AL-NAHRAIN JOURNAL OF LEGAL SCIENCE Vol.26 (NO. 3) 2024, pp. 221-244

AL-NAHRAIN UNIVERSITY
COLLEGE OF LAW

ISSN:3006- 0605 DOI:10.58255

مجلة النهرين للعلوم القانونية العدد: ٣ المجلد: ٢٦ آب ٢٠٢٤

Received:5/5/2024 Accepted: 1/7/2024 Published: 1/8/2024

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0)

The Role of Criminal Law in Protecting Digital Data

Dr. Sabreen Naji Taha
Al – Nahrain University/College of Law
sabreen.naje@nahrainuniv.edu.iq

Extracted
First of all, it must be said that digital data is all the information that is transmitted through electronic technologies, and digital data has not been spared from the effects resulting from the information revolution and technology, because the required compatibility between the naturalness of data and the nature of the crime from which it is generated, led to the multiplicity of digital data resulting from the multiplicity of moral and software components of computers and the information network, and with the technical development in technologies, criminals are using these techniques to attack digital data.
Therefore, the problem of our research revolves around showing the extent to which Iraqi government institutions are able to protect digital data and what are the frameworks of criminal legal texts on which the judiciary is based to provide criminal protection for these data, in the absence of a legal text that keeps pace with the continuous developments in these technologies.
The provision of criminal protection for these data entails taking into account the confidentiality and privacy of these data, and ensuring that government policies and regulatory legislation achieve a balance between the need for all transactions and the development of digital content and services, ensuring the criminal protection of personal data and reducing Information Technology Crimes.
Keywords: protection, data, digital, law.

دور القانون الجنائي في حماية البيانات الرقمية

م. د. صابرين ناجي طه
كلية الحقوق – جامعة النهرين
sabreen.naje@nahrainuniv.edu.iq

المستخلص
بداية لابدَّ من القول ان البيانات الرقمية هي جميع المعلومات التي يتم مناقلتها عبر التقنيات الالكترونية، ولم تسلم البيانات الرقمية من التأثيرات الناتجة عن ثورة المعلومات والتكنلوجيا، ذلك ان التوافق المطلوب تحقيقه بين طبيعية البيانات وطبيعة الجريمة التي يتولد منها، ادى الى تعدد البيانات الرقمية الناتجة عن تعدد المكونات المعنوية والبرمجية للحواسيب وشبكة المعلومات، ومع التطور التقني في التقنيات اضحى المجرمون يستخدمون هذه التقنيات للإعتداء على البيانات الرقمية.
وعليه تدور اشكالية بحثنا حول بيان مدى قدرة المؤسسات الحكومية العراقية على حماية البيانات الرقمية وما هي اطر النصوص القانونية الجزائية التي يستند اليها القضاء لتوفير الحماية الجنائية لهذه البيانات، في ظل عدم وجود نص قانوني يواكب التطورات المتواصلة في هذه التقنيات.
مع العرض توفير الحماية الجنائية لهذه البيانات يستلزم مراعاة السرية والخصوصية لهذه البيانات، والتأكد من ان السياسات الحكومية والتشريعات المنظمة تحقق التوازن بين الحاجة الى جميع المعاملات وتطوير المحتوى والخدمات الرقمية، وضمان الحماية الجنائية للبيانات الشخصية والحد من جرائم تقنية المعلومات.ا
لكلمات المفتاحية: الحماية، البيانات، الرقمية، القانون.

المقدمة

يعتبر الأمن الركيزة الأساسية للمجتمع، بحيث لا يمكن تصور نمو أي نشاط لدوائر الدولة بعيداً عن تحققه، سواء أكان ذلك على المستوى التقني أم على المستوى القانوني، إذ يشكل الامن احد اهم قطاع الخدمات والتي تعد قيمة مضافة ودعامة أساسية لأنشطة الحكومات والافراد، على السواء ، كما هو الحال مع التطبيقات الخاصة بالحكومة الالكترونية، والصحة الالكترونية، الإ ان الوجوه المتعددة لسياسة آمن المعلومات ومضاعفها الخطيرة لا تقف عند حدود الافراد والمؤسسات بل تتعداها الى تعريض سلامة الدول والحكومات، ونتج عن ظهور أنظمة سياسة أمن المعلومات العديد من التحديات والمخاطر التي لم تكن معروفة في السابق والتي تستدعي من الدوائر الامنية أن تقوم بتطوير أنشطة الرقابة الداخلية لديها من خلال إعداد السياسات والإجراءات التي تتيح الرقابة على هذه الأنظمة الإلكترونية.

وقد ظهرت سياسة حماية البيانات الرقمية كأحد نتائج هذا التطور التكنولوجي المتسارع، حيث انتشرت هذه الأنظمة بسرعة كبيرة مدفوعة بعدة عوامل منها الحاجة لتوفير المعلومات الملائمة والموثوقة والتي تساعد اجهزة الدولة على اتخاذ القرارات المناسبة على الصعيدين المحلي والدولي بالإضافة لتطور العمليات وتعقيدها وصعوبة تعامل العنصر البشري مع هذا الحجم الهائل من البيانات الناتجة عنها، ويصاحب الانتشار الواسع للتحول الرقمي دائما جرائم مرتبطة بالبيانات، لأن هذا الأول قائم على فكرة البيانات وتحويلها من ملموسة وورقية إلى افتراضية غير ورقية، تتعدد وتتنوع صور جرائم البيانات التي ظهرت في عصر التحول الرقمي، ونعرض بعضا منها لتوضيح خطورة هذه الجرائم وأهمية التصدي لها ومكافحتها، وهذا يعد المغذى الحقيقي من وراء الدارسات الاستباقية للتطورات الحديثة وتأثيرها على أشكال ومعدل الجريمة، وذلك من أجل الحد من انتشار الجريمة سواء باتباع اجراءات احترازية معينة أو وضع عقوبات صارمة تحقق الردع العام داخل المجتمع.

أولاً: أهمية البحث: تتمحور أهمية موضوع بحثنا في مدى أهمية البيانات الرقمية وآلية حمايتها جنائياً وهذا ما سنلخصه في ضوء النقاط الآتية:

١- تتعرض البيانات الى انواعاً كثيره من الاعتداء كالأتلاف والاستيلاء أو الجمع غير المشروع لها.

٢- زيادة قدرات التقنيات الحديثة، وتدفق البيانات والنقل المتكرر لها بين الجهات، بالإضافة إلى العولمة المتطورة التي زادت من اهمية البيانات الرقمية.

٣- ارتباط حماية البيانات مع الأمن القومي الدولي لما يشكله جمع واستغلال واختراق البيانات بطرق غير مشروعة من خطورة مطلقة على الدولة.

٤- خطورة استغلال هذه البيانات بصوره غير شرعية باستخدام خوارزميات الذكاء الاصطناعي، لتفلتر اهتمامات وميول أصحاب تلك البيانات.

ثانيا- هدف البحث: تتركز أهمية البحث في ضوء النقاط الآتية:

١- بيان مفهوم البيانات الرقمية ومدى خطورة الاعتداء عليها.

٢- تسليط الضوء على إمكانية تطبيق النصوص الجنائية التقليدية على هذا النوع من الجرائم ومعرفة نقاط القصور في بعض التشريعات والنصوص الإجرائية التي تتصدى للجرائم الإلكترونية.

٣- أن حماية البيانات الرقمية لها اهمية كبيرة في الحد من الاختراقات الامنية ، وتوفير أمن نظم المعلومات الإلكترونية والمرتبط بإمكانية مواجهة سـرقة المعلومات والبيانات أو فقدانها أو تعديلها.

ثالثا- اشكالية البحث: تتركز أشكالية موضوع بحثنا في ضوء التساؤلات الآتية:

١- بيان مدى جواز اختراق موقع إلكتروني – كنوع من أنواع الدفاع الشرعي – في حالة قيامه بنشر محتوى يشكل انتهاك لخصوصية شخص ما؟

٢- هل تتوفر السرية والخصوصية والحماية ضد التلاعب للبيانات الالكترونية، وماهي التشريعات التي تم سنها من أجل ضمان الحماية الجنائية للبيانات؟

٣- الإطار القانوني لخدمات سياسة امن المعلومات وآلية الحد من الاختراقات الامنية، وبيات الالتزامات القانونية المترتبة على ذلك والعلاقات بين أطراف خدمات امن المعلومات.

٤- عدم توفر المعرفة الكافية عن مدى احتواء أنظمة سياسة امن المعلومات على وسائل وأدوات لمنع واكتشاف الأساليب المختلفة للاختراقات الإلكتروني المرتبطة بأمن المعلومات المحاسبية الإلكترونية والإجراءات اللازمة لتصحيح ثغرات النظام؟

٥- مدى فاعلية إجراءات حماية البيانات الرقمية في منع الاختراقات الإلكترونية المرتبط بأمن المعلومات قبل حدوثه؟ وما هي فاعليتها في الحد من الاختراقات الامنية؟

٦- ما هي الثغرات الامنية التي تســـببت الاختراقات الامنية المرتبط بأمن المعلومات لدوائر الدولة؟ وما هي المعوقات المؤثرة في الرقابة الداخلية المرتبطة بمخاطر أمن دوائر الدولة؟

رابعا- منهج البحث:

للإجابة عن الاشكالية الرئيسة للبحث وعن التساؤلات الفرعية قرّرنا اعتماد **المنهج الوصفي والاستقرائي** الذي يتركز هذا المنهج على جمع البيانات والمعلومات المتعلقة بموضوع بحثنا، للوقوف على معرفة تامة عن **دور القانون الجنائي في حماية البيانات الرقمية.**

خامسا- هيكلية البحث: قسمنا بحثنا الموسوم اعلاه الى ثلاث مطالب بينا في الاول مفهوم حماية البيانات الرقمية، وتطرقنا في الثاني الى استخدام الحاسوب في الأعتداء على البيانات الرقمية، وخصصنا الثالث الى الآليات الاجتماعية والقانونية والفنية في حماية البيانات الرقمية، واختتمنا البحث ببعض الاستنتاجات والمقترحات .

المطلب الاول

مفهوم حماية البيانات الرقمية

ادى التطور الهائل والانتشار السريع والمخيف لشبكات المعلومات الى اختصار المسافات بين الدول ولتشمل العالم كله جاعلة منه قرية صغيرة وأصبح المستفيد من الممكن أن يكون أي شخص، وبيئة التشغيل أصبحت من الممكن أن تكون أي مكان، أي أن التقنية يمكن أن تستخدم في أي مكان وزمان مع هذا التطور ازدادت أهمية قضية أمن المعلومات وقضية الأمن بشكل عام فأصبحت بالفعل مشكلة تبحث عن حل وأصبحت هذه القضية تهم رجال الأعمال والمدراء وكل من لديه معلومات وأصبحت تهم المستفيد العادي ودوائر الدولة التي تقدم خدمات المعلومات ومصممي النظم والتطبيقات وكذلك الشركات المطورة للأجهزة والبرمجيات، ومن هذا المنطلق اصبح لزاماً بيان تعريف البيانات الرقمية، ومفهوم حمايتها وذلك في الآتي:

الفرع الاول

تعريف البيانات الرقمية لغة واصطلاحا

أن مصطلح "البيانات" شائع منذ خمسينات القرن الماضي وتم استعماله في مجالات متنوعة مما جعل له استخدامات متنوعة في الاستعمال الدارج، و"والبيانات" أصلها في اللغة الفرنسية والانجليزية والالمانية والروسية كلمة "Informlio" اللاتينية بحسب الاصل والدالة على شيء للإبلاغ والتوضيح

أو على عملية "Process" اي الابلاغ أو التنقل أو التوصيل وهو نفس ما تعنيه مفردة "Xinxi" المقابلة لها في اللغة الصينية[١].

وتُعرف "البيانات الرقمية" بأنها تعبير عن مجموعة من الارقام والكلمات والرموز أو الحقائق أو الاحصاءات الخام الالكترونية التي لا علاقة بين بعضها البعض ولم تخضع بعد للتفسير او التجهيز للاستخدام والتي تخلو من المعنى الظاهر في اغلب الاحيان[٢].

وعلى العموم فالبيانات في ابسط تعريفاتها الاصطلاحية تعني " المعطيات الأولية التي تتعلق بنشاط أو قطاع ما"[٣]، اما الأستاذ "Parke" فقد عرفها بأنها " مجموعة من الصور والرموز أو الحقائق أو المفاهيم أو التعليمات التي تصلح لأن تكون محلاً للتبادل والاتصال أو التفسير والتأويل أو المعالجة، سواءٌ بواسطة الافراد أو الانظمة الالكترونية"، وهي تتميز بالمرونة بحيث يمكن تغيرها وتجزئتها وجمعها أو نقلها بوسائل وأشكال مختلفة[٤].

ومن الناحية التشريعية فقد عرفها قانون التوقيع الالكتروني والمعاملات الإلكترونية العراقي رقم ٧٨ لسنة ٢٠١٢ بالقول "المعلومات، البيانات والنصوص والصور والأشكال والأصوات والرموز وما شابه ذلك التي تنشأ أو تدمج أو تخزن أو تعالج أو ترسل أو تسلم بوسائل إلكترونية"[٥].

الفرع الثاني

تعريف حماية البيانات الرقمية

تعد حماية البيانات الرقمية من أهم حقوق الإنسان المعترف بها، وقد أثرت تقنية المعلومات على هذا الحق حين انتشرت شبكات الحاسوب والمعلومات في المجتمعات المعاصرة ، وإزاء هذه الطفرة بدأت الطرق التقليدية لجمع وتنظيم المعلومات عاجزة عن تلبية احتياجات المستفيدين من المعلومات، وأصبح محتما استخدام تقنية علمية متطورة لمواجهة فيض المعلومات المتدفق من خلال جهاز الحاسب الآلي، الأمر الذي أدى إلى التحكم في المعلومات وتجميعها ومعالجتها واختزانها واسترجاعها[٦]

---

[١] احمد حسام الدين طه تمام: الحماية الجنائية لتكنولوجيا الاتصالات. دراسة مقارنة، ط٢، دار النهضة العربية، القاهرة، ٢٠٠٢، ص٧٨.

[٢] جلال محمد الزعبي واحمد محمد المناعسة: جرائم تقنية المعلومات الالكترونية، ط١، دار الثقافة للنشر والتوزيع، عمان، ٢٠١٠، ص١٠٠.

[٣] د. سليم عبد الله الجبوري: الحماية القانونية لمعلومات شبكة الانترنيت، ط١، منشورات الحلبي الحقوقية، ٢٠١١، ص٣٥.

[٤] أحمد كيلان عبد الله / بلال عبد الرحمن محمود: سياسة أستبدال الصفة الجنائية للعقوبة، دراسة مقارنة، المركز العربي للنشر والتوزيع، مصر، ٢٠١٩، ص٥٥.

[٥] ينظر: الفقرة ثالثا من المادة ١ منه.

[٦] ياسر الأمير، فاروق، مراقبة الأحاديث الخاصة في الإجراءات الجنائية، الطبعة الأولى، دار المطبوعات، الجامعية، الإسكندرية، ٢٠٠٩ص٢٩.

وتحسين الانتفاع بها ، وفي ذهب الأستاذ الدكتور رمسيس بهنام إلى القول ان حماية البيانات الخاصة بالإنسان هي قيادة الإنسان لذاته في الكون المحيط به، ويعنى ذلك قيادة الإنسان لجسمه في الكون المادي المحيط لجسمه وقيادة الإنسان لنفسه في الكون النفسي المحيط به" ، وتعرّف حماية البيانات الرقمية بأنها "هي السياج الواقي لتلك الحياة من قيود ترد دون مبرر على حرية مباشرتها ومن أضرار تصيب بدون مسوغ صاحبها من وراء هذه المباشرة" فالحياة الخاصة للإنسان تأبى أي قيد يرد على حرية قيادته لنفسه كما تأبى أي ضرر يصيبه في جسمه أو في نفسه بدون وجه حق من وراء مباشرته لتلك القيادة . كما تعرّف حماية البيانات[٣] الرقمية على انها حق الفرد في إضفاء طابع السرية على المعلومات التي تتولد عن ممارسته حياته الخاصة.[٤]

وفي ذلك تناول الدستور المصري الصادر عام ٢٠١٤ مفهوم حماية البيانات الرقمية عن طريق التأكيد على الحق في الخصوصية وفي ذلك سردت المادة ٥٧ منه صور حماية الحق في الخصوصية في مجال الاتصالات الشخصية حيث نصت على انه (للحياة الخاصة حرمة، وهي مصونة لا تمس، وللمراسلات البريدية، والبرقية، والإلكترونية، والمحادثات الهاتفية، وغيرها من وسائل الاتصال حرمة، وسريتها مكفولة، ولا يجوز مصادرتها، أو الاطلاع عليها، أو رقابتها إلا بأمر قضائي مسبب، ولمدة محددة، وفي الأحوال التي يبينها القانون، كما تلتزم الدولة بحماية حق المواطنين في استخدام وسائل الاتصال العامة بكافة أشكالها، ولا يجوز تعطيلها أو وقفها أو حرمان المواطنين منها، بشكل تعسفي، وينظم القانون ذلك).[٦]

ولم يتضمن نص المادة ما يسمح بالخروج عن هذه القاعدة وانتهاك البيانات الرقمية إلا في حالة تنفيذ الأوامر القضائية والتي أيضا خضعت لضوابط زمنية ومُبررات يجب أن تكون واضحة، وبالإضافة إلى ذلك فقد تضمنت الفقرة الثانية من نص المادة ٥٧ من الدستور عبارات قد تسمح للمُشرع الدستوري بالنص على ضوابط تتعلق بتنظيم عملية تعطيل أو وقف وسائل الاتصال، ولم تضع سوى قيد واحد على المشرع الدستوري، ألا يكون وقف أو تعطيل الاتصالات بشكل تعسفي، ونصت المادة ٥٤ من الدستور المصري الصادر عام ٢٠١٤ «للمنازل حرمة، وفيما عدا حالات الخطر، أو الاستغاثة لا[٧]

---

[١] علواني هليل فرج ، التحقيق الجنائي والتصرف فيه، دار المطبوعات الجامعية، الإسكندرية، ٢٠٠٦، ص٤٨٠.
[٢] رمسيس بهنام، نطاق الحق في الحياة الخاصة - بحث مقدم لمؤتمر الحق في الحياة الخاصة المنعقد بكلية الحقوق - جامعة الاسكندرية في الفترة من ٤-٦ يونيه، ١٩٨٧، ص٩٨.
[٣] أحمد حسام الدين طه تمام، مرجع سابق، ص٨٩.
[٤] محمد علي السالم عياد الحلبي، ضمانات الحرية الشخصية أثناء التحري والاستدلال في القانون المقارن، بلا دار نشر وطبعة، ١٩٨١ص٣٣.
[٥] علي يوسف، الشكري، حقوق الانسان بين النص والتطبيق، دار صفاء للنشر، عمان ط١، ٢٠١١ص٨٧.
[٦] سحر محمد نجيب، التنظيم الدستوري لضمانات حقوق الانسان وحرياته، مطابع شتات، مصر، ٢٠١١ص٣٣.
[٧] وسن حميد، رشيد، الرقابة على دستورية القوانين في العراق والامارات العربية المتحدة، رسالة ماجستير مقدمة الى اكاديمية الدراسات العليا، طرابلس، ليبيا٢٠٠٩، ص٨٧.

يجوز دخولها، ولا تفتيشها، ولا مراقبتها أو التنصت عليها إلا بأمر قضائي مسبب، يحدد المكان، والتوقيت، والغرض منه، وذلك كله في الأحوال المبينة في القانون، وبالكيفية التي ينص عليها، ويجب تنبيه من في المنازل عند دخولها أو تفتيشها، واطلاعهم على الأمر الصادر في هذا الشأن"، بالإضافة إلى النصوص التي توفر حماية للحق في الخصوصية يتضمن الدستور نصّا خاصّا يتعلق بعدم جواز تقادم الجرائم المرتبطة بالاعتداء على الحقوق والحريات بشكل عام، وبالجرائم التي تُشكل اعتداء على الحياة الخاصة للمواطنين بشكل خاص»، اما المادة ٩٩ من الدستور المصري الصادر عام ٢٠١٤ «كل اعتداء على الحرية الشخصية أو حرمة الحياة الخاصة للمواطنين، وغيرها من الحقوق والحريات العامة التي يكفلها الدستور والقانون، جريمة لا تسقط الدعوى الجنائية ولا المدنية الناشئة عنها بالتقادم، وللمضرور إقامة الدعوى الجنائية بالطريق المباشر، وتكفل الدولة تعويضا عادلا لمن وقع عليه الاعتداء، وللمجلس القومي لحقوق الإنسان إبلاغ النيابة العامة عن أي أنتهاك لهذه الحقوق، وله أن يتدخل في الدعوى المدنية منضمّا إلى المضرور بناء على طلبه، وذلك كله على الوجه المبين بالقانون».[٢]

اما موقف المشرع العراقي من مفهوم حماية البيانات الرقمية، فلم تتضمن التشريعات مفهوما للبيانات الرقمية الا انه كفل حمايتها في العديد من النصوص منها المادة (٣٧) من دستور جمهورية العراق لعام ٢٠٠٥ التي اشارة ان حرية الفرد العراقي وكرامته مصونة وكذلك في المادة (١٧) منه والتي تضمنت الحق في الخصوصية الشخصية للفرد العراقي بما لا يتنافى مع حقوق الآخرين، وكذلك الحال في المادة ٤٠ من الدستور آنف الذكر التي نصت على ان حرية الاتصالات والمراسلات البريدية والهاتفية والالكترونية وغيرها مكفولة ولا يجوز مراقبتها أو التصنت عليها إلا لضرورة قانونية أو أمنية و بقرار قضائي. وعلى صعيد قانون العقوبات العراقي المرقم ١١١ لسنة ١٩٦٩ المعدل حيث نصت المادة (٣٢٨) منه على: "يعاقب بالسجن مدة لا تزيد على سبع سنوات أو بالحبس كل موظف أو مستخدم في دائرة البريد والبرق والهاتف وكل موظف أو مكلف بخدمة عامة فتح أو اتلف أو أخفى رسالة أو برقية أودعت أو سلمت للدوائر المذكورة أو سهل لغيره ذلك". كما نصت المادة (٤٣٨) على ان: "يعاقب بالحبس مدة لا تزيد على سنة وبغرامة أو بإحدى هاتين العقوبتين، كل من نشر بإحدى طرق العلانية أخبارا أو صورا أو تعليقات تتصل بأسرار الحياة الخاصة أو العائلية أو الإفراد، ولو كانت صحيحة، اذا كان من شأنها الإساءة إليهم، ومن اطلع من غير من ذكروا في

[١] صالح جواد كاظم، ملاحظات حول مفهوم علوية حقوق الانسان، مباحث في القانون الدولي، دار الشؤون الثقافية العامة، بغداد، ط١، ١٩٩١، ص٨٧.

[٢] عثمان خليل عثمان، المبادئ الدستورية العامة، مكتبة عبدالله وهبة، ١٩٩٩، ص٢٢.

المادة (٣٢٨) من قانون العقوبات العراقي على رسالة أو برقية أو مكالمة هاتفية، فأفشاها لغير من وجهت إليه اذا كان من شأن ذلك إلحاق الضرر بأحد".

يتضح للباحثة مما تقدم ان المشرع العراقي حمّى البيانات الرقمية في العديد من نصوص الدستور العراقي، وكذلك الحال في مواد قانون العقوبات العراقي الذي وأن كان تشريعه في عام ١٩٦٩ أي قبل اختراع الشبكة المعلوماتية، فهو تضمن عددا من النصوص التقليدية التي يمكن تطويعها في اطار حماية البيانات الرقمية عن طريق التفسير الواسع لتلك النصوص، مع العرض فالضرورة تقتضي تشريع قانون مكافحة الجرائم المعلوماتية وسد الفراغ التشريعي بخصوص تلك الجرائم المستحدثة ضد البيانات الرقمية.

المطلب الثاني

استخدام الحاسوب في الأعتداء على البيانات الرقمية

لا يستطيع احد ان ينكر اهمية الحاسوب بوصفه من المظاهر الفذة للتقدم العلمي التي وفرت على الانسانية جهداً كبيراً ، ولكن في الوقت نفسه لا يمكن التغاضي عن مثالبه ذات الخطورة الجمة ، حتى قيل ان شفافية الانسان وخصوصياته قد باتت عارية امام ما تمخض عنه العلم من اعجاز في مجال الحاسوب ، ورغم المزايا العظيمة التي[١] يقدمها الحاسوب لمجتمعنا المعاصر ، والتي هي في تكاثر مستمر فانها قد اوجدت الى جانب ذلك العديد من الاخطار الجديدة وامكانية التعرض الى اضرار جسيمة جعل البعض يشك حتى في مصداقية جدواها او فائدتها للبشرية مطالباً بوقف العمل بانظمة الحاسوب او تجميدها لفترة ما .[٢]

وتعد اساءة استخدام الحاسوب السبب الرئيسي لاكثر اخطار الحاسوب واوسعها نطاقاً حيث تشمل الافعال غير القانونية كافة سواء عدت جرائم ام لا ، وهذا ما سنتطرق له في الآتي:

الفرع الاول : استخدام المعلومات الشخصية لغرض المراقبة

لما كان الحاسوب اله لاسلكية للمراقبة، و يخلق امكانية صنع نموذج معقد للمراقبة، اذ ان بعض نظم معلومات الحاسوب تستطيع اذا شاء لها مشغلوها ان تستخدم بكفاءة عالية لأغراض المراقبة و هذا ينطبق بوضوح على الحواسيب الكبيرة التي تديرها حالياً اجهزة الامن في معظم دول الغرب ومنظمات الخدمات و المؤسسات الاخرى ، و قد شاع استخدام هذه المعلومات الاستخبارية المبرمجة التي تتضمن معلومات دقيقة عن كل شخص ، مثل العادات الشخصية

[١] د. ممدوح خليل بحر ، الحماية القانونية لبرامج الكمبيوتر واثرها في الامن القومي العربي، بغداد : مجلة الامن العام ، ع ١ ، س ١٢ ، ١٩٩٢ ، ص ١٢١ .

[٢] طارق الدسوقي عطية: الأمن المعلوماتي، " النظام القانوني للحماية المعلوماتية"، دار الجامعة الجديدة، الاسكندرية، ٢٠١٠، ص٢٣

والاماكن المفضـــلة التي يرتادها الاشـــخاص حتى وان لم تتعلق بجريمة اذ ان مثل هذه المعلومات انما تدخل جهاز الحاسوب لتثبت و يساء استخدامها لاحقاً .[1]

بل قيل ان هذه المعلومات تعد حجر الزاوية لنظام اكثر اتساعاً و شمولاً تقصد منه الرقابة الدائمة لعشر السكان و جميع ارقام السيارات و اسماء اصحابها و عناوينهم، ذلك ان القدرة الخيالية التي وصـــل اليها الحاســـوب في تجميع المعلومات المختلفة عن الفرد في كل تحرك من تحركات حياته او تصـــرف مما يقوم به تجعل الفرد اســـيراً للمعلومات التي جمعتها عنه هذه الاله، بل ان احتمالات الرقابة المعلوماتية ستكون مروعة ، فمنذ شروع الفرد صباحاً بأخذ واسطة النقل الى مقر عمله و حتى عودته مساءً ستكون جميع تحركاته و تصرفاته مدونة في انظمة الذاكرة الالكترونية و في كل خطوة أي حين يوقف مركبته في المرآب او عند دخوله دائرته او حين استخدامه للهاتف او تناوله طعامه او مراجعته للطبيب ، كل ذلك سوف يسجل وستكون حالات قليلة يستطيع خلالها الفرد ان يتحرك وهو محتفظ بخصوصيته الشخصية .[2]

وبدأ بعض الباحثين بأثارة اسئلة عن ضمان الحياة الخاصة ، و التحرر في عصر التطور الالكتروني ، ولكن هذه الاصـوات لها صـوت تحذيري ضـعيف امام الجمع الكبير من مصـممي الحواسيب و مستخدميها الذين يندفعون الى تصميم منظومات متكاملة و حرة الانتشار.

الفرع الثاني : استخدام المعلومات الشخصية لغرض تجاري

من ابلغ الأخطار التي تهدد حياة الفرد الخاصة هو ان المعلومات التي جمعت عنه تستخدم لإغراض الكسب غير المشروع ، و رغم استمرار الجدل حول نشاط الشركات الكبرى ، فأن جدلاً اكثر حدة يدور الان حول الشـركات التي تدير قواعد معلومات صـغيرة و تعرض بياناتها بأسـعار منخفضـة تقل كثيراً عن اسعار الشركات الكبرى ، و المشكلة ان الشركات الصغيرة لا تأبه كثيراً لخصوصية المعلومات او حساسيتها فالمهم عندها ان يكون الزبون قادراً على الدفع سواء كان مخبراً او صحفيا خاصاً او محصل ضرائب او زوجاً و غيرهم .[3]

و نجم عن ذلك تحول عمليات جمع البيانات الى صـــناعة تدر ملايين الدولارات ســـنوياً والمفارقة ان البعض يقـدم البيانات الضرورية لهذه الصناعـة مجانـاً دون ان يدري، فعند الحصول على إجازة سوق او قرض عقاري او جهاز هاتف او عند الدخول الى المستشفى او التقدم الى عمل ، يقوم الأشخاص المعنيون بملء استمارات حافلة بالأسئلة الشخصية (كالوضع المالي او الصحي

[1] سليم عبد الله الناصر ، الحماية القانونية لمعلومات شبكة المعلومات (الانترنت) ،رسالة دكتوراه ، جامعة النهرين ، كلية الحقوق ، ٢٠٠١ ، ص٢٦٢ .

[2] عمر محمد يونس: المجتمع المعلوماتي والحكومة الالكترونية، الطبعة الاولى، الأبحاث، موسوعة التشريعات العربية ٢٠٠٣، دار الفكر الجامعي، الاسكندرية، ٢٠٠٣، ص٢٣.

[3] نبيل عبد المنعم جاد: جرائم الحاسب الآلي، مؤتمر المواجهة الامنية للجرائم المعلوماتية، دبي، الامارات العربية المتحدة، ٢٠٠٠، ص٢٣.

او الاجتماعي ٠٠٠) والتي تتلقفها شـــركات المعلومات و تقارنها بمعلومات حصـــلت عليها من مصادر أخرى (بعضها حكومية) ، لرسم صورة أوضح و ادق للزبائن و الأهداف المنتخبة .

و كمثل صارخ في عــدم الاهتمام بالحرمــات الشخصية في عالم الحاســوب ما حدث في الولايات المتحدة الأمريكية لإحدى هيئات نظام البيانات عندما أنهت أعمالها فعرضت للبيع و بأعـــلى سعر محتويات معلوماتها عن ثلاثة ملايين مواطن [٢] .

و لمواجهة مخاطر الانتفاع المعلوماتي اقترح المدافعون عن الخصـــوصـــية تشـــكيل هيئة خاصة لحماية البيانات تنحصر مهمتها بضمان عدم إساءة استخدام المعلومات الشخصية المخزنة في الحواسيب الحكومية ، و يطمع هؤلاء إلى تنظيم استخدام المعلومات من قبل الشركات الخاصة و ذلك بفرض المزيد من القيود على عملها و إجبارها على استحصال موافقة الشخص المعني قبل التصرف بالمعلومات المتعلقة به ، علماً إن مراكز جمع المعلومات الشخصية كانت قد التزمت عام ١٩٩٨، بأن تطبق مبادئ تضمن حسن السلوك عبرها ، و مع ذلك يبقى الشك حول مدى التزام تلك المراكز بالمحافظة على خصـوصـية الأفراد وحرياتهم مما يجعل التصـدي التشـريعي لمواجهة تلك الأخطار ضرورة قصوى [٣] .

و إيجاد هيئات قضـائية متخصـصـة و مؤهلة للحكم في قضـايا المعلوماتية و إقرار مبدأ التعويض للإفراد كلما بيعت معلومات شخصية عنهم .

الفرع الثالث : استخدام البيانات الرقمية لغرض الإساءة الى السمعة

تعد سمعة الفرد من أدق أمور حياته الخاصة ، و الصورة التقليدية للاعتداء على الحق في الخصوصية تكون عن طريق الكشف عن الخصوصيات أي عن طريق اعلانها للغير ، فالنشر هو الذي يجعل الحياة الخاصـــة عرضـــة للانظار و مادة تناقلها الألســن ، ولهذا لا يجوز لأية جهة او وكالة ان تنشـــر ما يصـــل الى علمها من و قائع او معلومات تتعلق بالحياة الخاصـــة للغير الا بعد الحصـول على إذن صـاحب الشـأن، وان موافقة الفرد المعني حول جمع المعلومات عنه ومعالجتها الكترونياً تفيد انه قد ائتمن جهة معينة على ان تلتزم بكتمان اسرار حياته الشـخصـية ، اما في حالة اطلاع الغير على هذه المعلومات دون تخويل او موافقة مسـبقة ، فأن هذه الجهة تتعرض للمسـاءلة القانونية عن جريمة افشـــاء معلومات مبرمجة في الحاســـوب اذا كان من شـــأنها ان تمس شـــرف الشـــخص و اعتباره او تتعلق بحياته الخاصـــة ، وبذلك فأن الفرد لايزال يواجه مخاطر تعرضـــه

[١] فاتن ليث الربيعي ، في مجتمع المعلومات المفتوحة حرب ساخنة ضد قراصنة المعلومات ، مقال نشر في جريدة الجمهورية ، ع٨٠٥٥ ، س٢٥ ، ٥ك١ ، ١٩٩١ ، ص٥٠ .

[٢] يوسف صغير: الجريمة المرتكبة عبر الانترنت، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، الجزائر، ٢٠١٣، ص٨٧.

[٣] احمد، طارق عفيفي: الجرائم الالكترونية، جرائم الهاتف المحمول، دراسة مقارنة بين القانون المصري والاماراتي والنظام السعودي المركز القومي للاصدارات القانونية، مصر ٢٠١٤، ص٧٠.

للتشـهير ، والى نشـر ما لا يرغب ان يعرفه الناس عنه ، اذ ان نشـر معلومات تضـعه في موضـع غير صـحيح يؤدي الى الحط من سمعته لدى أفراد المجتمع او تجعله عرضـة للبغض والسـخرية او تؤدي به الى الانزواء و الانعزال [١] .

و هو الامر ذاته الذي يمكن تصوره في نشر امور تتعلق بفرد من افراد عائلة هذا الشخص او قضـية تتصـل بها ، مما يجعل سـمعته عرضـه للأقاويل و التي هو في غنى عنها ، فالحياة الخاصـة للشـخص تعد أيضـا و أثناء حياته جزءً من الحياة الخاصـة للعائلة ، فهذه الحياة لا تخص الشـخص فقط و انما تخص الأسرة ايضـاً ، و من ثم فمن حق الأسرة ان تدافع عنها حتى في حياة الشخص نفسه [٢] .

و هكذا و بوجود نظام المعالجة الالكترونية للمعلومات الشـخصـية ، فأن نشـر معلومات خاطئة عن شخص ما قد يعرض الهيئات المعنية الى المساءلة وهو الامر الذي يستلزم ان يستحق المضرور التعويض عنه .

المطلب الثالث

الآليات الاجتماعية والقانونية والفنية في حماية البيانات الرقمية

تتزايد التهديدات التي تتعرض لها المنظمات نتيجة التطور المتسـارع في الأسـاليب التي يمكن من خلالها الوصول لبيانات ومعلومات سرية خاصـة بالمنظمة بشكل غير مصرح به بهدف تعديلها أو سرقتها أو حتى تدميرها، والمتمثلة في اختراق الشبكات بقصد به الوصول غير المصرح به للشبكة أو نظام المعلومات المحاسـبي بهدف تعديل البيانات أو المعلومات أو سـرقتها أو تدميرها، ويحتوي هذا الأسـلوب على عدة تقنيات منها التالية التي تم اختيارها في أداة الدراسـة كأمثلة على تقنيات شائعة جداً في هذا المجال ، فضلاً عن سرقة كلمة السر، واختراق الشبكة والإطلاع على المعلومات الخاصـة بالدوائر الأمنية من خلال سـرقة كلمة السـر الخاصـة بالمعنيين داخل الدوائر الأمنية، ولما كانت الأعمال والتجارة لا تزدهر أو تسـتقر إلا بتوافر الثقة والأمن بسـائر أنواعهما ومراتبهما سـواء الاجتماعية، الفنية "التقنية" والقانونية فإننا نبسـط في هذه الورقة مفهوم الأمن الاجتماعي والفني والقانوني للأعمال الإلكترونية[٣]. وسنتناول ذلك على النحو الآتي:

[١] احمد حسام طه: الجرائم الناشئة عن الحاسب الآلي، دار النهضة العربية، القاهرة، ٢٠٠٠، ص٩٨.
[٢] خالد ممدوح ابراهيم: حوكمة الانترنيت، ط١، دار الفكر الجامعي، الاسكندرية، ٢٠١١، ص١٢٢.
[٣] سامي علي حامد عياد: الجريمة المعلوماتية وجرائم الانترنيت، دار الفكر الجامعي، الاسكندرية، ٢٠٠٧، ص٦٦.

الفرع الاول: الآليات الاجتماعية في حماية البيانات الرقمية:

في كل مجتمع من المجتمعات المعاصرة تسود معايير أخلاقية بشكل أو بآخر تكيف بعض الأفعال على أنها من قبيل الصواب والبعض الآخر من قبيل الخطأ، كما يوجد نوع ثالث من الأفعال في منطقة رمادية غير محددة المعالم لا يمكن وصفها بأنها صواباً أو خطأ. إن الرادع الأخلاقي كان ولا يزال بشكل أقل متجذراً في الأصل بالعقائد الدينية ومع مقدم عصر النهضة في الدول الأوروبية وما تبع ذلك من ثورة تجارية وصناعية في العالم العربي وطغيان قيم الحضارة المادية والفصل في كثير من المجتمعات الحديثة بين الدين والدولة ظهور الانقسام في العالم العربي الحديث بين ما يعرف بشؤون الكنسية وشؤون الدولة حيث أصبحت العقائد الدينية في الكثير من المجتمعات الغربية الحديثة مسائل شخصية وأضحى كثير من البشر في المجتمعات الغربية الحديثة منصاعين لما يعرف بالثورة العلمية والتكنولوجية الحديثة واعتقد البعض أن الإنسان هو سيد الكون وقد نتج عن ذلك فلسفات متعددة تقوم على اساس لا ديني علماني بشري بحت ومثالها النزعات النفعية، الليبرالية، الوضعية، الماركسية والمادية المفرطة بل تطرق البعض إلى القول بوحدانية السوق[١]، بل ظهر ما يعرف بمعتقدات العصر الجديد بعيدة عن الوحي الإلهي وأصبح في تلك المجتمعات الغربية المعيار الأخلاقي قائماً على أساس وأيدلوجيات جاء بها الفكر الإنساني الفلسفي أو على نظم التعامل العملية القائمة على العقد الاجتماعي حيث تحول المجتمع في جانب كبير منه من المجتمع الإيماني إلى المجتمع العلماني الذي يقوم على الأساس النفعي التعاقدي، هذا وقد تأثرت تلك المجتمعات بالتغير السريع في العلوم والتكنولوجيا وتبدلت العادات الاجتماعية فظهر السلوك النسبي مع الابتعاد عن المطلق بل إن الفصل بين الكنيسة والدولة في المجتمعات الغربية أدى إلى انتشار مبدأ منطق الدولة ومنطق المؤسسة الاقتصادية الذي قد لا يعبأ كثيراً بقيم دينية أو أخلاقية فيما يتعلق بسلوك الدولة أو سلوك المنشأة الاقتصادية هذا ومع ذلك ولا يزال لخط الدفاع الأول أو الرادع الأخلاقي أثره حيث يقرر منطق البقاء السائد في المجتمعات الغربية. إن لكل فعل رد فعل "وأن الإنسان ترتد عليه بشكل مادي ملموس نتائج أفعاله فيفضل من باب الذكاء الاجتماعي أن يعامل الإنسان الغير كما يجب أن يتم التعامل معه ووجدت تلك المجتمعات أن الأمانة وعدم الغش في حد ذاتهما لهما فوائد نفعية عملية[٢]، ومن الممكن للدولة أن تطالب بإعمال سيف القانون لكن ليست كل مشكلة قابلة للحل بإعمال القانون أو باستحداث قوانين جديدة ذلك أن للمجتمع حدوداً في القدرة على تطبيق وتنفيذ قوانين وتبقى الأخلاق هي خط الدفاع الأول.

[١] د. ايمن عبدالله فكري: جرائم نظم المعلومات، دراسة مقارنة، دار الجامعة الجديدة للنشر، الاسكندرية، ٢٠٠٧، ص٢٢.

[٢] أ.م.د نغم حمد الشأوي/ بلال عبد الرحمن محمود المشهداني: ابحاث في القانون الجنائي، مكتبة القانون المقارن، ط١، بغداد، ٢٠٢٠، ص٢٠.

الفرع الثاني: الآليات الفنية التقنية في حماية البيانات الرقمية: يشمل أمن المعلومات والاتصالات استخدام وسائل تقليدية لتحقيق الأمن وكذلك وسائل حديثة غير تقليدية[١].

اولا– الاساليب التقليدية في حماية البيانات الرقمية: تتمثل تلك الوسائل المؤمنة في وسائل الإنذار ضد الاختراق أو الحريق وتكون درجة الأمن التقليدي متناسبة مع أهمية وحساسية وموقع منشآت وأجهزة الاتصالات أو المعلومات أو الحاسبات المطلوب حمايتها ويقوم الأمن التقليدي على عناصر فنية وإدارية وهندسية بوجود إدارات الأمن في المنشآت واستخدام الوسائل والأدوات الفنية التقليدية في الحماية والتأمين إضافة إلى التصميم الهندسي الآمن لتلك المنشآت وصفوة القول في هذا المقام هو ما قرره عالم حديث من أن الأمن التقليدي يتمثل في الحراسة، التحصين، التشريع، التدريع، القفل والفتح[٢].

ثانيا– الأساليب والوسائل غير التقليدية في حماية البيانات الرقمية: ضرورة وجود نظام كفء لإدارة المعلومات وأمن المعلومات والاتصالات ويشمل ذلك:

أ. تطبيق إجراءات أمن المعلومات وأمن الاتصالات ومنها ما يلي[٣]:

١. تبني سياسة أمنية جيدة ومرنة.

٢. تحديد المسؤوليات والسلطات درءاً لشيوع المسؤولية والالتزام بالنظام من الكبير والصغير.

٣. حصول كل مستخدم لنظام المعلومات والاتصالات على مفتاح الدخول خاص به المختلف عن مفاتيح الغير للدخول إلى النظام مع خضوع مفتاح الدخول لجميع متطلبات السياسة الأمنية المتبناة.

٤. إيجاد الوسائل الفنية الآلية لتسجيل محاولات الاختراق الفاشلة للنظام وتسجيل ميعاد وتاريخ حدوثها وكذلك تحديد الوحدة الطرفية التي تمت من خلالها محاولة الاختراق لتمكن من الوصول إلى الفاعل.

٥. مناقشة وتحليل كل محاولات الاختراق غير الناجحة واتخاذ ما يلزم لتحصين النظام.

٦. تشفير وترميز المعلومات والبيانات الحساسة.

٧. تغير مفاتيح التشفير بكل متكرر غير دوري.

٨.إسناد مهمة إدارة مفاتيح التشفير لشخصين وليس لشخص واحد باستخدام نظام ثنائي منعاً" من انفراد شخص بذلك.

٩. فصل خطوط الاتصالات غير اللازمة للدخول إلى نظم الحاسبات والمعلومات.

١٠. قصر توزيع المعلومات والبيانات المشفرة والحساسة على عدد محدود ومعلوم ومرخص له في تداول تلك البيانات بقدر ما يلزم .

---

[١] د. محمد عبيد الكعبي: الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت، الطبعة الثانية، دار النهضة العربية، ٢٠٠٩، ص٩٠.

[٢] أحمد كيلان عبد الله / بلال عبد الرحمن محمود: مرجع سابق، ص٣٣.

[٣] حسن الغافري: السياسة الجنائية في مواجهة جرائم الانترنيت، دار النهضة العربية، القاهرة، ٢٠٠٩، ص٦٥.

١١. حصر توزيع المعلومات على الأفراد أو الأقسام التي تكون تلك المعلومات لازمة وضرورية لها للقيام بوظائف تلك الأقسام أو الأعمال دون غيرها.

١٢. الحفاظ على البيانات في بنك بيانات محدد تتوافر له الحماية.

١٣. تحديد مستويات الولوج أو الدخول إلى النظم بشكل متعدد الطبقات.

١٤. في حالة استخدام المعاملات المالية المشفرة تحفظ أرقام بطاقات الاعتماد في بنوك بيانات مستقلة غير متصلة بالشبكات ويجب ألا يتضمن تداول البيانات بين الأقسام الرقم الكامل لكارت الائتمان بل آخر ٤ أرقام فقط.

ب. الوسائل والأدوات الفنية لتوفير أمن المعلومات والاتصالات، ومنها على سبيل المثال[ ]:

١. استخدام خطوط تليفونات واتصالات ووحدات تلفونات وقناة اتصالات ملونة .

٢. استخدام تكنولوجيا SSL وهي تكنولوجيا تتضمن بروتوكولاً أمنياً للإنترنت فيكون الولوج إلى النظام لمن هم مرخص لهم بذلك.

٣. استخدام تكنولوجيا التوقيع الرقمي أو الإلكتروني في الرسائل الإلكترونية للتحقق من نسب المستند الإلكتروني لمنشئه ومرسله.

٤. استخدام خدمات التحقق والتصديق الإلكتروني وهي خدمات متاحة عن طريق سلطات كهيئات البريد في بعض الدول أو بعض دوائر الدولة المرخص لها وهي توفر تحققاً للمتعامل في التجارة الإلكترونية من شخصية مرسل البيانات أو الطرف الآخر في العلاقات التعاقدية الإلكترونية.

٥. استخدام تكنولوجيا العلامات المائية أو الأختام الإلكترونية الخاصة على الوثائق الإلكترونية.

٦. استخدام الوسائط البيوقياسية للدخول إلى النظم ومن ذلك ماسح بصمة اليد أو قزحية أو شبكة العين وخاصة في الأجهزة المحمولة.

٧. استخدام النقود الإلكترونية في المعاملات الإلكترونية درءاً للنصب والاحتيال والسرقة.

الفرع الثالث: الآليات القانونية في حماية البيانات الرقمية:

لا يمكن تأمين جميع التعاملات الإلكترونية بشكل مطلق فالتقنيات وآليات سلامة الأجهزة والاتصالات قد تفشل في التزويد بالحماية الفعالة ضد الهجمات المعقدة وكذلك فالأمن القانوني يستطيع تدعيم النواقص الأمنية. وفي هذه الحالة فإنه من الضروري الحصول على إمكانية المحاكمة القانونية

[ ]حنان ريحان المضحكي: الجرائم المعلوماتية "دراسة مقارنة"، ط١، منشورات الحلبي الحقوقية، بيروت، ٢٠١٤، ص٣٤.

للمهاجمين والمخربين والمتنصلين، إن عصب الأعمال الإلكترونية والتجارة الإلكترونية هو الوثيقة الإلكترونية التي هي في أساسها بيانات ومعلومات يتم توليدها وتبادلها عبر وسائط إلكترونية بين الأطراف كبديل عن الوثائق الورقية فتحل الرسائل الإلكترونية والعقود الإلكترونية محل الرسائل والعقود التقليدية التي تحرر على الوسيط المادي الورقي[١].

والغرض من توافر الأمن القانوني هو تحقيق عدة غايات وقائية وغايات علاجية، ولابد من وجود الأسس والمستلزمات والأركان الضرورية لقيام التعامل الإلكتروني بشكل قانوني سليم وهي الأركان التي يجب توافرها في الوثيقة الإلكترونية إذا ما أردنا إيجاد تجارة وأعمال إلكترونية، ولقد أصبحت تكنولوجيا الاتصالات، مثل الإنترنت والهواتف الذكية النقالة والأجهزة العاملة بالاتصال اللاسلكي بالإنترنت، جزءاً من الحياة اليومية، وبإدخال تحسينات جذرية على إمكانية الوصول إلى المعلومات والاتصال الفوري، عززت الابتكارات في مجال تكنولوجيا الاتصالات حرية التعبير ويسرت النقاش العالمي ووطدت المشاركة الديمقراطية. وبتضخيم أصوات المدافعين عن حقوق الإنسان وتزويدهم بأدوات جديدة لتوثيق التجاوزات وكشفها، تَعِدُ هذه التكنولوجيات القوية بتحسين التمتع بحقوق الإنسان، وفي الوقت الذي أصبحت فيه وقائع الحياة المعاصرة تدور في الفضاء الإلكتروني أكثر من أي وقت مضى، أصبحت الإنترنت، في الوقت نفسه، موجودة في كل مكان وحميمية بشكل متزايد، وفي العصر الرقمي، عززت تكنولوجيا الاتصالات أيضاً قدرات الحكومات والمؤسسات والأفراد على القيام بأعمال المراقبة واعتراض الاتصالات وجمع البيانات، وكما لاحظ المقرر الخاص المعني بالحق في حرية التعبير والرأي، تعني أوجه التقدم التكنولوجي أن فعالية الدولة في القيام بعمل المراقبة لم تعد محدودة من حيث النطاق والمدة. وأدى انخفاض تكاليف التكنولوجيا وتخزين البيانات إلى القضاء على الروادع المالية والعملية للقيام بعمل المراقبة، وتملك الدول حالياً من القدرات أكثر من أي وقت مضى للقيام بعمل مراقبة متزامن واقتحامي ومحدد الهدف وواسع النطاق، وبعبارة أخرى، فإن المنصات التكنولوجية التي تعتمد عليها الحياة السياسية والاقتصادية والاجتماعية العالمية بشكل متزايد ليست غير حصينة أمام المراقبة الجماعية فحسب، بل يمكن في الحقيقة أن تيسر هذه المراقبة[٢].

وفي التشريع العراقي صدر قانون العقوبات العراقي رقم (١١) لسنة ١٩٦٩ بنص يحرم الاعتداء على وسائل الاتصال السلكي واللاسلكي في المادة (٣٦٣) فيه لم يعالج الجريمة الحاسوبية ولكن جاء بنص عام، وصدر القانون رقم (٣١) لسنة ٢٠١٣ لتصديق الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، صدر قانون التوقيع الالكترونية والمعاملات الالكترونية رقم (٧٨) لسنة ٢٠١٢.

---

[١] سالم روضان الموسوي: جرائم القذف والسب عبر القنوات الفضائية، ط١، منشورات الحلبي الحقوقية، بيروت، ٢٠١٢، ص٧٦.

[٢] حنان ريحان المضحكي، مرجع سابق، ص٧٦.

الخاتمة

توصلت الباحثة الى أن التطور التكنلوجي غير المسبوق في مجال الاتصالات الذي يشهده العالم في الربع الأخير من القرن الماضي أدى إلى طفرة تكنلوجية في مجال الاتصالات والمعلومات وأنتجت شبكة المعلومات الدولية (الانترنت)وقد صار يستخدم على نطاق واسع في تبادل المعلومات والبيانات وإتاحتها من وإلى أي مكان في العالم دون أن تقف للحدود الجغرافية عائقا أمام هذا التدفق المتواصل للمعلومات والبيانات المختلفة وقد ظهرت مشكلات قانونية عديدة ولعل أهمها ما يتعلق بحماية البيانات الرقمية عبرها إذ توجد على الشبكة العديد من البيانات المختلفة سواء البيانات التي تم ترقيمها بمحتواها أو بشكلها ليتم بثها عبر الانترنيت ومن المعلوم أن البيانات المتاحة على الشبكة منها ما هو محمي بموجب حقوق الملكية الفكرية الأدبية لحقوق المؤلف أو الحقوق المجاورة ومنها محمي بموجب حقوق الملكية الفكرية الصناعية والواقع أن خطورة الانترنيت على البيانات الرقمية تتأكد من عدة جوانب ففي الجانب أول أن التحول إلى شبكة الانترنيت لا يخلو في حد ذاته من مخاطر النسخ غير المشروع أو التحوير بالنسبة لتلك البيانات ومن جانب أخر أن تقنيات الترقيم قد تقتضي بطبيعتها تحوير المصنف ليلائمها أو عن طريق ما تنتجه تقنيات الوسائط المتعددة إذ يتم دمج بيانات محمية بعد تحويرها لتخرج في صورة معلومات أو بيانات رقمية تبث على الانترنيت دون الحصول على ترخيص بذلك من قبل صاحب الحق في تلك البيانات ، ومن ثم فأي تنوع وتعدد لصور الاعتداء على البيانات الرقمية، لذا فان الحاجة الملحة لتوفير الحماية الفعالة للبيانات الرقمية تقتضي تشريع القوانين المناسبة لحماية حقوق البيانات الرقمية في ظل تقنيات تجوب بمحل حقوقه أرجاء العالم عبر شبكة المعلومات الدولية. وعلى اساس ذلك توصلنا الى عدد من الاستنتاجات والمقترحات وفق الآتي:

اولا- الاستنتاجات

١- اتجاه غالبية الدول إلى تعديل تشريعاتها الحالية وسن قوانين شاملة، تعتمد فيها على القواعد المستقر عليها دوليا، وتهدف إلى وضع إطار عام يضمن حماية الحياة الخاصة للأفراد، وضمان خصوصية البيانات الرقمية في ظل التطورات التكنولوجية الحديثة، وأيا كانت مسوغات إدراج الحقوق والحريات في الدساتير، هناك أتفاق على أن غياب النص عليها بصورة صريحة قد يتخذه الحكام ولاسيما في بلدان العالم الأقل تطورا أو ذات الأنظمة الشمولية ذريعة لحرمان المواطن من التمتع بهذا الحق أو ذاك بحجة عدم النص عليه.

٢- أفرز التقدم العلمي ظهور انماط مستحدثة من المجرمين لم تكن موجودة من قبل مثل نمط الهواة والمبتدئين والهاكرز والكراكرز، ارتبط ظهور انماط مستحدثة من مرتكبي الجرائم بعدم

الاقتصار على ذات الدوافع في ارتكاب الجرائم التقليدية، إذ ظهرت دوافع ايضاً تتسم بالحداثة وشملت بجانب تحقيق المكسب المادي والانتقام ايضاً اثبات التفوق العلمي والدعابة والتسلية كدوافع جديدة على ارتكاب الجرائم.

٣- بزوغ وسائل حديثة في ارتكاب الجرائم تختلف عن الوسائل التقليدية المعروفة، كبرنامج الفيروس والبرامج الشبيهة بالفيروس، فضلاً عن ظهور انماط حديثة في اساليب ارتكاب الجرائم مثل كسر كلمات السر وانتحال الشخصية وغيرها من الاساليب الاجرامية الحديثة.

٤- محدودية سياسة آمن المعلومات في الحد من الاختراقات الامنية وذلك لعدّة اسباب أهمها القصور التشريعي في مواجهة تلك الجرائم، وعدم وجود كوادر أمنية مؤهلة لمواجهة هذه الانماط الاجرامية المستحدثة، وكذلك ضعف آليات الأجهزة الشرطية لمواجهة هذه الجرائم.

٥- على الرغم من فاعلية اجهزة الرقابة الداخلية على أمن المعلومات غلا أن درجة الفاعلية كانت تعتمد على عاملين وهما وجود مدققين داخليين يعملون ضمن كادر الدوائر الامنية، وايضا وجود كفاءات علمية تعمل على تعزيز إجراءات الرقابة الداخلية.

ثانيا- المقترحات:

١- على الصعيد الاجتماعي:

أ- إلزام شركات الهاتف النقال بالتأكد من صحة المستمسكات الرسمية لأصحاب الارقام (الخطوط) وأجراء التحديث عليها، وبيان أصحابها الحقيقين ومتابعة انتقال ملكيتها أو اي تغيير فيها والتعاون مع الجهات التحقيقية في تزويدها بكل ما تحتاجه من بيانات ومعلومات لغرض انجاز التحقيقات في قضايا أنتهاك الحق في الخصوصية.

ب-ضرورة نشر الوعي المجتمعي بمخاطر أنتهاك حق الإنسان في أتصالاته الشخصية بتظافر جهود منظمات المجتمع المدني ووسائل الاعلام من خلال إقامة الحلقات النقاشية وورش العمل والندوات والمؤتمرات وخاصة للفئات المستهدفة للطلبة في المدارس والجامعات وكذلك لرجال الدين من خلال التعريف بالآثار السلبية لأنتهاك الحق بالخصوصية الشخصية.

٢- على الصعيد الفني التقني:

أ- الدعوة إلى إنشاء أجهزة متخصصة للتحقيق في الجرائم السبيرانية والجرائم التي تنطوي على إدلة الكترونية، وتبرز صعوبة هذه الدعوى العدد القليل من أفراد الشرطة المتخصصين إذ ما قورنت بعدد مستخدمي الانترنيت.

ت- تفعيل استخدام تقنيات التحاليل الجنائية التي تتضمن إنشاء نسخ (مطابقة الأصل من المعلومات المخزونة والمحذوفة، واستخدام برامج (منع الكتابة) من أجل ضمان عدم تحريف المعلومات الأصلية، واستخدام الخوارزميات للملفات المشفرة أو استخدام التوقيفات الرقمية بغية ابراز أي تعديلات تدخل على المعلومات.

ث- اتباع القواعد التي تحكم أمن المعلومات من خلال تحديد المعلومات المهمة وتحليل المخاطر والتهديدات وتحليل القابلية للعدوان وتطبيق الإجراءات المضادة ومرحلة التقييم، الاهتمام بوجود انظمة الاستكشافات والاقتحام داخل المنشآت أو المؤسسات من خلال دوائر الحماية، وحدة الضبط، جهاز الاشارة، وسيلة ارسال، جهاز انذار، إضاءة كافية.

ج- الاهتمام بتطبيق انظمة للسيطرة على قواعد الدخول والخروج من خلال اتباع قواعد ضبط الدخول والخروج للأشخاص وتحديد الهوية بالرؤية والمعرفة الخاصة أو باستخدام الخصائص البيولوجية، وتطبيق نظم الدوائر التلفزيونية المغلقة من خلال الكاميرات وشاشات الرصد وأجهزة نقل الصور من خلال شبكات الألياف الضوئية والبلاستيكية.

ح- ضرورة دعم الإدارة لأنشطة الرقابة الداخلية على أمن المعلومات من خلال توفير الكوادر المؤهلة في قسم التدقيق الداخلي بالإضافة لتوفير التدريب اللازم لهم للتعرف على التحديات الجديدة التي أمن المعلومات وأساليب مكافحتها.

خ- تكوين فريق لمواجهة الجرائم الالكترونية بداية من المدير ومشغل النظام والمراقب والمراجع والمحقق الجنائي والمستشار الفني وأفراد الحماية، تحديد اختصاص كل عضو بالفريق، واتباع عناصر التدريب للحد من الاختراقات الامنية.

د- تحديد اسلوب عمل في الحد من الاختراقات الامنية بحيث يتواكب مع أسلوب عمل المنشأة مع عدم أهمال الأسس التي يجب على اي فريق اتباعها عند مواجهته للأزمة المعلوماتية، وهذه الاسس هي القدرة على تحقيق التنسيق والتكامل والترابط بين مختلف الانشطة التي يقوم

عليها اعضاء الفريق الواحد، فضلاً عن القدرة على التنبؤ بالأحداث المستقبلية والمرونة في التنفيذ السريع لمواجهة الاحداث المتتابعة والسريعة والفجائية، وتوفير الامكانيات اللازمة لذلك.

٣- على الصعيد الأمني:

أ- تعزيز وحدات الشرطة الديمقراطية بدلا من الإبقاء على المفهوم التقليدي لقوى الأمن القائم على مراقبة السلوك المادي للأفراد والتي تعمل بالمشاركة مع الأفراد من خلال أبراز الجانب التوعوي والتعبوي ضد الجريمة عموما وذلك بالنظر لحداثة الوسائل المستخدمة في الجريمة الالكترونية وتنوع صور ارتكابها مما يتطلب أشراكهم في المتابعة والتحري لضمان سرعة الإبلاغ والوصول للجناة .

ب-إنشاء مكاتب متخصصة من الشرطة أسوة بالقانون كقانون جرائم المعلوماتية السوداني لسنة ٢٠٠٧ ، وتعزيز التعاون الدولي بين أجهزة الشرطة وان كان يرتبط ذلك بوجود مفهوم موحد للجريمة الالكترونية، مع إنشاء هيئة للمساعدة التقنية تتولى مهمة التعاون مع أجهزة الأمن وتعمل بالتنسيق مع شركات الاتصالات والانترنيت التي عليها الاحتفاظ بمعلومات المشتركين.

٤- على الصعيد القانوني:

أ- لابد من إيجاد متطلبات للتعامل الدولي وفق الأسس التي ينص عليها القانون الدولي. لان اغلب القوانين التشريعية الجنائية لا تمتلك الأطر القانونية لإتباعها في هذا المجال. لاسيما أن في اغلب الأحيان ليس من الضروري أن تقع كل عناصر الجريمة السيبرانية داخل البلد من أجل تأكيد ولايته القضائية الإقليمية وذلك من خلال تحديد موقع النظم والبيانات الحاسوبية المستخدمة في ارتكاب الجريمة.

ب-تمكين السلطة المختصة من ملاحظة إعداد النظام ألمعلوماتي بما يضر بحق الخصوصية، وتأهيل جهة التفتيش حفاظا على أدلة الإثبات، فرض عقوبة مشددة لمن يفشي السرية نتيجة التفتيش، ويفضل أن يكون الشاهد من ذوي الخبرة وعلى ان يعزز الشهادة بطبع الملفات والاخبار عن كلمة السر، لايجوز إهمال أي دليل الكتروني.

ت-وجود قضاء حكم متخصص حفاظا على حيادية القاضي واستقلاله.

ث- إمكانية وجود اتفاق دولي لتسيل المساعدة القضائية المتبادلة وتسليم المجرمين وسهولة تنفيذ الأحكام.

ج- استخدام الخصائص البيولوجية وتطويعها في الحماية الجنائية سواء عن طريق بصمة الإبهام أو حدقة العين أو بصمة الصوت، أو بصمة خط اليد في عملية التأمين، اعداد برامج امن المعلومات من خلال تحديد أشخاص تتولى المسؤولية في اتمام ذلك.

ح- سد الفراغ التشريعي في مجال مكافحة الجريمة الإلكترونية، على أن يكون شاملا للقواعد الموضوعية والإجرائية، وعلى وجه الخصوص النص صراحة على تجريم الدخول غير المصرح به إلى الحاسب الآلي وشبكات الاتصال (الإنترنت) والبريد الإلكتروني، وكذلك اعتبار البرامج والمعلومات من الأموال المنقولة ذات القيمة، أي تحديد الطبيعة القانونية للأنشطة الإجرامية التي تمارس على الحاسب الآلي والإنترنت، وأيضا الاعتراف بحجية للأدلة الرقمية وإعطاؤها حكم المحررات التي يقبل بها القانون كدليل إثبات.

خ- دعوة المشرع العراقي الى ضرورة التدخل بإصدار قانون مكافحة الجرائم المعلوماتية، بما لا يتعارض مع الحقوق والحريات المكفولة دستوريا في العراق، مع تضمينه نص يجيز للجهات المعنية القبض ومحاكمة مجرمي أنتهاك الحق في الخصوصية، وتوفير ضمانات لضحايا الجريمة محل البحث.

د- التنسيق وتوحيد الجهود بين الجهات المختلفة: التشريعية، والقضائية، والضبطية، والفنية، وذلك من اجل سد منافذ جريمة أنتهاك حق الإنسان في أتصالاته الشخصية قدر المستطاع، والعمل على ضبطها واثباتها بالطرق القانونية والفنية.

قائمة المراجع:

اولا– الكتب القانونية:

١. احمد حسام الدين طه تمام: الحماية الجنائية لتكنولوجيا الاتصالات. دراسة مقارنة، ط٢، دار النهضة العربية، القاهرة، ٢٠٠٢.

٢. احمد حسام طه: الجرائم الناشئة عن الحاسب الآلي، دار النهضة العربية، القاهرة، ٢٠٠٠.

٣. أحمد كيلان عبد الله / بلال عبد الرحمن محمود: سياسة أستبدال الصفة الجنائية للعقوبة، دراسة مقارنة، المركز العربي للنشر والتوزيع، مصر، ٢٠١٩.

٤. احمد، طارق عفيفي: الجرائم الالكترونية، جرائم الهاتف المحمول، دراسة مقارنة بين القانون المصري والاماراتي والنظام السعودي المركز القومي للاصدارات القانونية، مصر ٢٠١٤.

٥. ايمن عبدالله فكري: جرائم نظم المعلومات، دراسة مقارنة، دار الجامعة الجديدة للنشر، الاسكندرية، ٢٠٠٧.

٦. جلال محمد الزعبي واحمد محمد المناعسة: جرائم تقنية المعلومات الالكترونية، ط١، دار الثقافة للنشر والتوزيع، عمان، ٢٠١٠.

٧. حسن الغافري: السياسة الجنائية في مواجهة جرائم الانترنيت، دار النهضة العربية، القاهرة، ٢٠٠٩.

٨. حنان ريحان المضحكي: الجرائم المعلوماتية "دراسة مقارنة"، ط١، منشورات الحلبي الحقوقية، بيروت، ٢٠١٤.

٩. خالد ممدوح ابراهيم: حوكمة الانترنيت، ط١، دار الفكر الجامعي، الاسكندرية، ٢٠١١.

١٠. سالم روضان الموسوي: جرائم القذف والسب عبر القنوات الفضائية، ط١، منشورات الحلبي الحقوقية، بيروت، ٢٠١٢.

١١. سامي علي حامد عياد: الجريمة المعلوماتية وجرائم الانترنيت، دار الفكر الجامعي، الاسكندرية، ٢٠٠٧.

١٢. سحر محمد نجيب، التنظيم الدستوري لضمانات حقوق الانسان وحرياته، مطابع شتات، مصر، ٢٠١١ص٣٣.

١٣. سليم عبد الله الجبوري: الحماية القانونية لمعلومات شبكة الانترنيت، ط١، منشورات الحلبي الحقوقية، ٢٠١١.

١٤. صالح جواد كاظم، ملاحظات حول مفهوم علوية حقوق الانسان، مباحث في القانون الدولي، دار الشؤون الثقافية العامة، بغداد، ط١، ١٩٩١.

١٥. طارق الدسوقي عطية: الأمن المعلوماتي، " النظام القانوني للحماية المعلوماتية"، دار الجامعة الجديدة، الاسكندرية، ٢٠١٠.

١٦. عثمان خليل عثمان، المبادئ الدستورية العامة، مكتبة عبدالله وهبة، ١٩٩٩.

١٧. علواني هليل فرج ، التحقيق الجنائي والتصرف فيه، دار المطبوعات الجامعية، الإسكندرية، ٢٠٠٦.

١٨. علي يوسف، الشكري، حقوق الانسان بين النص والتطبيق، دار صفاء للنشر، عمان ط١، ٢٠١١.

١٩. عمر محمد يونس: المجتمع المعلوماتي والحكومة الالكترونية، الطبعة الاولى، الأبحاث، موسوعة التشريعات العربية ٢٠٠٣، دار الفكر الجامعي، الاسكندرية، ٢٠٠٣.

٢٠. محمد عبيد الكعبي: الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت، الطبعة الثانية، دار النهضة العربية، ٢٠٠٩.

٢١. محمد علي السالم عياد الحلبي، ضمانات الحرية الشخصية أثناء التحري والاستدلال في القانون المقارن، بلا دار نشر وطبعة، ١٩٨١.

٢٢. نبيل عبد المنعم جاد: جرائم الحاسب الآلي، مؤتمر المواجهة الامنية للجرائم المعلوماتية، دبي، الامارات العربية المتحدة، ٢٠٠٠.

٢٣. نغم حمد الشأوي/ بلال عبد الرحمن محمود المشهداني: ابحاث في القانون الجنائي، مكتبة القانون المقارن، ط١، بغداد، ٢٠٢٠.

٢٤. ياسر الأمير، فاروق، مراقبة الأحاديث الخاصة في الإجراءات الجنائية، الطبعة الأولى، دار المطبوعات، الجامعية، الإسكندرية، ٢٠٠٩.

ثانيا– الرسائل والاطاريح الجامعية

١. سـليم عبد الله الناصـر ، الحماية القانونية لمعلومات شـبكة المعلومات (الانترنت) ،رسـالة دكتوراه ، جامعة النهرين ، كلية الحقوق ، ٢٠٠١ .

٢. وسن حميد، رشيد، الرقابة على دستورية القوانين في العراق والامارات العربية المتحدة، رسالة ماجستير مقدمة الى اكاديمية الدراسات العليا، طرابلس، ليبيا٢٠٠٩.

٣. يوسـف صـغير: الجريمة المرتكبة عبر الانترنت، رسـالة ماجسـتير، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، الجزائر، ٢٠١٣.

ثالثا– البحوث والدوريات

١. رمسيس بهنام، نطاق الحق في الحياة الخاصة – بحث مقدم لمؤتمر الحق في الحياة الخاصة المنعقد بكلية الحقوق – جامعة الاسكندرية في الفترة من ٤–٦ يونيه، ١٩٨٧.

٢. فاتن ليث الربيعي ، في مجتمع المعلومات المفتوحة حرب ساخنة ضد قراصنة المعلومات ، مقال نشر في جريدة الجمهورية ، ع٨٠٥٥ ، س٢٥ ، ٥ك١ ، ١٩٩١ .

٣. ممدوح خليل بحر ، الحماية القانونية لبرامج الكمبيوتر واثرها في الامن القومي العربي، بغداد : مجلة الامن العام ، ع ١ ، س ١٢ ، ١٩٩٢.

رابعا– الدساتير والقوانين:

١. دستور المصري الصادر عام ٢٠١٤

٢. دستور جمهورية العراق لعام ٢٠٠٥

٣. قانون التوقيع الالكتروني والمعاملات الإلكترونية العراقي رقم ٧٨ لسنة ٢٠١٢

٤. قانون العقوبات العراقي المرقم ١١١ لسنة ١٩٦٩ المعدل