«القوانين والتشريعات الحاكمة لحماية أمن المعلومات»

« دراسة مقارنة»

د. السيد رمضان عبد الصمد عشماوي*

مستخلص

الحقيقة التي لا يساورها أدنى شك أن موضوع الأمن المعلوماتي يحتل أهمية بالغة خاصة في عصرنا الحالي، وهو ما آمن به المشرع المصري في دستور عام 2014م، وذلك من خلال المادة (31) منه، حيث نصَّ على أن: «أمن الفضاء المعلوماتي جزء أساسي من منظومة الاقتصاد والأمن القومي، وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه، على النحو الذي ينظمه القانون».

بَيْدَ أن الأحداث التي نعرفها خير شاهد على أن الإعلام جزء وأداة من أدوات تحقيق الأمن القومي التي بدورها تمثل لُبَّ وجوهر وعصب التنمية، التي تجد أهمية قصوى لدى الدولة المصرية؛ الأمر الذي أثار انتباهنا على دراسة التشريعات والقوانين الحاكمة لحماية أمن المعلومات، لِتَمَاسِّ أمن المعلومات والدور الإعلامي والأمن القومي، وكفالة التشريعات والقوانين المختلفة، والحماية اللازمة لأمن المعلومات على المستويات كافة، يكفي أن نذكر تأثير الأمن المعلوماتي في الأمن الإعلامي والأمن القومي وسياسات الدولة الاقتصادية والاجتماعية، ونتساءل: كيف يُسْهِم الأمن المعلوماتي في حماية الأمن القومي؟

تَجْدُرُ الإشارة إلى أن الهدف الأساسي لأمن المعلومات هو حماية الموجودات المعلوماتية للدولة وللمؤسسات الحكومية والأفراد من الاختراقات التي تستهدف استخدامًا غير مشروع لمواردها، أو إحداث خلل في هيكلها أو محتواها، وهذا يفرض علينا دراسة العلاقة ما بين الأمن المعلوماتي والأمن القومي، ثم نعرض التشريعات والقوانين الحاكمة لحماية أمن المعلومات العربي، وأيضًا الغربي، كلما دعت الحاجه لذلك، وأخيرًا نستعرض ونقترح دور الدولة والأجهزة الرقابية في الحدِّ من ظاهرة الإخلال بحماية أمن المعلومات بما يتفق مع رؤية مصر 2020-2030م بشأن تحقيق التنمية المستدامة.

الكلمات الافتتاحية: الأ المعلوماتي – الأمن القومي -أمن المعلومات العربى – القوانين والتشريعات – الإخلال بحماية أمن المعلومات - التنمية المستدامة.

*مستشار بمجلس الدولة. دكتوراه في القانون – جامعة القاهرة

Laws and legislation governing information security protection: "Comparative study"

Abstract

The truth is not below doubt that the theme of information security is particularly important in our current time, which is safe by the Egyptian legislator in the 19th Constitution, through article 31, providing that: "Information space security is an essential part of The national economy and security system, and the State is committed to taking the necessary measures to preserve it, as governed by law" .

However, the events we know best witness that the media is part and a tool for the national security of national security. Which raised our attention to the study of legislation and governing laws to protect information security, to seek information security, information and national security, and to ensure different legislation and laws and laws for information security at all levels, enough to mention the impact of information security in media security and national security and economic and social security Waiting: How did information security contribute to the protection of national security?

It should be noted that the basic objective of information security is to protect state assets for State and government institutions and individuals aimed at an illegal use of their resources, or the creation of its structure or content. To protect the security of Arab information, and also Western, the sooner the need, and finally we review and suggest the role of state and control devices in reducing the phenomenon of prejudice to the protection of information security in accordance with Egypt's 2020-2030 vision on sustainable development.

Opening Words: Information Security - National Security - Security of Arab Information - Laws and Legislation - Due to Protecting Information Security - Sustainable Development.

مقدمة

الحقيقة أنه بدأ علم أمن المعلومات وتطوَّر مع بداية تِقْنِيَّة المعلومات وازدهارها، فعندما بدأت الحاسبات الآلية باحتواء معلومات مهمة بدأ القلق على أمن هذه المعلومات والأجهزة التي تعالجها؛ لذلك بدأ التفكير في تأمين المعلومات والأجهزة التي تحتويها ضد المخاطر المحتملة التي قد تتعرض لها.

لذلك أصبحت حماية المعلومات في عصر العولمة أمرًا بالغ الأهمية من أجل ضمان استمرارية الأعمال؛ حيث إن التصدِّيَ للتهديدات الأمنية لنُظُم المعلومات أصبح تحديًا يواجه العديد من المنظمات، فأمن المعلومات لا يعني تأمين المعلومة والحفاظ على سرية ونزاهة المعلومات وتوافرها فقط، ولكن أيضًا تأمين البِنْية التحتية التي تسهل استخدامها من أجهزة وبرمجيات وعوامل بشرية ومادية، واعترافًا بذلك بذلت الدول والمنظمات جهودًا كبيرة في إدارة ومعالجة أمن المعلومات، وأصبح من الضروري عليها أن تهتم بوضع نظم وإجراءات تعمل على الحدِّ من تلك المخاطر، ووضع نظام جيد لإدارتها والعمل على نجاح برنامجها الأمني[1].

ناهيك بأن أمن المعلوماتي المصري والعربي ضرورة ملحة يفرضها الواقع لقيام حكومات إلكترونية عربية، ولا شك أننا بحاجة لتأكيد حماية ما لدينا من معلومات ضد مخاطر القرصنة أو إرهاب المعلوماتي.

إشكالية البحث

الإشكالية الأساسية للبحث تتمثل في مدى تناول المشرّع للقوانين الحاكمة للأمن المعلوماتي وعلاقة التَّمَاسّ الواضحة بين هذا الأخير والأمن القومي، ومن جهة أخري تعارض بعض هذه القوانين مع حريات الأفراد التي كَفَلَها المشرِّع بقوانين وتشريعات من أجل الحفاظ على الخصوصية المعلوماتية.

الأهداف المرجوة من دراسة هذا الموضوع

تتمثل الأهداف المبتغاة من دراسة هذا الموضوع في الوقوف على التشريعات الحاكمة لمسألة الأمن المعلوماتي، ومدى تناول المشرِّع لها، مع ضمان عدم التعرض للأفراد في حقهم في الخصوصية.

يُضاف لذلك إيضاح دور الدولة والأجهزة الرقابية في كفالة وحماية أكثر فاعلية للأمن المعلوماتي؛ لِما لهذا الموضوع من الأهمية الكبيرة على الأقل للأمن القومي وبقاء الدولة وتقدُّمها في شتي المجالات: الاقتصادية، والأمنية، والسياسية، ... إلخ.

أهمية البحث

لا شكَّ أن تناول موضوع القوانين والتشريعات الحاكمة لحماية أمن المعلومات له كثيرٌ من الأهمية العلمية والعملية، وهذه الأخيرة في التعرُّض لموضوع الأمن المعلوماتي ومدى نجاح

التشريعات في حماية المعلومات بما يتوافق مع حق الأفراد في الخصوصية.

أما الأهمية العلمية لموضوع البحث؛ فتتمثَّل في تناول التشريعات الإلكترونية وتنظيم الاتصالات ودراسات الحاسب الآلي، وهي بالطبع مجالات مستحدثة، فضلًا عن تناول القانون الخاص للأمن المعلوماتي باستفاضة بخلاف القانون العام أو جهة الإدارة.

صعوبات البحث

تتمثل صعوبات البحث في قِلَّة، بل نُدْرَة الدراسات الفقهية المباشرة في موضوع الحماية التشريعية للأمن المعلوماتي وعلاقته بالأمن القومي مثلًا، وإحجام القضاء أيضًا عن تطبيق وتناول موضوع الأمن المعلوماتي، فضلًا عن تشعُّب موضوع الأمن المعلوماتي وتَمَاسِّه بالقانونَين الخاص والعام، والدولي العام، والقانون التجاري.

وأيضًا صعوبة وغموض بعض المصطلحات التي تناولت موضوع الأمن المعلوماتي، منها: الأمن السيبراني، والطيف الترددي، وغيرهما من الألفاظ التي يكتنفها بعض الغموض.

منهج البحث

يتمحور منهج البحث في تناول موضوع البحث بمنهج استقرائي عن طريق تناول القوانين والتشريعات وعرضها وتأصيلها والتعليق عليها.

ومن زاوية أخرى منهج مقارنة بالعرض والتعليق لنماذج قوانين تناولت موضوع البحث كالقانونَين الإنجليزي والفرنسي وغيرهما من التشريعات.

خطة البحث

من كل ذلك سوف نتناول موضوع البحث: «القوانين والتشريعات الحاكمة لحماية الأمن المعلوماتي» بإجمال غير مُخلٍّ وإطناب غير مُمِلٍّ، وذلك على النحو التالي:

مبحث تمهيدي: ماهية الأمن المعلوماتي.

المبحث الأول: علاقة الأمن المعلوماتي بالأمن القومي.

المبحث الثاني: القوانين والتشريعات الحاكمة لحماية أمن المعلومات.

المبحث الثالث: دور الدولة والأجهزة الرقابية في الحدِّ من ظاهرة الإخلال بحماية أمن المعلومات.

مبحث تمهيدي

ماهية الأمن المعلوماتي

بداية نشير إلى أن الأمن المعلوماتي يُعرَّف من الزاوية الأكاديمية بأنه: «العلم الذي يبحث في نظريات وإستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها».

أما من الزاوية التِّقْنِيَّة فيُعرَّف بأنه: «مجموعة الوسائل والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية».

وأخيرًا يُعرِّف جهاز تكنولوجيا المعلومات الحكومي البريطاني «الأمن السيبرياني» من الزاوية القانونية بأنه: «مجموعة من الإجراءات والتِّقْنِيَّات التي تستخدمها الدولة بهدف حماية أنظمتها الإلكترونية المختلفة من الهجمات الإلكترونية المختلفة أو من أي وصول غير مصرح به لأجهزة الدولة الحيوية».

وتَجْدُر الإشارة إلى أنه تتعين التفرقة بين المعلومات والبيانات؛ فالبيانات تُعَبِّر عن مجموعة من الأرقام والكلمات والرموز أو الحقائق أو الإحصاءات الخام التي لا علاقة بين بعضها بعضًا، أما المعلومات فهي المعنى الذي يُستخلص من هذه البيانات؛ فالبيانات «Data» هي المدخلات «Put In» إلى جهاز الكمبيوتر بهدف تشغيلها، ومعالجتها داخل الجهاز والحصول على المخرجات «Put Out» في صورة معلومات «Informations».[2]

ويمكننا القول إن الأمن السيبراني هو حماية الشبكات وأنظمة تقْنِيَّة المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحتويه من بيانات، من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع، ويشمل مفهوم الأمن السيبراني أمن المعلومات والأمن الإلكتروني والأمن الرقمي وما شابه ذلك[3].

بَيْدَ أن لجنة أنظمة الأمن القومي الأمريكية « Committee on National Security Systems» عرَّفت أمن المعلومات «Information Security (IS)» على أنه «حماية المعلومات وعناصرها المهمة بما في ذلك الأنظمة والأجهزة التي تستخدم هذه المعلومات وتخزِّنها وترسلها».

والحقيقة أننا نرى أن أمن المعلومات يشمل حماية المعلومات وأنظمة المعلومات ضد الوصول غير المصرح به أو الاستخدام أو الإفشاء أو التعديل أو التدمير؛ لضمان السرية والنزاهة والتوافر، بمعنى آخر؛ أمن المعلومات هو مستوى حماية المصالح الوطنية للبلد في مجال المعلومات على أساس متوازن للمصالح الحيوية للفرد والمجتمع والدولة ضد التهديدات الداخلية والخارجية.

ومن منظور آخر، فإن أمن المعلومات عبارة عن مجموعة من المؤشرات النوعية التي تضمن سلامة وإدارة وجوهر وإمكانيات وسمعة مختلفة لميزات الكائن واتجاهات التطوير،

وتشمل اهتمامات المجتمع في قطاع المعلومات ضمان مصالح الفرد في هذا المجال، وتعزيز الديمقراطية، وتكوين دولة قانونية، وتحقيق التكافل الاجتماعي.

لذلك يذهب رأي في الفقه إلى القول[4] بأنه تشمل اهتمامات الفرد في مجال المعلومات قضايا مثل: توافر المعلومات، واستخدام المعلومات لأغراض لا يحظرها القانون، من أجل التنمية الجسدية والمعنوية والفكرية، وكذلك لحماية المعلومات الشخصية والمعلومات التي تضمن الأمن الشخصي.

وعلى ضوء التعريفات السابقة يمكننا القول إن أمن المعلومات هو كل السياسات والإجراءات المُطَبَّقة بهدف حماية المعلومات عن طريق توفير الأمن لكل المكونات المادية من محالَّ وأجهزة، والمكونات التِّقْنِيَّة كالبرمجيات والشبكات والاتصالات، وكل التكنولوجيات المستعملة في تداول المعلومات، وتوعية العنصر البشري.

ناهيك بأن حماية الأمن المعلوماتي تهدف وبالضرورة إلى حماية مصالح الدولة في مجال المعلومات، التي تتكون من التنمية المستدامة والمتوازنة للبنية التحتية المعلوماتية للدولة، وخلق الظروف المواتية لإعمال الحقوق الدستورية للمواطنين من حيث المعلومات، وحماية موارد معلومات الدولة من الوصول غير القانوني، وضمان أمن المعلومات وأنظمة الاتصالات في الدولة.

المبحث الأول

علاقة الأمن المعلوماتي بالأمن القومي

الحقيقة التي لا يراودها أدنى شكٍّ أن الأمن المعلوماتي يرتبط أشد الارتباط بالأمن القومي؛ فالتحديث الدائم للنُّظم التشريعية والإجراءات الوقائية والعمل على مكافحة الجريمة وتطوير التنمية البشرية والسياسية لجميع أفراد المجتمع لغاية مُثْلَى، وهي دعم أطياف وألوان المجتمع كافة وانخراطهم في الحياة السياسية؛ يحافظ بلا شكٍّ على الدولة وشعبها وإقليمها، وهي غاية الأمن المعلوماتي والأمن القومي.

ونتيجة لذلك تركز جميع البلدان المتقدمة بشكل خاصٍّ على إنشاء وتطوير البنية التحتية والأنظمة المعلوماتية المختلفة لضمان مستوى عالٍ من الأمن القومي، ولارتباط أمن المعلومات ارتباطًا وثيقًا بالأمن القومي ومكوناته المختلفة[5].

ويذهب رأي في الفقه المقارن[6]، وهو في سبيلة لتوضيح العلاقة بين الأمن المعلوماتي والأمن السيبراني (القومي) إلى القول بأنه، يتم استخدام مفهوم الأمن السيبراني في الأدبيات العلمية ذات الصلة بالتوازي مع مفهوم «أمن المعلومات»، وذلك في بعض الحالات، ويتم استخدام هذه المصطلحات أيضًا بشكل مترادف[7].

ويضيف: ومع ذلك فإننا نعتقد أن «أمن المعلومات» هو مفهوم أوسع، وأن الأمن السيبراني جزء لا يتجزأ منه، ومن ثَمَّ فإن أمن المعلومات يغطي كلًا من بيئة المعلومات المادية والإلكترونية، ولكن يغطي الأمن السيبراني بيئة المعلومات الإلكترونية فقط.

ويضيف أخيرًا أنه يوجد اليوم قدر كافٍ من موارد المعلومات على الوسائط المادية التي تعمل بوصفها كائنًا للأمن، والتي تُشَكِّل فئات قانونية، مثل: أسرار الدولة، والأسرار التجارية، والملكية الفكرية، والمعلومات الشخصية.

وعلى الجانب الآخر يذهب رأي في الفقه[8] إلى القول بأن الأمن القومي مفهوم شامل، ليس مسألة حماية للحدود وحسب، ولا قضية إقامة ترسانة من السلاح، بل إنه يجمع كل هذه المتطلبات وغيرها، فهو قضية مجتمعية تشمل الكيان الاجتماعي بجميع جوانبه وعلاقاته؛ لتأمين كيان الدولة ضد الأخطار التي تهددها داخليًّا وخارجيًّا وتأمين مصالحها وتحقيق أهدافها وغايتها القومية.

ويذهب رأي آخر في الفقه[9] إلى القول بأنه تتكون مصالح الدولة في مجال المعلومات من التنمية المستدامة والمتوازنة للبنية التحتية المعلوماتية للبلد، وخلق الظروف المواتية لإعمال الحقوق الدستورية للمواطنين من حيث المعلومات، وحماية موارد معلومات الدولة من الوصول غير القانوني، وضمان أمن المعلومات وأنظمة الاتصالات في الدولة.

وعلى الجانب الآخر نجد القضاء قد غلَّب مصلحة الدولة والأمن القومي على حق الأفراد في التعبير؛ لذلك ذهبت المحكمة الإدارية العليا في أحد أحكامها[10] إلى القول بأن «الطيف الترددي الذي يمثل حَيِّزَ الموجات التي يمكن استخدامها في الاتصال اللاسلكي طبقًا لإصدارات الاتحاد الدولي، وضمان الاستخدام الأمثل لهذا الطيف مع مواكبة التقدم العلمي والفني والتكنولوجي ووضع قواعد وشروط منح التراخيص الخاصة باستخدام الطيف، وإصدار هذه التراخيص وتجديدها وإلغاءها ومراقبة تنفيذها، وذلك كله بما لا يُخِلُّ بالمصلحة العليا للدولة والأمن القومي للبلاد.

وحيث إنه ولئن كانت التشريعات المصرية -بما فيها قانون تنظيم الاتصالات سالف الذكر- لم تحدد الحالات التي تستدعي حجب المواقع الإلكترونية؛ فإن ذلك لا يُخِلُّ بحق الأجهزة الحكومية والجهاز القومي لتنظيم الاتصالات في حجب بعض المواقع على الشبكة الدولية للإنترنت حينما يكون هناك مِسَاسٌ بالأمن القومي أو المصالح العليا للدولة، وذلك بما لتلك الأجهزة من سلطة في مجال الضبط الإداري لحماية النظام العام بمفهومه المُثَلَّثِ: الأمن العام والصحة العامة والسكينة العامة للمواطنين، وذلك تحت رقابة القضاء.

وتتعين التفرقة في هذا الصدد بين التعدي على الحق الفردي للأشخاص والتعدي على المجتمع وأمنه وأمانه، وإن كان كلاهما مَمْقُوتًا مَمْجُوجًا تَلْفِظُه الشرائع ونصوص الدستور والقانون، وبَيْدَ أن المِسَاسَ بالحق الشخصي كفلَ دفعَه ولوجُ سبيل التقاضي جنائيًّا أو مدنيًّا أو كليهما معًا، حسبما ألمحت إليه المادة (76) من قانون تنظيم الاتصالات المشار إليه، أما حال المِسَاسِ بأمن المجتمع وأمانه؛ فلا يدرؤه إلا أن يُوصَدَ منبع هذا الخطر، موقعًا كان على شبكة الإنترنت، أو غيره».

لذلك نجد المشرّع المصري وهو بصدد وضع التعريفات العامة بقانون مكافحة جرائم تِقْنِيَّة المعلومات بالمادة الأولي منه[11] يعرّف الأمن القومي على أنه: «كل ما يتصل باستقلال

واستقرار وأمن الوطن ووحدة وسلامة أراضيه، وما يتعلق بشئون رئاسة الجمهورية ومجلس الدفاع الوطني ومجلس الأمن القومي، ووزارتي الدفاع والإنتاج الحربى، ووزارة الداخلية، والمخابرات العامة، وهيئة الرقابة الإدارية، والأجهزة التابعة لتلك الجهات».

وعرَّف أيضًا جهات الأمن القومي على أنها تشمل: «رئاسة الجمهورية، ووزارة الدفاع، ووزارة الداخلية، والمخابرات العامة، وهيئة الرقابة الإدارية».

وفي تطبيق لهذا القانون ذهبت المحكمة الإدارية العليا[12] إلى القول بأنه: «ومن حيث إن المشرّع المصري -بالقانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقْنِيَّة المعلومات- وضع مصر على خريطة العالم الرقمي، وجاءت نصوصه كاشفة عن أنه قانون عقابي للمجرم المعلوماتي، وليس رقابيًّا؛ فهو احترازي لا اختراقي، يمنح المواطنين الحرية في الفضاء الإلكتروني أيًّا كانت وسائله سواء: «الفيسبوك، أو تويتر، أو إنستجرام، أو غيرها» ما دامت تلك الحرية تُمَارَسُ في إطار القانون دون المِسَاسِ بالأمن القومي للبلاد أو بسمعة المواطنين، أو خرق حياتهم الخاصة بما يسيء إليهم، وحفاظًا على سمعة المواطنين؛ فإن المشرّع انتهج في هذا القانون تجريم هذه الأفعال التي تقع بهذه الوسائل، وقرر لها عقابًا صارمًا لآثارها المدمرة على الوطن في مِسَاسِها بالأمن القومي له والنظام العام والآداب به، وعلى المواطن بمِسَاسِها بشرفه وعرضه، واعتباره بين أهله وذويه؛ فنَصَّ في المادة 25 من القانون على تحديد الجرائم المتعلقة بالاعتداء على حرمة الحياة الخاصة والمحتوى المعلوماتي غير المشروع، وأَبَانَ عن أنها كل اعتداء على أيٍّ من المبادئ أو القيم الأسرية في المجتمع المصري، أو انتهك حرمة الحياه الخاصة، أو أرسل بكثافة العديد من الرسائل الإلكترونية لشخص معين دون موافقته، أو منح بيانات شخصية إلى نظام أو موقع إلكتروني لترويج السلع أو الخدمات دون موافقته، أو نشر عن طريق الشبكة المعلوماتية أو بإحدى وسائل تِقْنِيَّة المعلومات معلوماتٍ أو أخبارًا أو صورًا وما في حكمها، تنتهك خصوصية أي شخص دون رضاه، سواء كانت المعلومات المنشورة صحيحة أو غير صحيحة».

المبحث الثاني

القوانين والتشريعات الحاكمة لحماية أمن المعلومات

يغلب تشريعات الدول الأجنبية الأمن المعلوماتي في حالة تهديد الأمن العام ثَمة اعتبار آخر؛ فهناك عدد كبير من التشريعات[13] صدرت بهدف وضع معايير لأمن المعلومات التي تتيح تبادل البيانات والتشفير، ومنها النموذجان الأمريكي والفرنسي، اللذان تناولتهما الدراسات الفقهية بالبحث[14].

ففي الولايات المتحدة الأمريكية[15] تم سَنُّ قانون حماية المعلومات السرية والكفاءة الإحصائية لإنشاء حماية السرية للمعلومات التي تم جمعها للأغراض الإحصائية من قِبل الوكالات الإحصائية الأمريكية، مثل: المركز الوطني لإحصاءات التعليم لعام 2019، وقانون حماية المعلومات السرية، وقانون الكفاءة الإحصائية، الذي تم سَنُّه بوصفه جزءًا من قانون الحكومة الإلكترونية لعام 2002، قانون حماية المعلومات السرية والكفاءة الإحصائية

هو إجراء قصير نسبيًّا، وينصُّ على أن جميع معلومات تحديد الهوية الشخصية المقدمة من قِبل الأفراد «سواء بشكل مباشر أو من منظمة أخرى» إلى وكالة اتحادية لأغراض إحصائية يجب أن تظل سرية، ولا تُستخدم إلا للأغراض الإحصائية، ما لم يوافق الفرد الأساسي بشكل محدد على الإفصاح. وينتهج قانون حماية المعلومات السرية والكفاءة الإحصائية عقوبات صارمة، يمكن أن يُسجن أيُّ موظف في الوكالة يُفصِحُ عمدًا عن أي معلومات تحديد الهوية الشخصية بطريقة لا يسمح بها قانون حماية المعلومات السرية والكفاءة الإحصائية لمدة تصل إلى خمس سنوات، وتُحكم عليه بالغرامة حتى 250 ألف دولار.

أما على الصعيد العربي[16]؛ فنجد دولة سلطنة عمان[17]، ودولة الإمارات العربية المتحدة[18] هما من النماذج الرائدة في صياغة هذه المسألة لحماية أمنهما المعلوماتي وخلق بيئة معلوماتية للاستثمار الآمن.

أما المشرّع القطري فقد أصدر القانون رقم 13 لسنة 2016م[19] الخاص بحماية خصوصية البيانات الشخصية، الذي جاء بالمادة (18) منه على أن: «للجهة المختصة أن تقرر معالجة بعض البيانات الشخصية دون التقيد بأحكام المواد: «4، و9، و15، و17» من مواد هذا القانون، وذلك لتحقيق أيٍّ من الأغراض الآتية:

1- حماية الأمن الوطني والأمن العام.

2- حماية العلاقات الدولية للدولة.

3- حماية المصالح الاقتصادية أو المالية للدولة.

4- منع أي جريمة جنائية، أو جمع معلومات عنها، أو التحقيق فيها، وتحتفظ الجهة المختصة بسجل خاص تُقَيَّدُ به البيانات التي تحقِّق الأغراضَ المشار إليها، ويَصْدُرُ بتحديد شروط وضوابط وأحوال القيد في هذا السجل قرارٌ من الوزير».

وهو ما آمن به المشرّع المصري –كما قلنا- في دستور عام 2014م[20]، وذلك من خلال المادة (31) منه التي نصَّت على أنه: «أمن الفضاء المعلوماتي جزء أساسي من منظومة الاقتصاد والأمن القومي، وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه، على النحو الذي ينظمه القانون».

كما تنص المادة 57 منه على أن للحياة الخاصة حُرْمَةً، وهي مصونة لا تُمَسُّ، وللمراسلات البريدية والبرقية والإلكترونية والمحادثات الهاتفية، وغيرها من وسائل الاتصال، حُرْمَةً وسريتها مكفولة، ولا تجوز مصادرتها، أو الاطلاع عليها، أو رقابتها إلا بأمر قضائي، ولمدة محددة، وفى الأحوال التي يبينها القانون. كما تلتزم الدولة بحماية حق المواطنين في استخدام وسائل الاتصال العامة بكل أشكالها، ولا يجوز تعطيلها أو وقفها أو حرمان المواطنين منها بشكل تعسفي.

هذا إلى جانب العديد من القرارات التنظيمية التي أصدرتها الوزارة المعنية[21] بتكنولوجيا المعلومات والاتصالات بهدف حماية تِقْنِيَّة المعلومات والاتصالات، وما زال هناك العديد من

الدراسات القانونية والجهود التشريعية التي تُبذلُ من أجل تأمين المعاملات الإلكترونية المختلفة من جميع جوانبها القانونية والجنائية.

وقد أنشأت مصر بموجب قرار مجلس الوزراء رقم 2259 لسنة 2014م مجلسًا أعلى للأمن السيبراني[22]؛ لتكون مهمته وضع إستراتيجية وطنية لمواجهة الأخطار والهجمات السيبرانية والإشراف على تنفيذها وتحديثها تماشيًا مع التطورات التِّقْنِيَّة.

ثم صدر القانون رقم 2018/175 [23] الصادر بشأن مكافحة جرائم تقْنِيَّة المعلومات ولائحته التنفيذية رقم 1699 لسنة 2020م.

ونصَّت المادة (34) من هذا القانون على أن: «إذا وقعت أي جريمة من الجرائم المنصوص عليها في هذا القانون بغرض الإخلال بالنظام العام، أو تعريض سلامة المجتمع وأمنه للخطر، أو الإضرار بالأمن القومي للبلاد أو بمركزها الاقتصادي، أو منع أو عرقلة ممارسة السلطات العامة لأعمالها، أو تعطيل أحكام الدستور أو القوانين أو اللوائح، أو الإضرار بالوحدة الوطنية والسلام الاجتماعي، تكون العقوبة السجن المشدد»[24].

وصدر قرار وزير الجهاز المركزي للتنظيم والإدارة رقم 87 لسنة 2019م[25] بشأن التقسيم التنظيمي لنُظم المعلومات والتحول الرقمي.

ونَصَّ في مادته الخامسة على أن: «يختص التقسيم التنظيمي الفرعي «للبنيه الأساسية وتأمين المعلومات» بالآتي: 1- ...2- ....3- ....4- .... 5- توفير التأمين السيبراني لنُظم معلومات الوحدة ضد المخاطر المحتملة سواء بشرية أو طبيعية ووضع الضوابط اللازمة لذلك».

وكان آخر هذه التطورات التشريعية وأهمها القانون رقم 151 لسنة 2020م[26] بشأن حماية البيانات الشخصية المعالجة إلكترونيًّا جزئيًّا أو كليًّا لدى أي حائز أو متحكم أو معالج لها، وذلك بالنسبة للأشخاص الطبيعيين.

ثم أصدر رئيس الجمهورية قرارًا بقانون 150 لسنة 2021م[27] بتعديل بعض أحكام قانون العقوبات الذي نَصَّ في مادته الأولى على أن «يُستبدل بنصِّ المادة 80 (أ) من قانون العقوبات، النصُّ الآتي: مادة 80 (أ):

مع عدم الإخلال بأي عقوبة أشد يَنُصُّ عليها أي قانون آخر، يُعاقب بالحبس مدة لا تقل عن ستة أشهر ولا تزيد على خمس سنوات وبغرامة لا تقل عن خمسة آلاف جنيه ولا تجاوز خمسين ألف جنيه:

1 - كلُّ مَن حصل بأي وسيلة غير مشروعة على سرٍّ من أسرار الدفاع عن البلاد، ولم يقصد تسليمه أو إفشاءه لدولة أجنبية، أو لأحد ممن يعملون لمصلحتها.

2 - كلُّ مَن أذاع بأي طريقة سرًّا من أسرار الدفاع عن البلاد.

3 - كلُّ مَن نظم أو استعمل أي وسيلة من وسائل التراسل بقصد الحصول على سرٍّ من أسرار الدفاع عن البلاد أو تسليمه أو إذاعته.

4 - كلُّ مَن قام بجمع الاستبيانات أو الإحصاءات أو إجراء الدراسات لأي معلومات أو بيانات تتعلق بالقوات المسلحة أو مهامها أو أفرادها الحاليين أو السابقين بسبب وظيفتهم دون تصريح كتابي من وزارة الدفاع.

فإذا وقعت الجريمة في زمن الحرب، أو باستعمال وسيلة من وسائل الخداع أو الغش أو التخفي أو إخفاء الشخصية أو الجنسية أو المهنة أو الصفة، أو بإحدى وسائل تقْنِيَّة المعلومات، أو كان الجاني من ضباط القوات المسلحة أو أحد أفرادها أو من العاملين المدنيين لديها كانت العقوبة السجن.

ويُعاقب بالعقوبات نفسها على الشروع في ارتكاب هذه الجرائم».

ثم صدر قرار رئيس جمهورية مصر العربية رقم 232 لسنة 2021م[28] بإنشاء مجمع الإصدارات المؤمنة والذكية، الذي نَصَّ في مادته الأولي على بعض التعريفات منها تعريف النظام «البيومتري» بأنه: نظام معلوماتي يَكْفُلُ تَمْيِيز كل فرد عن الآخر عن طريق الخصائص الحيوية التي يتم التزام الجهات كافة بتطبيقها، على أن يتم توحيد وسائل وتقنيات إدخالها لبيانات على مستوى الدولة ومؤسساتها المختلفة.

البيانات «البيومترية»: البيانات التي تحدد هوية الفرد بما يَكْفُلُ تَمْيِيزه عن الآخرين ويضمن عدم تكرارها.

أما على الجانب العربي وبتاريخ 2014/9/19؛ فقد أصدر السيد رئيس الجمهورية القرار رقم 277 لسنة 2014م، بشأن الموافقة على انضمام مصر إلى الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية الموقعة في القاهرة بتاريخ 2010/12/21م.

ثم أصدر وزير الخارجية المصري قرارًا[29] بالموافقة على الاتفاقية العربية لمكافحة جرائم المعلومات وتهدف هذه الاتفاقية إلى تعزيز التعاون بين الدول العربية في مجال مكافحة جرائم تِقْنِيَّة المعلومات لدرء أخطار هذه الجرائم؛ حفاظًا على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها.

القوانين والتشريعات الحاكمة لحماية أمن المعلومات في إنجلترا

من المعروف أن أمن المعلومات يهتم بضمان أن المستخدمين المصرَّح لهم لديهم دائمًا إمكانية الوصول إلى المعلومات عندما يحتاجون إليها، والسلامة «حماية دقتها واكتمالها»، والسرية «ضمان أن المعلومات الحساسة لا يمكن الوصول إليها إلا للأشخاص المصرَّح لهم باستخدامها ذلك»، ويتناول أيضًا الأساليب المناسبة للتخلص من المعلومات التي لم تعد مطلوبة.

جدير بالذكر أن الأمن ضروري لنجاح كل نشاط أكاديمي وإداري تقريبًا، ويتم تحقيق الأمن الفعَّال من خلال العمل ضمن إطار عمل مناسب، بما يتوافق مع التشريعات وسياسات المملكة المتحدة، ومن خلال الالتزام بالإجراءات المعتمدة[30].

أهداف السياسة الخاصة بأمن المعلومات في المملكة المتحدة

من أهم الأهداف التي ترمي إليها السياسة الخاصة بأمن المعلومات بالمملكة هي التأكد من أن جميع مرافق وبرامج وبيانات وشبكات ومُعِدَّات الحوسبة في المملكة المتحدة محمية بشكل كافٍ ضد الإهدار أو سوء الاستخدام، والتأكد من أن جميع المستخدمين على دراية ببيان السياسة هذا وجميع السياسات المرتبطة بها والامتثال الكامل لها، وأنهم على دراية بالإجراءات وقواعد الممارسة ذات الصلة ويعملون وَفْقًا لها، وضمان حفظ السجلات الورقية بشكل آمن وإدارتها بشكل فعَّال؛ والتأكد من أن جميع المستخدمين على دراية بالتشريعات البريطانية ذات الصلة والامتثال الكامل لها، وخلق وَعْيٍ في جميع أنحاء المملكة المتحدة بضرورة تنفيذ التدابير الأمنية المناسبة بوصفها جزءًا من التشغيل الفعَّال ودعم أنظمة إدارة المعلومات، والتأكد من أن جميع المستخدمين يفهمون مسئولياتهم الخاصة لحماية سرية وسلامة البيانات التي يتعاملون معها، والتأكد من التخلص من المعلومات بطريقة آمنة بشكل مناسب عندما لا تصبح ذات صلة أو مطلوبة[31].

جدير بالذكر في هذا الصدد أن المملكة المتحدة أصدرت عدة تشريعات تحكم الأمن المعلوماتي[32] منها على سبيل المثال: قانون إساءة استخدام الكمبيوتر لعام 1990، وقانون حماية البيانات لعام 2018، وقانون حقوق الإنسان لعام 1998، وقانون تنظيم سلطات التحقيق لعام 2000، وقانون الإرهاب لعام 2006، وقانون مكافحة الإرهاب والأمن لعام 2015.

يُذكر أن هناك إجراءات متبعة عند التعرض لخرق الأمن المعلوماتي منها أنه يتعين على أي شخص يشكُّ في أن أمان نظام الكمبيوتر قد تم اختراقه أو من المحتمل أن يتم انتهاكه، يجب عليه إبلاغ مجموعة أمان المعلومات في المملكة المتحدة من الفور، حيث قد يكون هناك انتهاك لقانون حماية البيانات لعام 2018؛ ما قد يؤدي إلى إجراءات مدنية أو جنائية، لذلك، من الضروري أن يمتثل مستخدمو أنظمة المعلومات في المملكة المتحدة، ليس فقط لهذه السياسة، ولكن أيضًا لسياسة حماية البيانات في المملكة المتحدة وقواعد الممارسة المرتبطة بها.

ناهيك بأنه يتعين على الشخص الذي يتعرض لانتهاك للأمن المعلوماتي أن يُسارِع بالإبلاغ عن جميع الانتهاكات الأمنية المادية لمكاتب الأمن في المملكة المتحدة[33].

المبحث الثالث

دور الدولة والأجهزة الرقابية في الحد من ظاهرة الإخلال بحماية أمن المعلومات

المعروف أن أمن المعلومات[34] هو محل دراسات وتدابير حماية سرية وسلامة محتوى توافر المعلومات ومكافحة أنشطة الاعتداء عليها أو استغلال نُظُمِها في ارتكاب الجريمة،

وهو هدف وغرض تشريعات حماية المعلومات من الأنشطة غير المشروعة وغير القانونية التي تستهدف المعلومات ونُظُمَها.

أما المعلومة فما هي سوى حقائق وأفكار يتبادلها الناس في حياتهم العادية عبر وسائل الاتصال المختلفة، من خلال مراكز ونُظُم المعلومات المختلفة في المجتمع والإنسان؛ فالمعلومة هي -إذن- تعبير يستهدف جعل رسالة قابلة للتوصيل إلى الغير، وتتطلب المعلومة بطبيعتها وجود وَسَطٍ تُخَزَّنُ فيه، وبهذا يتسع مفهوم الأمن المعلوماتي؛ ليشمل المحاور التالية:

- حماية المعلومات من الضرر بالأشكال كافة، سواء أكان مصدره أشخاصًا كالمحترفين، أم برامج كالفيروسات، وسواء أكان متعمَّدًا أم عن طريق الخطأ.

- حماية المعلومات من: الوصول غير المصرَّح به، أو السرقة، أو الالتقاط، أو التغيير، أو إعادة التوجيه، أو سوء الاستخدام.

- حماية قدرة المنشأة على الاستمرار وأداء أعمالها على أكمل وجه.

- تمكين أنظمة تِقْنِيَّة المعلومات والبرامج التطبيقية لدى المنشأة من العمل بشكل آمن.

ولتوفير الحماية المطلوبة للمعلومة في المحاور السابقة وجب ضمان توافر العناصر التالية لأي معلومات يُراد توفير الحماية الكافية لها:

- «Confidentiality»: السرية أو الموثوقية، وتعني التأكد من أن المعلومات لا تُكشف، ولا يُطَّلَع عليها من قبل الأشخاص غير المُخَوَّلين وغير المصرَّح لهم بذلك.

- «Integrity»: التكاملية وسلامة المحتوى: التأكد من أن محتوى المعلومات صحيح، ولم يتم تعديله أو العبث به، وبشكل خاصٍ لن يتم تدمير المحتوى أو تغيره أو العبث به في أي مرحلة من مراحل المعالجة أو التبادل، سواء في مرحلة التعامل الداخلي مع المعلومات أو عن طريق تدخل غير مشروع؛ فالهدف هو الحفاظ على المعلومة واتخاذ التدابير اللازمة لحمايتها من التغيير.

لكل ذلك سوف نقترح مجموعة من الوسائل لحماية الأمن المعلوماتي والأمن القومي، وذلك من خلال الآتي[35]:

بما إن مخاطر أمن المعلومات باتت ترقى إلى مستوى تهديد الأمن القومي عامةً؛ فإن وسائل المواجهة والحماية لا بُدَّ أن تُظَلِّلَها منظومة أمن قومي، لأنه من الخطأ أن تكون الأخطار والتهديدات شاملة وربما مُنَسَّقة، ومُخَطَّط لها أحيانًا، ثم تأتي سبل ووسائل مواجهتها جزئية وعفوية وخالية من التخطيط، وتفتقر إلى التنسيق والرُّشد، وفي هذا الشأن تتعدد وتتنوع الوسائل التي تستخدمها الحكومات لحماية المعلوماتية بهدف حماية أمنها القومي، منها وسائل تقْنِيَّة وأخرى قانونية وأمنية.

ويتعين علينًا بداية الإقرار بحقيقة مهمة مُؤَدَّاها أن العنصر البشري هو الأساس في الحماية؛ إذ يكون على عاتقه التحرّي والمتابعة وضمان سرية المعلومات التي يعملون عليها، حيث يمكن تأمينهم باستخدام مجموعة من الوسائل المتعلقة بتعريف شخص المستخدم كالبطاقات الذكية المستخدمة للتعريف وكلمات السر، أو التعريفات البيولوجية التي تعتمد على سِمات معينة في الشخص، مثل تسجيل بصمة الأصابع أو العين أو الصوت، وغيرها من الخصائص الفيزيائية التي تعمل بوصفها حارسًا لنظام معين، وتسمح بمرورك أو عدم مرورك من بوابة معينة بناءً على خصائصك الفيزيائية مع المعلومات المخزَّنة في قاعدة البيانات.

أولًا: وسائل الحماية التِّقْنِيَّة

تحاول الوسائل التِّقْنِيَّة والتكنولوجية الموازنة والتقليل ما بين خطر القرصنة والخسائر المترتبة على هذه الاختراقات، وبين المعلومات المُراد حمايتها وأهميتها وتكلفة هذه الحماية، ومن الوسائل الفنية لهذه الحماية نذكر تشفير المعلومات واستخدام برامج ضد القرصنة.

1- تشفير المعلومات المنقولة والمحفوظة

حيث تظهر المعلومات بصورة مبهمة تمامًا لكل من يحاول التنصت عليها أو اختراقها سواء بوسائل الاتصال السلكية أو اللاسلكية، بحيث يهدف إلى منع الغير من التقاط الرسائل أو المعلومات. ويُعد التشفير من وسائل حفظ سرية المعلومات في نطاق الأجهزة الإلكترونية؛ إذ تمتلك كل جهة أو فرد مفتاحين لتشفير البيانات، المفتاح الأول هو المفتاح الخاص، ويكون فقط بحوزة الجهة المُخَوَّلة والمفتاح العام يتم نشره عبر شبكة الإنترنت من أجل استخدامه من قِبل الجهات الأخرى لتشفير الملفات والمعلومات المُراد إيصالها إلى الطرف الآخر.

ويذهب رأي في الفقه[36] إلى القول بأن آخر ما استُحدث في مجال التشفير هو تقْنِيَّة التشفير الكَمِّيّ «Quantum Cryptography»، وهي تقْنِيَّة تستخدم مبدأً من مبادئ علم الفيزياء الكَمِّيَّة، في عملية نقل البيانات من موقع إلى آخر بأسلوب آمن 100%، ومثل ذلك يجعل من المستحيل على أي مُتَنَصِّتٍ معرفة محتويات الرسالة المرسلة، إلا بتَغَيُّر المحتوى، وهذا جرس إنذار فوري.

2- البرامج المتخصصة ضد القرصنة

ويُوجد الكثير من البرامج المستخدمة لمنع القرصنة التي تعمل على الإيقاع بالقراصنة واكتشافهم كحصان طروادة، حيث يتم عمل مسح كامل لجميع الملفات الموجودة بجهاز المستخدم ومطابقتها مع الموجودة بقاعدة البيانات الأساسية، بالإضافة إلى برنامج ارتباطات الأمن المعلوماتي بالأمن القومي «طبق العسل»، الذي يهدف لخداع القراصنة عن طريق توجيه المخترق أو القرصان إلى نظام معلومات ليس ذي أهمية ومتصل بأجهزة الأمن والتنبيه.

ثانيًا: وسائل الحماية القانونية

وتتمثل هذه الوسائل في تطوير القواعد القانونية المحلية والمنظومة التشريعية الوطنية للتعزيز من الأمن المعلوماتي في مواجهة الجرائم المعلوماتية، إضافة إلى تطوير الاتفاقيات الأمنية الدولية؛ إذ لا تُوجد دولة في العالم لا تملك اتفاقات أمنية ثنائية أو جماعية مع دول خارجية، حيث من المفيد تطوير الاتفاقات الأمنية؛ لكي تشمل قضايا الأمن المعلوماتي بالإضافة إلى تبادل الخبرات الأمنية الإلكترونية والمعلوماتية.

إن الطابع المفتوح للإنترنت هو مصدر قوته، لكنه أيضًا موضع ضعفه الذي يعرضه لخطر المجرمين ومرتكبي الهجمات الإلكترونية، فلكي يؤدي الإنترنت دوره؛ يجب أن يحافظ على طابعه المفتوح وقابليته التشغيلية «Interoperability» مع التجهيزات والأنظمة الأخرى، إلا أن هذا الانفتاح يساعد مخترقي الشبكات على القيام بأعمالهم الإجرامية بشكل أسهل على الإنترنت، وقد أصبحت تطال اليوم أيضًا مَنَصَّات الهواتف النقالة[37].

والحقيقة أن سَنَّ القوانين والقرارات ذات النزعة الصارمة يفيد بشكل كبير في حماية الأمن المعلوماتي حتى لا يعتقد منتهكو الأمن المعلومات أنهم بمنأًى عن العقاب، ومن ثَمَّ الإفلات من المسئولية القانونية بالتخفي والهروب بارتكاب جرائمهم المُخِلّة بالأمن المعلوماتي عبر شبكات الإنترنت مثلًا؛ لذلك نقترح وندعم تدخل المشرع في أقرب تعديل تشريعي مُرْتَقَب بالنَّصِّ على تحول دخول الأفراد بتسجيلهم للبيانات الحقيقية والوافية للدخول على الشبكة لمراقبتها عند وقوع الواقعة، وهو ما نأمل من مشرّعنا النظر إليه قريبًا[38].

وهو ما نادى به رأي في الفقه حتى على المستوى الدولي يذهب[39] إلى القول بأن مسألة الأمن المعلوماتي أصبحت مسألة قانونية أكثر منها مسألة تقْنِيَّة؛ لتعلُّقها بمجالات الخصوصية «Privacy» وأمن المعلومات «security Data»، لذلك لا بُدَّ أن تُعِدَّ المنظمات حزمة القوانين المنظمة لأمن المعلوماتي، وأن يكون للقانونيين دور في تصميم الإجراءات والتدريب وتقديرات المخاطر.

بل يذهب رأي آخر في الفقه[40] إلى اقتراح التعاون بين القطاعين العام والخاص في حماية الأمن المعلوماتي.

ثالثًا: وسائل الحماية التوعوية

لكي يتم اعتماد سياسات الأمن المعلوماتي بتجنب أخطار القراصنة والمحترفين الأشرار في برنامج استهدافهم المستمرة للمعلومات الإستراتيجية في الدولة؛ فإنه تجب توعية الجمهور والمواطنين داخل إقليم الدولة، إذ من المهم، بل الضروري أن تقوم الدولة بحملة توعية عامة حول أمن البلاد من جانب الأمن المعلوماتي بداية من رأس الدولة وصولًا إلى موظفيها وجمهور المواطنين؛ حيث تشرح لهم المخاطر الأمنية وكيفية تفاديها، وما الإجراءات التي قامت وتقوم بها الدولة في هذا المجال، بالإضافة إلى إمكانية عقد ندوات تدريبية وتثقيفية وإصدار نشرات إعلامية وتوعوية بهذا الخصوص.

وفي الحقيقة تلعب وسائل الإعلام دورًا مهمًّا في تقديم المعلومات الحقيقية، ومن ثَمَّ يجب التحقق دائمًا –بشكل صارم– والتدقيق على المعلومات، كما ينبغي على محترفي وسائط الأخبار تعزيز الأخلاق المهنية، مع صرامة في صحة وموضوعية الأخبار ومصادرها، والإصرار على تقديم الحقائق في أي وقت؛ لضمان فَهْمٍ صحيح للحقائق، وتقوية شفافية الكشف عن المعلومات، كالذي حدث في معالجة جائحة «كوفيد 19»، حيث انتقل الإعلام إلى منهجية الوصول إلى الناس بدلًا من وصول الناس إلى الإعلام؛ فنشطت الرسائل الإعلامية، والمعلومات التي لم يقتصر نشرها على المواقع فحسب، بل كانت تُرسل إلى فئات المجتمع كافة، وبلغات مختلفة.

ناهيك بأن كتاب «المنطقة المعتمة التاريخ السري للحرب السيبرانية»[41] للكاتب «فرد كابلان» هي حرب لا تُسمع فيها أصوات الرصاص، لكنها حرب كثيرة الخسائر، واسعة المدى، تطال غالبية السكان؛ فتتعطل فيها مصالحهم، وتُسلب فيها أموالهم من البنوك، وتتعطل فيها حركة الملاحة الجوية، وتفقد فيها الاتصالات والإنترنت، وربما تُطلق فيها الصواريخ على غير أهدافها، إنها الحرب السيبرانية التي يستطيع فيها قراصنة الحاسوب خلف الشاشات القيام بكل هذا التخريب من خلال لوحات مفاتيح الكمبيوتر، هي خطر يهدد البشرية؛ إذ إن الحرب السيبرانية أوسع نطاقًا وأشد خطورة على حياة الانسان.

لذلك يذهب رأي في الفقه[42] إلى القول بأنه يتمثل أحد الأهداف الرئيسية لحرب المعلومات بالتوازي مع العمليات العسكرية في نشر معلومات مضلِّلة استفزازية، وتثبيط وإحباط ومضايقة الجيش الآخر أو الشعب بأكمله، ويوفر التطور السريع لتكنولوجيا المعلومات والاتصالات فرصًا كبيرة لمثل هذه التأثيرات النفسية.

وفي هذا الصدد، تتمثل إحدى المهام الرئيسية لأمن المعلومات في الاستعداد لحرب المعلومات واتخاذ التدابير ذات الصلة لمنعها في حالة حدوث تهديدات حقيقية.

ومن وجهة نظرنا، أخيرًا؛ أن إستراتيجيات الأمن الوطني وتأثير الأمن المعلوماتي في حياة الأفراد له من الأهمية الكبرى في بثِّ روح الهَوان والإحباط لجميع الأفراد عن طريق طرح مجرد معلومة مهمة بغرض توجيه المجتمع لفعل شيء ضارٍّ بمصالحهم، وهو ما نعيشه حاليًّا، وما نسمعه من أن الحرب الجارية بين دولتي روسيا وأوكرانيا تُنْبِئُ بحرب عالمية ثالثة؛ ما بَثَّ روح الضعف في نفوس أفراد المجتمع.

لذلك نناشد ونلتمس من الدولة المصرية التأكيد من خلال الضوابط السالف عرضها على بعض الحقائق التي تخدم الاقتصاد والسياسة والأمن القومي المصري، وهو ما نأمل تحقيقه.

الخاتمة

وفي خِتام هذه الدراسة، لنا مجموعة من النتائج لِمَا تم بحثه، ثم نُلْحِقُها بعدد من التوصيات راجين من المُشرّع المصري وقضائنا المُوَقَّر الأخذ بها لتقوية ودَعْمِ وحماية الأمن المعلوماتي، وذلك على النحو الآتي:

أولًا: النتائج

1- توصل الباحث إلى أن أمن المعلومات هو كل السياسات والإجراءات المُطَبَّقة بهدف حماية المعلومات عن طريق توفير الأمن لكل المكونات المادية من محالَّ وأجهزةٍ، والمكونات التِّقْنِيَّة كالبرمجيات والشبكات والاتصالات، وكل التكنولوجيات المستعملة في تداول المعلومات، وتوعية العنصر البشري.

2- حاول هذا البحث التأكيد على الأهمية البالغة لأمن المعلومات وإيضاح مدى ارتباطه بالأمن القومي بحماية النظام الدستوري والاستقرار الاجتماعي والسياسي والاقتصادي، واستقرار الدولة وسلامتها من التهديدات والأخطار والعدوان العسكري، بشكل فعَّال، وموارد المعلومات والفرص التكنولوجية؛ لتعزيز قدراتها العسكرية وتقوية أنظمتها الدفاعية.

3- تَبَيَّنَ للباحث أن أمن المعلومات في إنجلترا يهتم بضمان أن المستخدمين المصرَّح لهم لديهم دائمًا إمكانية الوصول إلى المعلومات عندما يحتاجون إليها، والسلامة «حماية دقتها واكتمالها»، والسرية «ضمان أن المعلومات الحساسة لا يمكن الوصول إليها إلا للأشخاص المصرَّح لهم باستخدامها ذلك»، ويتناول أيضًا الأساليب المناسبة للتخلص من المعلومات التي لم تَعُدْ مطلوبة.

4- تَجلَّى للباحث أن مسألة الأمن المعلوماتي أصبحت مسألة قانونية أكثر منها مسألةِ تِقْنِيَّة؛ لتعلُّقها بمجالات الخصوصية «Privacy» وأمن المعلومات «security Data»، لذلك لا بُدَّ أن تُعِدَّ المنظمات حزمة القوانين المنظمة للأمن المعلوماتي، وأن يكون للقانونيّين دور في تصميم الإجراءات، والتدريب، وتقديرات المخاطر.

5- اتضح للباحث أن وسائل الإعلام تلعب دورًا مهمًّا في تقديم المعلومات الحقيقية، ومن ثَمَّ يجب التحقق دائمًا –بشكل صارم– والتدقيق على المعلومات، كما ينبغي على محترفي وسائط الأخبار تعزيز الأخلاق المهنية، مع صرامة في صحة وموضوعية الأخبار ومصادرها، والإصرار على تقديم الحقائق في أي وقت؛ لضمان فَهْمٍ صحيح للحقائق، وتقوية شفافية الكشف عن المعلومات، كالذي حدث في معالجة جائحة «كوفيد 19»، حيث انتقل الإعلام إلى منهجية الوصول إلى الناس بدلًا من وصول الناس إلى الإعلام؛ فنشطت الرسائل الإعلامية، والمعلومات التي لم يقتصر نشرها على المواقع فحسب، بل كانت تُرسل إلى فئات المجتمع كافة، وبلغات مختلفة.

ثانيًا: وقد انتهينا من خلال بحثنا إلى مجموعة من التوصيات ننادي بها في هذا المقام منها:

- نقترح الاستعانة في سَدِّ الفراغ التشريعي الناتج عن تطور وظهور الجرائم المستحدثة وعابرة الحدود، بالتجارب التشريعية المقارنة لبعض الدول في الضبط التشريعي، وتأهيل رجال الضبط الإداري لمواجهة التهديدات «الأمن المعلوماتي»، كإنجلترا والولايات المتحدة الأمريكية.

- إدراج مادة ضمن المواد العلمية لكل من كليات القانون والشرطة والكليات العسكرية؛ لضمان فَهْمٍ سليم لأمن المعلومات وخطورة تعرضه للانتهاك، وارتباطه بالأمن القومي وسياسات الدولة، والإشراف على صياغة الكوادر المعلوماتية الوطنية، بما يعني إنشاء وتطوير البِنْيَة التحتية والأنظمة المعلوماتية المختلفة؛ لضمان مستوًى عالٍ من الأمن القومي.

- ضرورة إنشاء تشكيلات ووحدات خاصة بالأمن المعلوماتي داخل الإطار الحكومي تكون مهمتها تطوير الأمن المعلوماتي، ورسم سياسة الدفاع والهجوم الإلكتروني وحماية المعلومات.

- على الدول العربية أن تسعى لتطوير منظومتها القانونية العربية التي تنظم الجانب المعلوماتي وتطور تشريعاتها الوطنية ذات الصفة الأمنية.

- كفالة الدعم الكامل للإعلام المصري لدَعْمِ وإيضاح أهمية الأمن المعلوماتي، وتأكيد حماية ما لدينا من مخاطر القرصنة أو الإرهاب المعلوماتي.

قائمة المراجع

(1) رضا إبراهيم صالح وآخرون: دراسة أثر إدارة أمن المعلومات في نجاح برنامج أمن نظم المعلومات المحاسبية، مع دراسة ميدانية على الشركات المصرية، بحث منشور، مجلة الدراسات التجارية المعاصرة المجلد السادس – العدد العاشر – الجزء الأول 2020م، صـ111.

(2) راجع قريبًا من هذا المعنى، خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، الإسكندرية، الدار الجامعية، 2008م، صـ28، صـ29.

(3) قريب من ذلك، آية طارق عبد الهادي سيد، منار علي محمد أحمد: دور الإعلام الإلكتروني في التوعية بأهمية الأمن المعلوماتي وتفاعل الجمهور معه، دراسة تطبيقية على البنوك المصرية، بحث منشور بمجلة مستقبل العلوم الاجتماعية، العدد الثامن، يناير 2022م، صـ66.

A handbook prepared by Piret Pernik, Jesse Wojtkowiak, and Alexander Verschoor-Kirss, about information security and National Cyber Security Organisation: UNITED STATES, published in 2016, by NATO CCD COE, from P5. to P6..

(4) راجع في هذا المعنى، فيلالي أسماء، شليل عبد اللطيف: تهديدات أمن المعلومات وسبل التصدي لها، مجلة البشائر الاقتصادية، المجلد الرابع، العدد الثالث، 2019م، صـ165.

(5) راجع في هذا المعنى، ياسر محمد عبد السلام رجب: التطورات التشريعية المستحدثة في مجال الأمن المعلوماتي، دراسة مقارنة، المجلة العربية للمعلوماتية وأمن المعلومات، المؤسسة العربية للتربية والعلوم والآداب، المجلد 3 العدد 6، يناير 2022م، صـ127، وما بعدها، وما نشر بعنوان شهر التوعية بالأمن الإلكتروني المعلوماتي أو السيبراني 2021 م.

(6) Research Article prepared by Rasim M. Alguliyev , Yadigar N. Imamverdiyev Rasim Sh. Mahmudov and Ramiz M. Aliguliyev, about Information security as a national security component, published on 20 Jul 2020, published by Journal A Global Perspective, from P3. to P4.

(7) راجع في هذا المعنى، تقرير صادر عن هيئة الاتصالات وتقنية المعلومات، بعنوان « إجراءات التعامل مع حوادث الأمن السيبراني في قطاع الاتصالات وتقنية المعلومات والبريد بالمملكة العربية السعودية»، بتاريخ نوفمبر 2020م، صـ5.

(8) راجع بالتفصيل عن الأمن القومي العربي، علي الدين هلال: الوحدة والأمن القومي العربي، بحث منشور بمجلة الفكر العربي، عدد مزدوج 12-11، السنة الثانية، أغسطس 1979م، صـ94 وما بعدها .

(9)from pre-mentioned reference (Research Article prepared by Rasim M. Alguliyev , Yadigar N. Imamverdiyev Rasim Sh. Mahmudov and Ramiz M. Aliguliyev, about Information security as a national security component,

published on 20 Jul 2020, published by Journal A Global Perspective, from P.4 to P5).

(10) راجع حكم المحكمة الإدارية العليا – الطعن رقم 10171 لسنة 54 ق . ع – الصادر بجلسة 2011/2/26م، - مجلس الدولة – المكتب الفني – مجموعة المبادئ التي قررتها المحكمة الإدارية العليا، السنة الخامسة والخمسين والسادسة والخمسين – من أول أكتوبر 2009 إلى آخر سبتمبر 2011 – صـ877

(11) راجع القانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات الباب الأول المادة الأولى الأحكام العامة، ويتكون من أربعة أبواب وخمس وأربعين مادة، والمنشور بجريدة الوقائع المصرية بالعدد 32 مكرر (ج) بتاريخ 14 من أغسطس سنة 2018م.

(12) راجع بالتفصيل، المحكمة الإدارية العليا – الطعن رقم 15118 لسنة 65 ق – بتاريخ 2019/12/21م، وأيضًا المعنى ذاته ورد بحكم المحكمة الإدارية العليا – الطعن رقم 59568 لسنة 64 ق – بتاريخ 2020/6/13م متاح على موقع الموسوعة القانونية لوزارة العدل المصري، عبر الموقع الإلكتروني التالي:

https://emj-eg.com .

(13) ومن هذه التشريعات التي تتناول الأمن المعلوماتي راجع على سبيل المثال:

- قانون خصوصية الاتصال الإلكتروني بالولايات المتحدة الأمريكية الصادر عام 1986م، وهناك بعض القوانين تم إدراجها من المقترحات المعروضة على الكونجرس الأمريكي في الآونة الأخيرة منها قانون خصوصية المعلومات الشخيصة وأمنها لعام 2014م، قانون أمن البيانات لعام 2014م.
- قانون خصوصية المعطيات بالولايات المتحدة الامريكية والصادر عام 1997م.
- قانون حماية المعطيات بألمانيا والصادر عام2000 م.
- مشروع قانون حماية البيانات بألمانيا والصادر عام 2000م.
- قانون معالجة الآلية للمعطيات بفرنسا والمُعَدَّل في عام 2000م.
- قانون حماية المعطيات الإنجليزي والصادر عام1984 م.
- قانون حماية المعلومات بروسيا والصادر عام1995 م.
- قانون حماية البيانات في إيطاليا والصادر عام1996 م.

(14) راجع من هذه الدراسات على سبيل المثال، شريف يوسف خاطر: حماية الحق في الخصوصية المعلوماتية دراسة تحليلية لحق الاطلاع على البيانات الشخصية، دراسة مقارنة، الناشر دار الفكر والقانون، 2015م.

(15)A handbook prepared by JOANNA LYN GRAMA, VANTAGE TECHNOLOGY CONSULTING GROUP, about Protecting Privacy and Information Security

in a Federal System, published in May 2019, published by the Institute for Higher Education Policy, from P8. to P9.

Article prepared by James Andrew Lewis, about Cyber Security and Regulation in the United States, published in Fall 2015, edited on 17 April 2018, published by Center for Strategic and International Studies, edited by The Wall Street Journal, from #P. to P.

(16) راجع في ذلك، نشوى رأفت إبراهيم أحمد: «حماية الحقوق والحريات الشخصية في مواجهة التِّقْنِيَّة الحديثة البيانات الشخصية، المراسلات والمحادثات الشخصية، الحقّ في الصورة»، رسالة دكتوراه، كلية الحقوق جامعة المنصورة، 2012م، صـ277 وما بعدها.

(17) راجع، المرسوم السلطاني رقم 6/2022 بإصدار قانون حماية البيانات الشخصية، والمنشور بالجريدة الرسمية العدد 1429، السنة الحادية والخمسين، وذلك بتاريخ 13/2/2022م، والمكون من 5 فصول، و32 مادة، متاح عبر الموقع الإلكتروني التالي:

https://qanoon.om/p/2022/rd2022006/.

(18) راجع، المرسوم بقانون اتحادي رقم 5 لسنة 2012م، في شأن مكافحة جرائم تقنية المعلومات، والمعدَّل بالقانون الاتحادي رقم 12 لسنة 2016م، والمنشور بالجريدة الرسمية بملحق العدد 597 الموافقة 2016/5/31م، ويحظر القانون معالجة البيانات الشخصية دون موافقة صاحبها، وذلك باستثناء بعض الحالات التي من ضمنها أن تكون المعالجة ضرورية لحماية المصلحة العامة، أو لإقامة أي = =من إجراءات المطالبة بالحقوق والدعاوى القانونية، موقع وزارة العدل لدولة الامارات العربية المتحدة، وموقع دولة الامارات العربية المتحدة، متاح عبر الموقع الإلكتروني التالى:

:https://elaws.moj.gov.ae/MainPdfFromLaw.aspx،https://u.ae/ar-ae/about-the-uae/digital-uae/data/.

(19) راجع بالتفصيل القانون رقم 13 لسنة 2016م بشأن حماية خصوصية البيانات الشخصية القطري، والمكون من ثمانية فصول وعدد 32 مادة، منشور بالجريدة الرسمية القطرية بالعدد 15 بتاريخ 2016/11/3م، متاح عبر الموقع الإلكتروني التالي:.https://www.almeezan.qa/LawPage.aspx?id

(20) منشور بالجريدة الرسمية، بالعدد 3 مكرر (أ) بتاريخ18/1/2014 م، متاح عبر الموقع الإلكتروني التالي: http://alamiria.laa-eg.com/.

(21) من بين هذه الجهود والمحاولات التشريعية الأخرى ما يلي: قرار وزير الاتصالات 107 لسنة 2005 بشأن مكتب حماية برامج الحاسب الآلي وقواعد البيانات، قرار وزير الاتصالات 128 لسنة 2006 بشأن اختصاص الجهاز القومي لتنظيم الاتصالات بنظر المنازعات المتصلة بالاتصالات، وإنشاء إدارة

تُسمى «إدارة فض المنازعات» بالجهاز، قرار وزير الاتصالات رقم 108 لسنة 2005 بشأن تحديد الخدمات والأعمال الخاضعة لرسم تنمية صناعة تكنولوجيا المعلومات والاتصالات.

(22) نشر هذا القرار بالجريدة الرسمية في ديسمبر 2014، العدد الخمسون مكرر (أ)، بتاريخ 2014/12/15. ونص في مادته الأولى على أن ينشأ مجلس أعلى لأمن البِنْيَة التحتية للاتصالات وتكنولوجيا المعلومات يتبع رئاسة مجلس الوزراء ويسمى المجلس الأعلى للأمن السيبراني، ويُشَكَّل برئاسة وزير الاتصالات وتكنولوجيا المعلومات وعضوية ممثلي وزارات: «الدفاع، والخارجية، والداخلية، والبترول، و الثروة المعدنية، و الكهرباء والطاقة المتجددة، والصحة والسكان، والموارد المائية والري، والتموين والتجارة الداخلية، والاتصالات وتكنولوجيا المعلومات» وجهاز المخابرات العامة، والبنك المركزي المصري، وعدد 3 من ذوي الخبرة في الجهات البحثية والقطاع الخاص يرشحهم المجلس، ويصدر بتعيينهم قرار من وزير الاتصالات وتكنولوجيا المعلومات.

(23) منشور بالجريدة الرسمية – العدد 32 مكرر (ج) بتاريخ 2018/8/14.

(24) راجع المادة 34 من الفصل السادس «الظروف المشددة في الجريمة» من الباب الثالث «الجرائم والعقوبات» من قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018م.

(25) منشور بالوقائع المصرية العدد رقم 208 تابع، في 18 من سبتمبر 2019 م.

(26) راجع بالتفصيل، القانون رقم 151 لسنة 2020م بإصدار قانون حماية البيانات الشخصية، منشور بالجريدة الرسمية العدد 28 مكرر (هـ)، والصادر في 15 من يونيه سنة 2020م، والمكون من أربعة عشر فصلًا و49 مادة.

(27) راجع القانون رقم 150 لسنة 2021م بتعديل بعض أحكام قانون العقوبات، والمنشور بالجريدة الرسمية العدد رقم 46 مكرر، في 20 من نوفمبر 2021م.

(28) راجع بالتفصيل، قرار رئيس الجمهورية رقم 232 لسنة 2021 الجريدة الرسمية – العدد 22 (مكرر) – في يونيه سنة 2021 بإنشاء مجمع الإصدارات المؤمنة والذكية.

(29) راجع بالتفصيل قرار وزير الخارجية رقم 45 لسنة 2014م، بشأن الموافقة على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، والمنشور بالجريدة الرسمية بالعدد رقم 46 لسنة 2014م، بتاريخ 2014/11/13م.

(30) Reading book prepared by Tim Stevens, about Power in UK Cybersecurity and information protection, published in 2018, published by Office of Cyber Security, from P4. to P5.

(31) A handbook prepared by Harold F. Tipton, CISSP. Micki Krause, CISSP, about Information Security Management= =(Sixth Edition, VOLUME 2), published in December 2020, by CRC Press (Taylor and Francis group) from P1. to P7.

(32)A handbook prepared by Harold F. Tipton, CISSP. Micki Krause, CISSP, about Information Security Management (Sixth Edition, VOLUME 2), published in December 2020, by CRC Press (Taylor and Francis group) from P1. to P7.

(33)From pre-mentioned reference (Reading book prepared by Tim Stevens, about Power in UK Cybersecurity and information protection, published in 2018, published by Office of Cyber Security, from P3. to P5.)=

= Report prepared by Members of the House of Commons, about information and Cyber security in the UK, published on 15 May 2019, by House of Commons, from P2. to P8.

(34) راجع بالتفصيل في هذا المعنى، بحث بعنوان الإستراتيجية الوطنية للأمن السيبراني، مصر الرقمية 2017-2021م، متاح عبر الموقع الإلكتروني:

http://www.mcit.gov.eg.

(35) للمزيد حول الأمن المعلوماتي والأمن القومي راجع بالتفصيل، رياض بن عربية: الأبعاد الإستراتيجية للجرائم الإلكترونية وتهديداتها للأمن الوطني، دفاتر البحوث العلمية، المجلد 9، العدد 1، السنة 2021، الصفحة 259–279.

(36) راجع هذا الرأي: ليتيم فتيحة، ليتيم نادية: الأمن المعلوماتي للحوكمة وإرهاب القراصنة، مجلة الفكر، العدد الثاني عشر، من دون سنة نشر، صـ249.

(37) راجع بالتفصيل التقرير الصادر عن الأمم المتحدة «الإسكوا» تحت عنوان: «الأمان في الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية توصيات سياسية».

(38) راجع في هذا المعنى، ذياب البداينة، الإشاعة السيبرانية في المجتمع الرقمي، أمثلة على الوقاية في التعامل مع جائحة فيروس كورونا (COVID – 19)، مجلة الدراسات القانونية والأمنية، المجلد الأول – العدد الأول – يوليو 2021م، صـ44.

(39)The Emergence of cyber security law, prepared for the Indiana university Maurer school of law by Hanover Research, February, 2015.,3. “Lawyers must play a role in designing the procedures, training and risk assessments required to implement managerial operational and technical controls needed to protect data”.

(40)sales ،Nathan Alexander: Regulating cyper security – Northwestern university law Review 2013 vol., 107, No 4, p. 1506 “According to Brace smith, the united states follows a “bifurcated approach to network security prevention and public investment in prosecution .

(41) sales ،Nathan Alexander: Regulating cyper security – Northwestern university law Review 2013 vol., 107, No 4, p. 1506 “According to Brace smith, the united states follows a “bifurcated approach to network security prevention and public investment in prosecution .

(42) Research Article prepared by Rasim M. Alguliyev, Yadigar N. Imamverdiyev Rasim Sh. Mahmudov and Ramiz M. Aliguliyev, about Information security as a national security component, published on 20 Jul 2020, published by Journal A Global Perspective, from P6. to P7.