسا: الاستراتيجية الوطنية للأمن السيبراني.

تتضمن الاستراتيجية عددا من البرامج التي تدعم أهداف الأمن السيبراني... وقد تم وضع الخطة مرتبة الأهداف مع التأكيد على أهمية الشراكة المجتمعية بين الأجهزة الحكومية والقطاع الخاص ومؤسسات الأعمال والمجتمع المدني لتنفيذ الأهداف والإجراءات ذات

الصـلة، بما يدعم التحول نحو اقتصـاد رقمى متكامل، يحقق طموحات المواطنين في تنمية اجتماعية واقتصادية شاملة، ويحمى مصالحهم، ويحافظ على مصالح الدولة العليا، ويسهم في نهضـتها وازدهارها. وتعتمد الاسـتراتيجية على العديد من البرامج أهمها 1- برنامج لتطوير الاطار التشريع الملائم لأمن الفضاء السيبراني ومكافحة الجرائم السيبرانية وحماية الخصوصية والهوية الرقمية. 2- برنامج تطوير منظومة وطنية لحماية أمن الفضاء السيبراني وتأمين البنى التحتية للاتصـالات وتكنولوجيا المعلومات، وذلك باعداد وتفعيل ما يعرف بفرق الاسـتجابة لطوارئ الحاسـب. 3- برنامج لحماية الهوية الرقمية (برنامج المواطنة الرقمية)، وتفعيل البنى التحتية اللازمة لدعم الثقة في التعاملات الالكترونية بوجه عام، وفي الخدمات الحكومية الالكترونية بوجه خاص مثل بنية المفتاح المعلن التي يعتمد عليها التوقيع الالكتروني. 4- برنامج لاعداد الكوادر البشرية والخبرات اللازمة لتفعيل منظومة الأمن السـيبراني في مختلف القطاعات بالتعاون والشرـاكة بين الجهات الحكومية والقطاع الخاص والجامعات ومؤسـسـات المجتمع المدني اعتمادا على التجربة الرائدة التي قام بها الجهاز القومي لتنظيم الاتصـالات. 5- برنامج لدعم البحث العلمي والتطوير وتنمية صـناعة الأمن السـيبراني من خلال دعم برامج ومشرـوعات التعاون بين الجهات البحثية والشرـكات الوطنية، وخاصـة في مجال تحليل البرمجيات الخبيثة... الخ. 6- إنشـاء مراكز أو معامل وطنية لاعتماد الأنظمة والأجهزة والبرمجيات والتطبيقات المسـتخدمة في الجهات الحيوية، وفي البنى التحتية الهامة. 7- برنامج للتوعية المجتمعية بالفرص والمزايا التي تقدمها الخدمات الالكترونية للأفراد والمؤسـسـات والجهات الحكومية، وبأهمية الأمن السـيبراني، لحماية تلك الخدمات من المخاطر والتهديدات التي قد تواجهها. (الوزراء، م. 2017 – 2021، ص 1 وما بعدها)

النتائج والتوصيات

تناولنا بالبحث والدراسة تحديات الأمن السيبراني في ضوء تطور تكنولوجيا الذكاء الاصطناعي في وقت تتسارع فيه التقنية والتحول الرقمي، بحيث أصبح الأمن السيبراني أحد أكثر القضايا أهمية، لما يمثله من حماية أساسية للأنظمة والشبكات، من الوصول غير المصرح به، والهجمات السيبرانية المحتملة، لاسيما مع تزايد الاعتماد على التكنولوجيا الرقمية في جميع جوانب الحياة من الأعمال التجارية إلى الخدمات الحكومية، وازدياد المخاطر المرتبطة بالهجمات السيبرانية، وتتنوع هذه التهديدات بين الفيروسات، والبرمجيات الخبيثة إلى هجمات حجب الخدمة، مما فرض على مؤسسات الدولة حماية بيانتها من أية اختراقات، أو تجاوزات، أو قرصنة رقمية محتملة. وعلى ضوء ذلك، فقد توصل الباحث إلى العديد من النتائج الهامة تتمثل في الآتي:

أولا: أفرز التطور العلمي والتكنولوجي تصنيع الإنسان آلة، تساعده على إنجاز المهام بشكل أكثر دقة، وسرعة، ومرونة إكتسبت صفة الذكاء التي يتمتع بها الإنسان، أطلق عليها الذكاء الاصطناعي، مما يقتضي ضرورة إرساء قواعد قانونية، تتناسب مع طبيعة هذه التقنية التي من المتوقع لها أن تسود العالم أجمع.

ثانيا: انتشار تطبيقات التكنولوجيا الحديثة للاتصال بشكل واسع، سواء على الهاتف المحمول أو الحاسب الآلي ؛ إذ تشهد تزايدا واقبالا، بسبب تطور التقنية، وازدياد أساليب التواصل التي أصبحت تتحكم في أساليب إدارة الحياة العصرية، مع تزايد الأفكار والحاجة إلى تطبيقها بصورة رقمية ومبرمجة.

ثالثا: يعد الأمن الركيزة الأساسية للمجتمع، بحيث لا يمكن تصور نمو أي نشاط بعيدا عن تحققه على المستويين التقني والقانوني، والذي تحول مع بروز مجتمع المعلومات والفضاء السيبراني إلى أحد أهم القطاعات الخدمية التي تشكل قيمة مضافة، ودعامة أساسية لأنشطة الحكومات والأفراد على حد السواء.

رابعا: تزايد الإعتماد على التكنولوجيا الرقمية في جميع جوانب الحياة، مما دعا الدول النشطة رقميا أن تسعى جاهدة، لتوفير الأمن لمختلف البرامج والتطبيقات، وكذا الأجهزة

الالكترونية المستخدمة، والأنظمة والشبكات المعمول بها، بهدف حماية البيانات من أية اختراقات، أو تجاوزات، أو قرصنة رقمية محتملة.

وبناء على ما سبق فقد توصل الباحث إلى التوصيات الآتية

أولا: العمل على إنشاء منظومة وطنية لحماية أمن الفضاء السيبراني، وتأمين البنية التحتية للاتصالات وتكنولوجيا المعلومات ونظم قواعد البيانات، مع العمل على إصدار قانون الأمن السيبراني لرفع كفاءة الأمن السيبراني في المؤسسات الحائزة المشغلة للبنية التحتية الحرجة.

ثانيا: اعادة صياغة التشريعات المختصة بمكافحة الجرائم السيبرانية ومراجعتها أولا بأول، مع تشديد العقوبات بشأن الجرائم الواردة بها، وإعادة النظر في تصنيف الجرائم، والعمل على تكييفها لتتوائم مع التطورات التكنولوجية الحديثة.

ثالثا: نشر الوعى داخل المجتمع، بشأن الأمن السيبراني، من خلال تنظيم ندوات وحملات توعوية حول مخاطر التعامل مع الوسائل الالكترونية الحديثة، وتحفيزهم على الاستفادة من ايجابياتها.

رابعا: العمل على تنقيح المستوى الإعلامي الفكري المقدم على وسائل الاعلام المسموعة والمرئية والمقروءة، ووسائل الاتصال الحديثة، مع حجب كافة المواقع التي تتعارض مع القيم والمبادئ الأصلية للمجتمع المصري.

خامسا: أهمية العمل على دعم وتطوير البرامج المختصة بحماية الأمن السيبراني، مع ضرورة الانتقال من الاستراتيجية الدفاعية إلى الاستراتيجية الوقائية والاستباقية في مجال الأمن السيبراني.

سادسا: إدراج موضوع الأمن السيبراني ضمن المقررات الأساسية في الكليات والمعاهد المتخصصة، لتوعية الطلاب بشأن مخاطر الأمن السيبراني، لعدم الوقوع فريسة، أو ضحية لأي من صور الجرائم السيبرانية.

سابعا: تعزيز التعاون بين أجهزة ومؤسسات الدولة المختلفة، والهيئات والمؤسسات الدولية المعنية ذات الصلة لمواجهة الجرائم السيبرانية، بما في ذلك التعاون التقني والأمني... الخ.

ثامنا: العمل على تدريب القضاة، وأعضاء النيابة العامة، وضباط الشرطة، والمحامون على التحديات والصعوبات التي تواجه الأمن السيبراني.

تاسعا: ضرورة مراجعة الاستراتيجية المعنية بالأمن السيبراني باستمرار، والعمل على تحديثها لمواكبة التحديات التي تواجه الأمن السيبراني.

عاشرا: الاهتمام بمختلف أنماط الجريمة المنظمة في مؤسسات التشريع الوطني، وادراجها ضمن مختلف النصوص القانونية، بما يتلاءم والمتغيرات الدولية.

الحادي عشر: تحسين استخدام الموارد، والاستفادة من أحدث التقنيات، بما يمكن المؤسسات من تعزيز وضعها الأمني، دون تكلفة باهظة، من خلال نشر برامج أمن سيبراني متقدمة، وتطبيق الأتمتة، والاستفادة من الحلول القائمة على الذكاء الاصطناعي لتعزيز عملياتها الأمنية.

قائمة المراجع

أولا: المراجع العربية.

(أ) المؤلفات العامة.

منصور، أحمد. (2024). الذكاء الاصطناعي والأمن القومي. دار التعليم الجامعي.

غيطاس، جمال. (2007). أمن المعلومات والأمن القومي. الطبعة الأولى. دار نهضة مصر للطباعة والنشر والتوزيع.

الغثبر، خالد. (2009). أمن المعلومات بلغة ميسرة. الطبعة الأولى. مركز التميز للأمن المعلوماتي.

إبراهيم، خالد. (2022). التنظيم القانوني للذكاء الاصطناعي. الطبعة الأولى. دار الفكر الجامعي.

البداينة، ذياب. (2006). الأمن وحرب المعلومات. الطبعة الأولى. دار الشروق للنشر والتوزيع.

سالم، صلاح. (2003). تكنولوجيا المعلومات والاتصالات والأمن القومي للمجتمع، الطبعة الأولى، عين للدراسات والبحوث الإنسانية والاجتماعية.

عطية، طارق. (2009). الأمن المعلوماتي (النظام القانوني لحماية المعلوماتي). الطبعة الأولى. دار الجامعة الجديدة.

عطيات، عبد الرحمن. (2004).، أمن الوثائق والمعلومات. الطبعة الأولى. جامعة نايف للعلوم الأمنية.

العريان، محمد. (2004). الجرائم المعلوماتية. الطبعة الأولى. دار الجامعة الجديدة للنشر.

(ب) المؤلفات المتخصصة.

أحمد، أشرف. (2014). إستراتيجية أمن المعلومات (سرى للغاية). الطبعة الأولى. مطابع الشرطة للنشر والتوزيع.

طنطاوي، إبراهيم. (2003). أحكام التجريم والعقاب في قانون تنظيم الاتصالات. دراسة تأصيلية وتحليلية لنصوص القانون رقم 10 لسنة 2003. دار النهضة العربية.

داود، حسن. (2000). الحاسب وأمن المعلومات. مركز البحوث بمعهد الإدارة العامة بالسعودية.

مهدى، طارق. (2023). الذكاء الاصطناعي ومكافحة الارهاب. الطبعة الأولى. دار الفكر الجامعي.

أحمد، طارق. (2023). التحول الرقمي ما بين المعاملات المدنية والحكومة الالكترونية والجرائم السيبرانية. مركز المحمود لتوزيع الكتب القانونية.

علام، محمد. (2024). الإستراتيجية القانونية للذكاء الاصطناعي وتطبيقاته. دروب المعرفة للنشر والتوزيع.

موسى، مصطفي. (2009)، الإرهاب الالكتروني دراسة (قانونية – أمنية – نفسية – اجتماعية). الطبعة الأولى. دار الكتب والوثائق.

بيكر، هال. (1998). سرية وكمال المعلومات (المفاهيم – البناء – الإدارة). ترجمة عبد الفتاح الشاعر. الطبعة الأولى. مركز الإسكندرية للوسائط الثقافية والمكتبات.

ثانيا: الرسائل العلمية.

فكرى،أيمن. (2006). جرائم نظم المعلومات. دراسة مقارنة. رسالة دكتوراه. كلية الحقوق. جامعة المنصورة.

على، رشدى (2009). الحماية الجنائية للمعلومات على شبكة الانترنت. دراسة مقارنة. رسالة دكتوراه. كلية الحقوق. جامعة القاهرة.

جاد، رحاب. (2023). فلسفة التكنولوجيا مفهومها وطبيعتها. رسالة دكتوراه. كلية الآداب. جامعة المنصورة.

الكتبى، عشبة. (2023). جرائم الذكاء الاصطناعي وتأثيراتها على الأمن القومي. دراسة مقارنة. رسالة دكتوراه. كلية الحقوق. جامعة المنصورة.

العازمى، فهد. الإجراءات الجنائية المعلوماتية. رسالة دكتوراه. كلية الحقوق. جامعة عين شمس.

عبود، قاسم. (2017). الحق في الوصول إلى المعلومات التأرجح بين الإتاحة والتقييد. دراسة مقارنة. رسالة ماجستير في الأعمال. كلية الحقوق والعلوم السياسية والإدارية. الفرع الأول الجامعة اللبنانية.

رزق، كيرلس. (2016). الحماية القانونية لسرية الاتصالات العادية والالكترونية. رسالة دكتوراه. كلية الحقوق. جامعة بنى سويف.

علام، مها. (2014). ثورة المعلومات والأمن القومي. دراسة حالة الولايات المتحدة الأمريكية. رسالة مقدمة للحصول على درجة الماجستير في العلوم السياسية. كلية الاقتصاد والعلوم السياسية. جامعة القاهرة.

أحمد، نشوى. (2012). حماية الحقوق والحريات الشخصية في مواجهة التقنيات الحديثة (البيانات الشخصية، المراسلات والمحادثات الشخصية، الحق في الصورة). دراسة مقارنة. رسالة دكتوراه. كلية الحقوق. جامعة المنصورة.

العامرى، هدى. (2024). دور الحكومة الالكترونية في تعزيز الشفافية. رسالة دكتوراه. كلية الحقوق. جامعة المنصورة.

على، هدى. (2022) استخدام وسائل الذكاء الاصطناعي في الإثبات الجنائي. رسالة دكتوراه. كلية الحقوق. جامعة المنصورة.

ثالثا: الدوريات المتخصصة.

حمودة، أحمد. (2022). لوازم التحول الرقمي " الأمن السيبراني نموذجا "، رؤية فقهية مقاصدية، مجلة الشريعة والقانون، كلية الشريعة والقانون بالقاهرة جامعة الأزهر، العدد (40).

عبد الحفيظ، أيمن. (2002). المخاطر التي تتعرض لها شبكة الانترنت وسبل حمايتها. مجلة مركز بحوث الشرطة. أكاديمية الشرطة. العدد (22).

بسيونى، آمال. (2022). دور التحول الرقمي في مواجهة جائحة كورونا " الأبعاد – التحديات – رؤية مستقبلية وتجارب ناجحة ". مجلة التجارة والتمويل. كلية التجارة جامعة طنطا.

محمد، المعتز. (1998). المعلومات كأساس للتنبؤ والتخطيط الأمني. مجلة مركز بحوث الشرطة. أكاديمية الشرطة. العدد (13).

محمد، العيدانى. (2024). التهديدات السيبرانية وجرائم المعلومات. مجلة الاجتهاد للدراسات القانونية والاقتصادية. المركز الجامعي.. معهد الحقوق والعلوم السياسية. المجلد (13)، العدد (1).

الخبيزى، بدر. (2023). تحديات وتهديدات الأمن السيبراني وكيفية التغلب عليها. حوليات آداب عين شمس. المجلد (51)، عدد يوليو – سبتمبر.

جيلانى، جلالى. & يعقوب، بلشير. (2021). رهانات الأمن السيبراني الوطني في ظل التحول الرقمي. قراءة في التأصيل المعرفي واستراتيجية المواجهة المعرفية. مجلة كلية القانون الكويتية العالمية. المجلد (10). العدد (37).

الشهري، حسن. (2012). الأنظمة الرقمية المطورة لحفظ وحماية سرية المعلومات من التجسس. المجلة العربية للدراسات الأمنية والتدريب. العدد (56). المجلد (28).

لخضر، حرز الله. (2023). جرائم الانترنت وتحديات الأمن السيبراني: دراسة في متغيرات الجريمة ومقارباتها العلاجية. مجلة المفكر. كلية الحقوق والعلوم السياسية. جامعة محمد خيضر بسكرة. العدد (1). المجلد (18).

القاضى، رامى. (2021). نحو إقرار قواعد المسئولية الجنائية والعقاب على إساءة استخدام تطبيقات الذكاء الاصطناعي. مجلة البحوث القانونية والاقتصادية. كلية الحقوق. جامعة المنصورة. عدد خاص.

جربوعة، عادل. & بوطمين، عبد الجبار. (2023). الفضاء الرقمي والأمن السيبراني. مجلة العلوم الإنسانية. جامعة منتوري قسطنطينية بالجزائر. المجلد (34)، العدد (3).

الهدى، قادرى. (2023). الجريمة السيبرانية وآليات مكافحتها – مواجهة تحديات الأمن السيبراني. المجلة الجزائرية للحقوق والعلوم السياسية. معهد العلوم القانونية والادارية. المجلد (8). العدد (1).

بن برغوث، ليلى. (2023). الأمن السيبراني وحماية خصوصية البيانات الرقمية في الجزائر في عصر ـ لتحول الرقمي والذكاء الاصـطناعي (التهديدات، والتقنيات، والتحديات، وآليات التصدي). المجلة الدولية للاتصال الاجتماعي. كلية العلوم الإنسانية والاجتماعية. جامعة عبد الحميد بن باديس مستغانم. المجلد (10). العدد (1).

عبد العليم، محمد. (2024). المسـئولية الجنائية الناشـئة عن جرائم تقنيات الذكاء الاصطناعي (AI). مجلة الدراسات القانونية والاقتصادية. المجلد (10). العدد (1).

حسـكر، مراد. (2022). إشـكالية تطبيق أحكام المسـئولية الجنائية على جرائم الذكاء الاصـطناعي. مجلة الحقوق والعلوم الإنسـانية. جامعة زيان عاشـور. المجلد (15). العدد (1).

آل خليفة، مى. (2012) دور التحول الرقمي في تحقيق الأمن السـيبراني. دراسـة تطبيقية على وزارة العدل في قطر. مجلة البحوث الإدارية. أكاديمية السـادات للعلوم الإدارية. المجلد (35). العدد (3).

المزروعى، ناصر. (2024). أهمية دور الأمن السـيبراني في تحقيق الأمن الالكتروني بدولة الامارات العربية المتحدة. مجلة الباحث للدراسـات والأبحاث القانونية والاقتصـادية والعلوم الانسانية والشرعية. محمد قاسمى. العدد (71).

عدلى، هدى. (2023). واقع وتحديات الأمن السـيبراني واجراءاته. مجلة قانونك المغربية. العدد (16).

سعيد، وليد. (2022).، المسئولية الجنائية الناشئة عن تطبيقات الذكاء الاصطناعي. مجلة العلوم القانونية والاقتصادية. كلية الحقوق جامعة عين شمس. العدد (2). المجلد (64).

دهشـان، يحيى. (2022). جرائم الذكاء الاصـطناعي وآليات مكافحتها. مجلة روح القوانين. كلية الحقوق جامعة طنطا. العدد (100). الجزء (1).

رابعا: التقارير والنشرات.

الرفاتي، أ.، الحرب الجديدة.. السايبر الإيراني يقلق تل أبيب ؛ تقرير صحفي منشور بتاريخ 7 / 8 / 2025 على الموقع الالكتروني التالي https: / /www.almayadeen.net.

أكاديمية الجزيرة العالمية، الأمن السيبراني: حماية العالم الرقمي ؛ منشور بتاريخ 24 / 7 / 2025 على الموقع الالكتروني التالي https: / /aljazeeraacademy.com.

الأمم المتحدة، الجمعية العامة تعتمد اتفاقية تاريخية بشأن الجرائم الالكترونية ؛ منشور بتاريخ 331 / 7 / 2025 على الانترنت.

داسكال، ج. & مايو، د.، اتفاقية بودابست: ما هي وكيف يتم تحديثها ؟ ؛ منشور بتاريخ 3 / 7 / 2025 على الموقع الالكتروني التالي

https: / /www-crossborderdataforum-org.translate.goog /budapest-convention-what-is-it-and-how-is-it-being-updated /?_

سومير لينك، مستقبل الأمن السيبراني في عصر التحول الرقمي، منشور بتاريخ 24 / 7 / 2025 على الموقع الإلكتروني التالي https: / /sumer-link.com .

فضاء الذكاء الاصطناعي، كيف تحمى نفسك من التهديدات الأمنية المرتبطة بتقنيات الذكاء الاصطناعي ؟ ؛ منشور بتاريخ 18 / 8 / 2025 على الموقع الالكتروني التالي

https: / /www.fada2-ai.com /2025 /02 /The-security-challenges-of-artificial-intelligence..html

العساني، غ.، السرية في العمل الإداري ؛ بحث منشور على الموقع الالكتروني التالي

http: / /elsada.net /27501

ملال، ل. & ادعمى، س.، الذكاء الاصطناعي وتهديد الأمن القومي للدول ؛ منشور بتاريخ 9 / 8 / 2025 على الموقع الالكتروني التالي https: / /caus.org.lb .

السيد، هـ.، خسائرها تريليون دولار سنويا... خبير يكشف تفاصيل التأمين ضد الهجمات السيبرانية؛ تقرير صحفي منشور بتاريخ 26 / 7 / 2025 على الموقع الالكتروني التالي https: / /www.youm7.com.

المجلس الوطني المصري للتنافسية، الآفاق العالمية للأمن السيبراني 2025: دليل شامل لتعزيز القدرة التنافسية الرقمية في مصر، منشور بتاريخ 24 / 7 / 2025 على الموقع الالكتروني التالي https: //encc-eg.org /pressroom /press.aspx?id=267.

المركز الأوروبي لدراسات مكافحة الارهاب والاستخبارات، أمن قومى – توظيف الذكاء الاصطناعي داخل أجهزة الاستخبارات وداخل الجماعات المتطرفة (ملف) ؛ منشور بتاريخ 8 / 8 / 2025 على الموقع الالكتروني التالي https: //www.europarabct.com.

المركز القومي لتنظيم الاتصالات NTRA، المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات ؛ منشور بتاريخ 28 / 8 / 2025 على الموقع الالكتروني التالى https: //egcert.eg /ar/

خامسا: مجموعة القوانين واللوائح.

الاستراتيجية الوطنية للأمن السيبراني.

الدستور المصري الصادر عام 2014.

القانون رقم 10 لسنة 2003 بشأن إصدار قانون تنظيم الاتصالات.

القانون رقم 15 لسنة 2004 بتنظيم التوقيع الالكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات

القانون رقم 151 لسنة 2020 بإصدار قانون حماية البيانات الشخصية.

القانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات.

القانون رقم 5 لسنة 2022 بإصدار قانون تنظيم وتنمية استخدام التكنولوجيا المالية في الأنشطة المالية غير المصرفية.

قرار رئيس مجلس الوزراء رقم 1630 لسنة 2016 بشأن اختصاصات المجلس الأعلى للأمن السيبراني.

قرار رئيس مجلس الوزراء رقم 2259 لسنة 2014 بإنشاء المجلس الأعلى للأمن السيبراني.

قرار رئيس مجلس الوزراء رقم 994 لسنة 2017 بشأن ضرورة التزام كافة الجهات الحكومية بكافة مستوياتها وشركات قطاع الاعمال العام بتنفيذ قرارات وتوصيات المجلس الأعلى للأمن السيبراني

قرار وزير الاتصالات وتكنولوجيا المعلومات رقم 109 لسنة 2005 بإصدار اللائحة التنفيذية لقانون التوقيع الالكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات.

سادسا: أحكام القضاء.

نقض جنائى، الطعن رقم 50733 لسنة 85 قضائية، جلسة 22 / 11 / 2016، مكتب فنى، س 67 ؛ منشور بتاريخ 28 / 8 / 2025 على الموقع الرسمى لمحكمة النقض المصرية على العنوان الالكتروني التالى

https://www.cc.gov.eg/judgment_single?id=111363462&&ja=280554

نقض جنائى، الطعن رقم 3224 لسنة 90 قضائية، جلسة 5 سبتمبر سنة 2021، المستحدث من المبادىء الصادرة من الدوائر الجنائية بمحكمة النقض من أول أكتوبر 2020 لغاية نهاية سبتمبر سنة 2021 ؛ منشور بتاريخ 28 / 8 / 2025 على الموقع الرسمى لمحكمة النقض المصرية على العنوان الالكتروني التالى

https://www.cc.gov.eg/wp-content/uploads/2022

سابعا: الاتفاقيات والمواثيق الدولية.

الإتفاقية المتعلقة بالجريمة الالكترونية (بودابست 2001).

اتفاقية للأمم المتحدة لمكافحة الجرائم الالكترونية2024.

إتفاقية مجلس أوروبا بشأن الجرائم الالكترونية.

اللائحة العامة لحماية البيانات GDPR بالاتحاد الأوروبى.

ثامنا: المراجع الأجنبية.

(A) References English.

Lakshminath ،A. & Sarda ،M. (2012). DIGITAL REVOLUTION AND ARTIFICIAL INTELLIGENCE – CHALLENGES TO LEGAL EDUCATION AND LEGAL RESEARCH. Law Journal. Volume (2). P.

Metin ،B. & özhan ،F. & Wynn ، (2024). M. Digitalisation and Cybersecurity: Towards an Operational Framework. Electronic. (13). (4226). P.

Khan ، C. (2024). Criminal Liability Of Artificial Intelligence Frome The Respective Of Criminal Law: An Evaluation In The Context Of The General Theory Of Crime And Fundamental Principles. International Journal Of Eurasia Social Science. Vol (15). Issue (55). P.

DataGuard ، Cyber Security Strategy – How to Plan and Develop it ? Posted 18 / 8 / 2025 On the following website
https://www-dataguard-com.translate.goog/cyber-security/strategy/?
GDPR: General Data Protection Regulation. Posted 31 / 7 / 2025 on the following website https://www-gdpreu org.translate.google/?
Groot ، J. What Is Data Encryption ? (Definition ، Best Practices and More) ، FORTRA ، Published 29 / 7 / 2025 on the following website
https://www.digitalguardian.com/blog/what-data-encryption
Lerner ، K. & Lerner ، B. (2004). Encyclopedia Of Espionage ، Intelligence And Security. Volume (2). F-Q ، Thomson U S A.
Vdovichena ، O. (2024). Digital Technologies and Cybersecurity in the Strategy of Post –War Economic Recover. AESSRA. Economic Affairs. V 69 (03). P.
Osoba ، O. & Welser ، W. The Risk Of Artificial Intelligence to Security And The Future Of Work. Prespective. Rand Corporation. P 6 ; Published 11 / 8 / 2025 On the following website
https://www.rand.org/pubs/perspectives/PE237.html
Silobreaker ، Artificial Intelligence in Threat Intelligence. Posted 8 / 8 /2025 on the following website
https://www-silobreaker-com.translate.goog/glossary/ai-in-threat-intelligence/?
SwntinelOne ، Top 5 Cyber Security Challenges. Posted 18 / 8 / 2025 On the following website
https://www-sentinelone-com.translate.goog/cybersecurity-101/cybersecurity/cyber-security-challenges/?
University ، V. Artificial Intelligence (AI) Challenges and Advantages in National Security. Posted 8 / 8 / 2025 On the following website
https://onlinewilder-vcu-edu.translate.goog/blog/ai-challenges-and-opportunities-national-security/?

(B) Références français.

Moatti ، D. (1998). La Communication Informatique En Toute Liberte. Histoire Et éthique De L´Information Numérique. Association Des Publications De La Faculté Des Lettres De Nice.
Champy ، G. (1992). La Fraude Informatique.Tome (1). Presses Universitaires DAix-Marseille. Facculte De Droit Et De Science Polotique.
Catala ، P. (1983) Informatique Et Droit Penal. Travaux De L´Institute De Sciences Criminelles De Poitiers. Volume (IV). Editions Cujas. Paris.