Criminal Protection of Electronic Data in Iraqi Law
"A Critical Study of the Adequacy of Penal Provisions"

الحماية الجنائية للبيانات الإلكترونية في القانون العراقي

"دراسة نقدية في كفاية النصوص العقابية"

م.م سيف علي إبراهيم محمد

Saif Ali Ibraheem mohammed

الجامعة التقنية الوسطى/المعهد التقني / بلد

Middle Technical University/Balad Technical Institute

saif-ali@mtu.edu.iq

الملخص

يتناول هذا البحث موضوع الحماية الجنائية للبيانات الإلكترونية في القانون العراقي، حيث أصبح الأفراد بحاجة إلى ضرورة إضفاء الحماية القانونية على بياناتهم الشخصية خصوصاً في ظل التطور العلمي والتكنولوجي وإساءة استخدام المواقع الإلكترونية من خلال اتخاذها وسيلة للتجسس على بيانات ومعلومات الأفراد وإساءة استخدامها وابتزازهم ومساومتهم في هذا المجال، فالحياة الخاصة مصونه بموجب أحكام القانون ولكن ما تتعرض له من انتهاكات جاء بسبب الدخول إلى عالم الإنترنت والتكنولوجيا فهو عالم جديد قد يسيئ الكثير من الأفراد استخدامه سواء الشخص المعتدى عليها أو الشخص المعتدى لذا كان لا بد من معالجة قانونية في هذا المجال تحمي خصوصية الأفراد وتحافظ عليها، وتتضمن الحماية الجنائية للبيانات الإلكترونية في القانون العراقي نصوصاً متفرقة في قانون العقوبات رقم 111 لسنة 1969، وقانون التوقيع الإلكتروني والمعاملات الإلكترونية رقم 78 لسنة 2012، بهدف مكافحة الجرائم المعلوماتية، وحماية الخصوصية، وضمان أمن البيانات من الاختراق أو التزوير، وتركز الحماية على معاقبة الدخول غير المشروع، و التخريب، أو التداول غير القانوني للبيانات.

الكلمات المفتاحية: الحماية، البيانات الإلكترونية، التكنولوجيا، القانون العراقي.

Abstract

This research addresses the topic of criminal protection of electronic data in Iraqi law. Individuals now require legal protection for their personal data, especially in light of scientific and technological advancements and

the misuse of websites. These websites are often used to spy on, misuse, blackmail, and extort individuals' data and information. While privacy is protected by law, violations have arisen due to the advent of the internet and technology. This new world is susceptible to misuse by many, both as victims and perpetrators. Therefore, legal measures are necessary to protect and preserve individual privacy. Criminal protection of electronic data in Iraqi law is addressed in various provisions within the Penal Code No. 111 of 1969 and the Electronic Signature and Electronic Transactions Law No. 78 of 2012. These provisions aim to combat cybercrime, protect privacy, and ensure data security against hacking and forgery. The focus of this protection is on penalizing unauthorized access, tampering, and the illegal handling of data.

Keywords: Protection, Electronic Data, Technology, Iraqi Law

المقدمة:

يمثل الأمن الركيزة الأساسية للمجتمع، حيث لا يتصور تحقيق نمو أي نشاط لدوائر الدولة بعيداً عن تحققه، سواء أكان ذلك على المستوى التقني أم على المستوى القانوني، إلا أن الوجوه المتعددة لسياسة أمن المعلومات وآثارها 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، وما يزال الاهتمام بالفرد قائماً ومستمراً خاصة أمام التطورات العلمية والابتكارات التكنولوجية المتسارعة والإقبال المتعاظم على استخدام شبكة الإنترنت وتقنيات الحاسب الآلي فهو وسيلة لتخزين المعلومات من قبل المؤسسات والأفراد، وقيام جهات عديدة بجمع بيانات ومعلومات عن الأفراد لممارسة عملها، كالمصارف وشركات التأمين وشركات الاتصالات والاشتراك بالمواقع الإلكترونية، ومنتديات النقاش والشبكات الاجتماعية المختلفة وحتى لدى إبرام الشخص لعقود الشراء عبر الإنترنت حيث يضطر لتقديم بعض البيانات الخاصة به التي قد يتم استغلالها من قبل البعض لأغراض تجارية تسويقية أو حتى لأغراض غير مشروعة، وقد ظهرت سياسة حماية البيانات الإلكترونية كأحد نتائج هذا التطور التكنولوجي المتسارع، حيث انتشرت هذه الأنظمة بسرعة كبيرة مدفوعة بعدة عوامل منها الحاجة لتوفير المعلومات الملائمة والموثوقة والتي تساعد أجهزة 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 دائماً جرائم مرتبطة بالبيانات، لأن هذا قائم على فكرة البيانات وتحويلها من ملموسة وورقية إلى افتراضية غير

ورقية، وتتعدد وتتنوع صور جرائم البيانات الإلكترونية التي ظهرت في عصر التحول الرقمي، فهل هناك تشريع خاص بحماية هذه البيانات الإلكترونية؟ أم أن نصوص القانون الجنائي العراقي كفيلة بحمايتها؟

أهمية البحث:

أسهم التقدم العلمي والتكنولوجي في توسيع نطاق تداول البيانات والمعلومات الشخصية من خلال شبكات الاتصال الحديثة، الأمر الذي أدى إلى سهولة جمعها ومعالجتها وتبادلها عبر الفضاء الإلكتروني. وتشمل هذه البيانات معلومات ذات طابع شخصي تمس الجوانب المختلفة لحياة الفرد، كالتاريخ الشخصي والمهني والصحي والاجتماعي، بما يجعلها مرتبطة بشكل مباشر بخصوصية الشخص، ونتيجة لذلك، قد تتعرض هذه البيانات إلى صور متعددة من الاعتداء، مثل انتهاك الخصوصية أو استغلالها في التشهير أو الابتزاز، وهو ما يشكل خطراً حقيقياً على الأفراد. ومن هنا، اتجهت الدول إلى سن تشريعات تكفل حماية البيانات الشخصية، من خلال توفير الحماية القانونية لها، سواء على المستوى المدني أو الجنائي، بما يضمن الحفاظ على سريتها ومنع الاعتداء عليها، ومعاقبة كل من يتجاوز عليها بغير وجه حق[1]. ولذلك يمكننا القول بأن التطور التكنولوجي أدي إلى تهديد حرمة الحياة الخاصة، فلم يعد التستر والكتمان و الأسوار العالية قادر على حماية البيانات من التطفل والوصول إليها[(2)] ، فقد مكن التطور التكنولوجي من المساس بتلك الخصوصية وذلك من خلال القدرة على القيام بجمع وتخزين واسترجاع ونقل ومعالجة هذه البيانات و المعطيات المتعلقة بالأفراد، فقد تم تطوير أجهزة و معدات سهلت التجسس على خصوصية الأفراد ورصد حركاتهم وسكناتهم[(3)] ، لذلك فلابد من التصدي للثغرات والمشاكل القانونية الناتجة عن الممارسة العلمية لحماية حق الخصوصية في البيانات الإلكترونية ، حتى نستطيع حماية المعلومات والبيانات من الانتهاكات لابد من قوانين خاصة تحمي البيانات والمعلومات الشخصية وتقيد وتشكل أنشطة الشركات والحكومات والأفراد، وتكون بمثابة قيود رادعة أو بتنظيم واعي لاحترام الحياة الخاصة للأفراد . ومن هذا المنطلق تتمحور أهمية هذا البحث في التعرف على مدى أهمية البيانات الإلكترونية وآلية حمايتها جنائيا، حيث تتعرض البيانات إلى أنواعٍ عديدة من الاعتداء كالإتلاف والاستيلاء أو الجمع غير المشروع لها، وخطورة استغلال هذه البيانات بصوره غير مشروعة باستخدام خوارزميات الذكاء الاصطناعي لتفلتر اهتمامات وميول أصحاب تلك البيانات، ولذلك نسلط الضوء على إمكانية تطبيق النصوص الجنائية التقليدية

---

[1] سويلم، خالد سويلم محمد، (2022)، الحماية القانونية للبيانات الشخصية الإلكترونية - دراسة مقارنة، المجلة القانونية، المجلد 14، العدد6، ص 1886.

[(2)] - جدي، صبرينة، الحماية القانونية للحق في الخصوصية المعلوماتية، مجلة التواصل في الاقتصاد والادارة والقانون، المجلد الرابع والعشرون، العدد الثاني، ص 124 .

[(3)] انظر: جعفر، علي، (2013)، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة- دراسة مقارنة، منشورات زين الحقوقية، بيروت، ص405 -409 .

على هذه الجرائم ومعرفة نقاط القصور في التشريع العراقي والنصوص الإجرائية التي تتصدى للجرائم الإلكترونية.

• **إشكالية البحث:**

تُعد تكنولوجيا المعلومات الحديثة نتاجًا لاندماج نظم المعلومات مع نظم الاتصال، وما أسفر عنه ذلك من تطور في شبكات الاتصال وتبادل البيانات، الأمر الذي أدى إلى اتساع نطاق التعامل بالبيانات الإلكترونية بمختلف صورها. وفي ظل هذا التطور، برزت مسألة حماية البيانات، ولا سيما البيانات الشخصية، كأحد أهم الحقوق المرتبطة بحماية الخصوصية في البيئة الرقمية. إذ تُعرف البيانات الشخصية بأنها جميع المعلومات المتعلقة بشخص معين، سواء تعلقت بحياته الخاصة أو المهنية، متى ما أمكن تحديد هويته من خلالها ضمن نطاق الفضاء الإلكتروني. وقد أدى التحول الرقمي إلى اتساع نطاق الاعتداءات التي قد تمس حرمة الحياة الخاصة، مما استدعى ضرورة توفير حماية قانونية فعالة، لاسيما من الجانب الجنائي، لمواجهة صور الانتهاك التي تطال البيانات الإلكترونية للأفراد. ومن هنا تبرز أهمية تحديد ماهية البيانات التي تستحق الحماية، سواء كانت بيانات موضوعية كاسم الشخص وموطنه وحالته المدنية ووظيفته، أم بيانات ذات طابع شخصي أو تقييمي تعكس آراءً أو معلومات عن الغير، إذ إن كلا النوعين قد يمس بشكل مباشر خصوصية الأفراد داخل مجتمع المعلومات. وعليه[1].

في ظل التحول المتسارع لتكنولوجيا المعلومات والاتصالات، والتي أصبحت تمس مختلف جوانب الحياة وتشكل ركيزة أساسية للتطور والتنمية، برزت تحديات جديدة تمثلت في ظهور أنماط مستحدثة من الجرائم، ارتكبها أشخاص ذوو نوايا إجرامية يستهدفون البيانات والمعلومات الإلكترونية بقصد الاستيلاء عليها أو استغلالها بطرق غير مشروعة. وقد تنوعت هذه الجرائم لتشمل الدخول غير المشروع إلى الأنظمة المعلوماتية، والتعدي على سلامة أنظمة الدولة، وإعاقة عمل الشبكات الإلكترونية أو تعطيلها، فضلًا عن جرائم سرقة واختلاس البيانات الإلكترونية، ولا سيما تلك المتعلقة بمؤسسات الدولة، ومع تزايد هذه الجرائم وتطور أساليبها، برزت إشكالية قانونية مهمة تتمثل في غياب تشريع عراقي خاص ومتكامل لمكافحة الجرائم الإلكترونية، الأمر الذي أدى إلى اتساع نطاق هذه الجرائم بشكل قد يفوق قدرة النصوص القانونية النافذة على مواكبتها. وعلى الرغم من أن المشرع العراقي في قانون العقوبات رقم (111) لسنة 1969 قد اتسم بالمرونة وسعة الأفق في صياغة بعض نصوصه، مما أتاح إمكانية تطبيقها على بعض الجرائم المستحدثة، بما فيها الجرائم الإلكترونية، إلا أن ذلك لا

[1] الزيدي، كاظم عبد جاسم، (2022)، الحماية القانونية للبيانات الشخصية في القانون العراقي، https://dcc-iq.com/?p=41826

يغني عن الحاجة إلى نصوص عقابية صريحة ومتخصصة تتلاءم مع طبيعة هذه الجرائم وتعقيداتها التقنية[1]، وبناء على ذلك تتمثل مشكلة البحث في مدى كفاية النصوص العقابية في القانون العراقي في توفير الحماية الجنائية اللازمة لهذه البيانات، وقدرتها على مواكبة التطورات التقنية المتسارعة، الأمر الذي يستدعي دراسة نقدية لتحليل أوجه القصور التشريعي، وبيان مدى فاعلية الحماية المقررة في مواجهة الجرائم الواقعة على البيانات الإلكترونية.

أسئلة البحث:

السؤال الرئيسي: ما مدى فاعلية النصوص العقابية في توفير الحماية الجنائية للبيانات الإلكترونية في القانون العراقي؟

ويتفرع منها التالي:

1. ماهية البيانات الإلكترونية ومظاهر الاعتداء عليها؟
2. موقف التشريعات المختلفة والتشريع العراقي من الحماية الجناية للبيانات الالكترونية؟
3. ما مدى فعالية النصوص العقابية الحالية في مواجهة الاعتداءات على البيانات الإلكترونية؟

أهداف الدراسة:

يهدف البحث لتسليط الضوء حول مدى الحماية الجنائية للبيانات الإلكترونية في القانون العراقي بالإضافة للتعرف على مدى كفاية النصوص العقابية في العراق في توفير هذه الحماية، وحتى يتحقق هدف البحث يتم التعرف على:

1. التعرف على مفهوم البيانات الإلكترونية ومظاهر الاعتداء عليها.
2. موقف التشريعات المختلفة والتشريع العراقي من الحماية الجناية للبيانات الالكترونية؟

الدراسات السابقة.

دراسة (حيدر طالب محمد علي، 2025) بعنوان الحماية القانونية لحقوق الافراد وحرياتهم عند تجميع بياناتهم في الاجهزة الالكترونية، بحث منشور في مجلة كلية الحقوق جامعة النهرين، فقد هدف البحث إلى التعرف على طبيعة الحماية القانونية المتعلقة بحقوق الافراد وحرياتهم عند تجميع بياناتهم في الاجهزة الالكترونية، وتوصل البحث شهدت البيئة العراقية في السنوات الأخيرة توجهًا متزايدًا نحو الانفتاح على العالم الخارجي، رافقه توسع ملحوظ في استخدام الأجهزة والتقنيات الإلكترونية في إدارة شؤون الدولة ومؤسساتها، وذلك في ظل ظروف أمنية وإدارية فرضت الاعتماد المتنامي على الوسائل الرقمية. وقد أسهم هذا التحول في زيادة حجم البيانات

[1] القاضي: خليل، أريج، (2023)، جريمة سرقة واختلاس البيانات الإلكترونية للدولة، جمهورية العراق، مجلس القضاء الأعلى. https://www.sjc.iq/view.71508/

المتداولة إلكترونيًا، ولا سيما البيانات ذات الطابع الشخصي، الأمر الذي جعلها عرضة لمخاطر الاختراق أو سوء الاستخدام أو الاستغلال غير المشروع، ولذلك أوصي البحث بضرورة تدخل المشرّع العراقي بشكل أكثر فاعلية لتنظيم هذا المجال، من خلال وضع إطار قانوني متكامل يوفر الحماية اللازمة للبيانات الإلكترونية، على غرار ما اتجهت إليه بعض التشريعات المقارنة التي أولت عناية خاصة بحماية البيانات الشخصية. ويهدف هذا التوجه إلى تحقيق التوازن بين متطلبات التطور التكنولوجي وضمان حماية الحقوق والحريات الفردية، ولا سيما الحق في الخصوصية.

دراسة (الشعيبي،عبد القاسم مثني، 2024) الحماية الجناية للبيانات الشخصية في عصر التحول الرقمي في ضوء القانون الإماراتي رقم (45) لسنة 2021بشأن حماية البيانات الشخصية، اتبع الباحث في دراسة هذا الموضوع المنهج الوصفي التحليلي، هدف الوصول إلى نتائج علمية دقيقة تسهم في بيان مدى كفاية الحماية الجنائية للبيانات الإلكترونية في القانون الإماراتي، وتوصلت الدراسة إن التطور التكنولوجي والتقني في العصر الحديث شكل عاملًا رئيسيًا في تعريض البيانات الشخصية لمخاطر متزايدة، إذ أصبح انتهاك الحق في الخصوصية أكثر سهولة من أي وقت مضى. الأمر الذي يستدعي ضرورة مواكبة هذا التطور من خلال تبني مواجهة تشريعية مستمرة، إلى جانب اعتماد وسائل تقنية حديثة، كبرامج الحماية، التي تكفل صون حق الإنسان في الخصوصية، وتُعد كل معلومة تتعلق بشخص معين بياناتٍ شخصية تخضع للحماية القانونية، متى كان هذا الشخص محدد الهوية أو قابلاً للتحديد بصورة مباشرة أو غير مباشرة، وهو ما يوسع من نطاق الحماية ليشمل مختلف صور البيانات المرتبطة بالأفراد في البيئة الرقمية، يوصي الباحث المشرّع الإماراتي بضرورة تضمين قانون حماية البيانات الشخصية نصوصًا صريحة تُجرّم الأفعال التي تمس هذه البيانات، مع تقرير العقوبات المناسبة لها، وعدم الاكتفاء بالجزاءات الإدارية فقط، كما يوصي الباحث المشرّع العُماني بتعديل المادة (31) من قانون حماية البيانات الشخصية، وذلك بالنص على وجوبية المصادرة في الجرائم المتعلقة بالاعتداء على البيانات الشخصية، بما يعزز من فاعلية الحماية القانونية[1].

دراسة (خالد سويلم محمد، 2022) بعنوان الحماية القانونية للبيانات الشخصية الإلكترونية - دراسة مقارنة، هدفت هذه الدراسة إلى التعرف على طبيعة الحماية الخاصة بالبيانات الشخصية الإلكترونية التي توفرها التشريعات المختلفة، وقد توصلت النتائج أن الجهود الدولية ساهمت في سن القوانين الوطنية لضمان الحماية القانونية للبيانات الشخصية الإلكترونية بما قدمته من دور رائد وسباق وضاغط في هذا المجال، وكان ذلك نتاج الإيمان بقيمة الحق في الخصوصية المعلوماتية، تترتب المسئولية القانونية على أي مساس بتلك البيانات اعتداء

[1] الشعيبي، عبد القاسم مثني، (2024)، الحماية الجناية للبيانات الشخصية في عصر التحول الرقمي في ضوء القانون الإماراتي رقم (45) لسنة 2021بشأن حماية البيانات الشخصية، مؤتمر التحديات القانونية في العصر الرقمي، المؤتمر العلمي الثامن لكلية الحقوق ، جامعة السلطان قابوس.

على خصوصية أصحابها، ويستحق المخالف الجزاء الجنائي المترتب على مخالفة الالتزام قانون يتعلق بذلك ويسأل مدنياً عن الأضرار الناجمة عن ذلك الاعتداء، ومن ثم يلتزم بتعويض المضرور من جراء ذلك، ولذلك توصي الدراسة بضرورة التوعية المستمرة بأهمية الحماية القانونية للبيانات الشخصية الإلكترونية باعتبارها من تطبيقات الحق في الخصوصية.

دراسة(خميسي، 2019) بعنوان الضمانات القانونية في حماية البيانات الشخصية في الفضاء الرقمي، هدفت الدراسة إلى التعرف على أهم الضمانات الشخصية التي يقرها القانون من أجل حماية الأشخاص الطبيعيين في ظل تطبيق والاعتماد على تقنيات الفضاء الرقمي، وقد توصلت الدراسة إلى ضرورة القيام بمعالجة البيانات الشخصية بطريقة تكون مشروعة ونزيهة بما يساهم ذلك في احترام الحياة الخاصة للأفراد، والحفاظ على سريتها من أي تعديات أو اختراقات على خصوصية تلك البيانات، واستعمالها بطرق غير مشروعة، كما توصلت الدراسة إلى ضرورة إيجاد ضمانات لاستعمال هذه البيانات في الأغراض التي جُمعت لأجلها وذلك في أطار نصوص ومواد القانون، وبموافقة صريحة من أصحابها[1].

يتضح من عرض الدراسات السابقة أنها ركزت على بيان أهمية الحماية القانونية للبيانات الشخصية في ظل التطور التكنولوجي المتسارع، حيث تناولت دراسة (حيدر علي، 2025) واقع البيئة العراقية والحاجة إلى إطار قانوني متكامل لحماية البيانات الإلكترونية، في حين ركزت دراسة (الشعيبي، 2024) على الحماية الجنائية في التشريع الإماراتي، مع إبراز ضرورة تطوير النصوص العقابية لمواكبة التحديات الرقمية، أما دراسة (خالد سويلم ، 2022) فقد اتجهت إلى الطابع المقارن، مؤكدة على دور الجهود الدولية في تعزيز الحماية القانونية وربطها بالحق في الخصوصية.وعلى الرغم من أهمية هذه الدراسات، إلا أنها لم تتناول بشكل مباشر ومفصل مدى كفاية النصوص العقابية في القانون العراقي في مواجهة الجرائم الواقعة على البيانات الإلكترونية، وهو ما يميز البحث الحالي، إذ يركز على تقديم دراسة نقدية تحليلية للنصوص الجنائية العراقية، بهدف الكشف عن أوجه القصور التشريعي وبيان مدى قدرتها على تحقيق الحماية الفعالة في ظل التطورات التقنية الحديثة.

منهج البحث:

أصبحت قضية أمن وحماية البيانات والمعلومات في ظل تطبيق تقنية الفضاء الإلكتروني من أهم قضايا العصر، لذا يتم تسليط الضوء على دور التشريعات الدولية في حماية الحق في خصوصية البيانات الإلكترونية في ظل تطبيق تقنيات الفضاء الإلكتروني، ولذلك نعتمد على المنهج الوصفي التحليلي المقارن والذي يركز على جمع البيانات والمعلومات المتعلقة بموضوع بحثنا، للوقوف على معرفة تامة عن دور القانون الجنائي العراقي

[1] حميسي، رضا، (2019)، الضمانات القانونية في حماية البيانات الشخصية في الفضاء الرقمي، المؤتمر الدولي الثالث للقانون والعدالة، كلية الشريعة والقانون، المجلد الأول، إصدار خاص .

والقوانين المقارنة في حماية البيانات الإلكترونية. مع إجراء مقارنة دولية بين التشريعات الدولية في العراق ومصر وقطر

المبحث الأول: ماهية البيانات الإلكترونية ومظاهر الاعتداء عليها

تعد البيانات الإلكترونية من المصطلحات الحديثة نسبيًا، وقد ارتبط ظهوره بتطور أوعية المعلومات في مؤسسات المعلومات التقليدية كالمكتبات والأرشيفات. ومع التحول إلى البيئة الرقمية، أصبح استخدام البيانات الإلكترونية أكثر ارتباطًا بالمكتبات الرقمية، والأرشيفات الإلكترونية، والمستودعات الرقمية، حيث تؤدي دوراً مهماً في تنظيم المحتوى الرقمي وبنائه وإتاحته واسترجاعه عبر شبكة الإنترنت. ولذلك فينظر له أنها "بيانات تصف البيانات"، أي مجموعة من المعلومات الوصفية المرتبطة بالمحتوى الإلكتروني أو الرقمي على الشبكة الدولية للمعلومات (الإنترنت)، والتي تهدف إلى تسهيل عملية الوصول إلى هذا المحتوى، واستخدامه بكفاءة، واسترجاعه في أقصر وقت ممكن[1]. ونظراً إلى التطور الهائل والانتشار السريع لشبكات الإنترنت، ازدادت أهمية قضية أمن البيانات الإلكترونية، وقد عمل الفقه القانوني على التمييز بين نوعين من البيانات بيانات عامة وخاصة [(2)]، وسنتطرق في هذا المبحث إلى بيان مفهوم البيانات الإلكترونية ومظاهر الاعتداء عليها على النحو التالي

المطلب الأول: مفهوم البيانات الإلكترونية

أصبح الإعتماد على التكنولوجيا الحديثة في الحياة الاجتماعية سمة من سمات العصر، يتفاعل المستخدمون بشكل يومي مع هذه التقنيات، عن طريقها يتم تبادل البيانات والمعلومات الشخصية على نطاق واسع، وبسرعة فائقة عبر المنصات المختلفة، مما جعل هذه البيانات متاحة للغير وسهولة الوصول إليها[(3)] ، بدون أذن مسبق من صاحب هذه البيانات، حيث يثير ذلك العديد من المخاوف حول خصوصية بيانات الأفراد المتاحة على هذه التقنيات[(4)] ، حيث أن ذلك يعرض هذه البيانات لسوء الاستغلال من قبل مخترقي هذه المنصات، عن طريق بيع هذه المعلومات، أو ابتزاز أصحابها بهدف تحقيق منافع شخصية، وعوائد مادية وبالتالي تطلب الأمر حماية خصوصية البيانات والمعلومات الشخصية للأفراد .

---

[1] الخضر، أبو بكر سلطان محمد، وكروم، عفاف مصطفي حامد، (2021)، وصف البيانات الرقمية بمواقع مصادر الوصول الحر للمعلومات على الإنترنت – دراسة تقويمية، المجلة لعربية للمعلوماتية وآمن المعلومات، مج2، ع4، ص65.

[(2)] رستم، هشام فريد (1993)، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة لآلات الحديثة، ص18.

[(3)] - مشعل، محمد أحمد سلامة، (2017)، الحق في محو البيانات الشخصية دراسة تحليلية في ضوء لائحة حماية البيانات بالاتحاد الأوروبي GDPR واحكام المحاكم الأوروبية، مجلة الدراسات القانونية والاقتصادية، المجلد الثالث، العدد الثاني، ص 12 .

[(4)] - المعداوي، محمد احمد، مرجع سابق ذكره، ص 6 .

الفرع الأول: تعريف البيانات الإلكترونية.

أولاً: معني البيانات في اللغة.

البيانات لغةً مصدر من الفعل بين، أي ظهر، وأتضح، وأفصح، ومنه قوله تعالى: "علمه البيان"[1]. وكذلك تعني عبارة عن الأشياء، والحقائق المعروفة يقيناً، والتي يمكن عن طريقها الوصول إلى نتيجة معينة [2].

ثانياً: معني البيانات في الفقه.

وتعددت التعريفات الفقهية بشأن البيانات الإلكترونية، فعرفها البعض بأنها تعبير عن مجموعة من الأرقام والكلمات والرموز أو الحقائق أو الإحصاءات الخام التي تُنشأ أو تُخزن أو تُعالج بوسائل إلكترونية، والتي لا تكون بينها علاقة مترابطة في صورتها الأولية، ولم تخضع بعد لعمليات التفسير أو المعالجة أو التنظيم، ولذلك فهي غالبًا ما تخلو من معنى ظاهر أو دلالة محددة ما لم يتم تحليلها وتحويلها إلى معلومات قابلة للاستخدام . ويُستفاد من هذا التعريف أن البيانات الإلكترونية تمثل المادة الخام للنظام المعلوماتي، إذ تتحول من مجرد مدخلات رقمية غير مفسَّرة إلى معلومات ذات قيمة عند إخضاعها لعمليات المعالجة والتحليل، مما يمنحها دلالة ومعنى يمكن الاستفادة منهما في اتخاذ القرارات أو في إدارة الأنشطة المختلفة."[3]. كما عرّفها آخرون بأنها مجموعة من الصور أو الرموز أو الحقائق أو المفاهيم أو التعليمات التي يمكن أن تكون محلًا للتبادل والاتصال أو التفسير والتحليل والمعالجة، سواء تم ذلك من قبل الأفراد أو عبر الأنظمة الإلكترونية المختلفة. ويُفهم من هذا التعريف أن البيانات الإلكترونية لا تقتصر على الأرقام أو النصوص فقط، بل تشمل كل ما يمكن ترميزه وتداوله في بيئة رقمية. "[4].

وذهب جانبٌ آخر إلى تعريفها بأنها تعبير أو صياغة تُخصَّص بقصد نقل رسالة قابلة للتداول، وقد تتمثل في علامة أو رمز يتم اختياره وتوجيهه ليحمل مضمونًا معينًا إلى الغير. وبذلك فإن البيانات أو المعلومات تُعد قابلة للنقل والتحويل من وسيط إلى آخر، سواء بوسائل تقليدية أو إلكترونية.كما تُعرَّف بأنها نشاط أو عملية قادرة على نقل الوقائع والمعاني إلى الأفراد، بحيث تُمكّنهم من الفهم والإدراك واتخاذ القرار. ومن منظور اقتصادي،

---

(1) سورة الرحمن، الآية رقم (4).

(2) الشاذلي، فتوح، وعفيفي، كامل عفيفي (2003)، جرائم الكومبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون دراسة مقارنة، منشورات الحملي الحقوقية، لبنان، ص 29.

(3) الزعبي، جلال محمد (2010)، وأحمد محمد المناعسة، جرائم تقنية المعلومات الإلكترونية، ط 1، دار الثقافة للنشر والتوزيع، عمان، ص 100.

(4) عبد الله، أحمد كيلاني، ومحمود، بلال عبد الرحمن (92019)، سياسة استبدال الصفة الجنائية للعقوبة، دراسة مقارنة، المركز العربي للنشر والتوزيع، مصر، ص 55.

تُعد المعلومات شكلًا من أشكال القيمة، إذ تكتسب أهميتها بحسب ما تحمله من منفعة وما يوليه لها الأفراد من ثقة واقتناع، وهو ما يجعلها موردًا ذا طبيعة استراتيجية في البيئة الرقمية المعاصرة "[1].

الفرع الثاني: التعريف البيانات الإلكترونية في القانون العراقي والقوانين المقارنة

فقد ورد مفهوم البيانات الإلكترونية في القانون المصري رقم 175 لسنة 2018 في مادته الأولي بأنها" هي كل ما يمكن إنشاؤه أو تخزينه، أو معالجته أو تخليقه، أو نقله، أو مشاركته، أو نسخه بواسطة تقنية المعلومات؛ كالأرقام والأكواد والشفرات والحروف والرموز والإشارات والصور والأصوات، وما في حكمها[2].

وفي القانون القطري فقد تم تحديد معني البيانات الإلكترونية بموجب ما ورد في قانون رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية، في مادته الأولي على أن البيانات والمعلومات الإلكترونية هي كل ما يمكن تخزينه أو معالجته أو إنشاؤه أو نقله باستخدام وسيلة تقنية المعلومات، وبوجه خاص الكتابة أو الصور أو الصوت أو الأرقام أو الحروف أو الرموز أو الإشارات وغيرها[3].

كما عرف المشرع العراقي في قانون التوقيع الإلكتروني والمعاملات الإلكترونية رقم (78) لسنة 2012 المعلومات على أنها " عبارة عن بيانات ونصوص وصور وأشكال وأصوات ورموز التي يتم إنشاؤها، أو دمجها أو تخزينها، أو معالجتها، أو إرسالها، أو تسليمها عن طريق الوسائل الإلكترونية"[4].

أما عن البيانات الإلكترونية فلم يضع المشرع العراقي مفهوما للبيانات الإلكترونية الا انه كفل حمايتها في العديد من النصوص منها المادة (37) من دستور جمهورية العراق لعام 2005 التي اشارة ان حرية الفرد العراقي وكرامته مصونة كما نصّت المادة (17) من الدستور على كفالة الحق في الخصوصية الشخصية للفرد العراقي، بما لا يتعارض مع حقوق الآخرين أو الآداب العامة. ويُعد هذا النص تأكيدًا دستوريًا على حماية الحياة الخاصة وصونها من أي اعتداء أو تدخل غير مشروع. وكذلك جاءت المادة (40) من الدستور ذاته لتؤكد أن حرية الاتصالات والمراسلات البريدية والهاتفية والإلكترونية وغيرها من وسائل التواصل مكفولة، ولا يجوز مراقبتها أو التنصت عليها أو الكشف عنها إلا لضرورة قانونية أو أمنية، وبموجب قرار قضائي يصدر وفقًا لأحكام القانون.

---

[1] الجبوري، سليم عبد الله (2011)، الحماية القانونية لمعلومات شبكة الانترنيت ط 1، منشورات الحلبي الحقوقية، ص 35.

[2] القانون المصري رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات

[3] القانون القطري رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية

[4] مادة (1) (ثالثاً) قانون التوقيع الإلكتروني والمعاملات الإلكترونية رقم (78) لسنة 2012 من يقصد بالمصطلحات التالية: ثالثاً: "لأغراض هذا القانون المعاني المبينة ازاؤها البيانات والنصوص والصور والاشكال والاصوات والرموز وما شابهه ذلك التي تنشأ أو تدمج أو تخزن او تعالج أو ترسل أو تستلم بوسائل إلكترونية".

ويُبرز هذا التنظيم الدستوري مدى حرص المشرّع على تحقيق التوازن بين حماية الخصوصية الفردية ومتطلبات الأمن والنظام العام.[1]

يتضح من استعراض التعريفات القانونية للبيانات الإلكترونية في التشريعات المقارنة، ولا سيما القانون المصري والقطري، أنها اتجهت إلى تبني مفهوم واسع وشامل للبيانات الإلكترونية، حيث لم تقتصر على نوع معين من المعلومات، بل شملت كل ما يمكن إنشاؤه أو معالجته أو تخزينه أو نقله باستخدام تقنيات المعلومات، بما في ذلك النصوص والأرقام والصور والأصوات والرموز وغيرها. ويعكس هذا التوجه حرص المشرّعين على مواكبة التطور التقني وتعدد صور البيانات في البيئة الرقمية. وفي المقابل، يُلاحظ أن المشرّع العراقي لم يضع تعريفًا صريحًا ومباشرًا للبيانات الإلكترونية، وإنما اكتفى بالإشارة إلى مفهوم المعلومات في قانون التوقيع الإلكتروني والمعاملات الإلكترونية، مع الإقرار بحماية دستورية غير مباشرة للبيانات من خلال النصوص المتعلقة بحماية حرمة الحياة الخاصة، وحرية الاتصالات والمراسلات.

الفرع الثالث: خصائص البيانات الإلكترونية

1. **نوع المعلومة:** لا ريب أن المعلومات تتباين فيما بينها حسب نوعها، والأهمية التي تكون عليها، وقد تكون المعلومة معرفة، أو رسم هندسي، وقد تكون عبارة عن أوامر وإرشادات معينه، وقد تتعلق بالأمور المالية، أو قد تكون بالخلاف من ذلك يطغى عليها الطابع الفني أو الأدبي[2].
2. **الصورة التي توجد عليها المعلومات:** تتخذ المعلومات صورًا وأشكالًا متعددة، فقد تكون مشفّرة أو غير مشفّرة، كما قد تكون مسموعة أو مقروءة أو مخزّنة في وسائط رقمية مختلفة. وغالبًا ما تتحدد قيمة المعلومات وأهميتها بالهيئة التي توجد عليها، إذ إن طريقة عرضها أو حمايتها تؤثر في درجة سريتها وإمكانية الاستفادة منها.وفي حالة المعلومات المشفّرة، قد يؤدي تغيير حرف واحد أو جزء بسيط من محتواها إلى اختلاف جوهري في معناها مقارنة بالمعلومات غير المشفّرة، بل قد يفضي ذلك إلى إفسادها أو تحريف مضمونها أو كشف سريتها. ومن ثمّ فإن أي تعديل غير مشروع على المعلومات، سواء بالحذف أو الإضافة أو التحوير، يُعد اعتداءً عليها، ويُشكل جريمة يعاقب عليها القانون، لما يترتب عليه من أضرار تمس سلامة البيانات وخصوصيتها وأمنها.
3. **طريقة كتابة المعلومة:** الطريقة التي تكتب بها المعلومة هي التي تحدد الشكل الخاص بها، ويقصد بالشكل في مجال تكنولوجيا المعلومات يعني الشكل طريقة كتابة المعلومة عن طريق جهاز الحاسب الآلي[3].

---

[1] المادة 40 من دستور العراق الدائم لعام 2005. كاظم، صالح جواد (1991)، ملاحظات حول مفهوم علوية حقوق الإنسان مباحث في القانون الدولي، دار الشؤون الثقافية العامة، بغداد، ط1، ص87.

[2] هشام فريد رستم، مرجع سابق، ص 18.

[3] الشعبي، عبد الغني قاسم مثني، الحماية الجنائية للبيانات الشخصية في عصر التحول الرقمي في ضوء القانون الإماراتي رقم 45 لسنة 2021 بشأن حماية البيانات الشخصية، مؤتمر التحديات القانونية في العصر الرقمي، المؤتمر العلمي الثامن لكلية الحقوق، جامعة السلطان قابوس 2024، ص 149.

4. وسائط تخزين المعلومات: المعلومات بطبيعتها تتطلب وجود وسط يتم تخزينها فيه، حتى وإن كان ذلك الوسط يتمثل بعقل الإنسان، ووسائل التخزين تختلف فقد تكون حبراً أو لوناً، أو غير ذلك، وينسحب ذلك على جميع المعلومات التي يتم تدوينها، في الوصل الإلكتروني، أو الأوراق أو الإشارات الخاص به مثل الإشارات الرقمية في جهاز الكمبيوتر، ومما لا شك فيه أن المعلومات تتعرض للخطر في حالة التلاعب الذي يقع على هذا الوسط[1]

5. العمومية: فقد تكون المعلومة عامة يمكن الوصول إليها من قبل الجميع وفي أي وقت كان، فقد تسمح طبيعة المعلومات باطلاع الجميع عليها، أو قد تكون محصورة بفئة معينه من الأفراد.

6. أهمية المعلومات ومصداقيتها: قد تكون المعلومات على قدر من الأهمية والمصداقية، بحيث تهم مجموعة من الأفراد لذا فهم معنيون بها ويستخدمون الطرق المناسبة من أجل الوصول إليه.

المطلب الثاني: مظاهر الاعتداء على البيانات الإلكترونية

تتعدد وتتنوع صور الاعتداء على البيانات الإلكترونية، ويرجع ذلك إلى التطور العلمي والتكنولوجي، فكلما تطورت الوسائل التكنولوجية كلما ظهرت أساليب لانتهاك البيانات الإلكترونية، لأن العلم في تطور مستمر، لذا يجب أن يكون التشريع مواكباً لهذا التطور ولتلك الصور من الاعتداءات[2]، وبناءً على ذلك سنقسم هذا المطلب إلى الجرائم المرتكبة ضد سرية البيانات الشخصية في فرع اول، ثم نسرد الجرائم المرتكبة ضد سلامة البيانات في فرع ثاني، وذلك كالتالي:

الفرع الأول: الجرائم المرتكبة ضد سرية البيانات الشخصية

هناك العديد من الأفعال التي من شأن يؤدي إلى انتهاك حرمة سرية البيانات الشخصية والتي تتمثل بما يلي:

أولاً: جريمة الدخول والبقاء غير المشروع: تعني دخول للبيانات عن طريق الغش في المنظومة الخاصة بالمعالجات الآلية، فتنشأ الجريمة بمجرد تحقق فعل الدخول إلى نظام المعلومات، والدخول في هذا المجال يعني جميع الأفعال التي تسمح بالولوج إلى هذا النظام والسيطرة على المعطيات والمعلومات التي يحتويها والدخول في هذا المجال هو عبارة عن ظاهرة معنوية تشابه الدخول إلى فكرة أو مملكة التفكير، الخاصة بالإنسان، أي الدخول إلى العمليات الذهنية الخاصة بنظام المعالجات الآلية[3].

---

[1] مجيد، سوز حميد، الحماية القانونية للحق في خصوصية البيانات الشخصية في العراق، دراسة تحليلية مقارنة، مجلة دراسات قانونية وسياسية، العدد11، السنة 6، 2018، ص 171.

[2] حزام فتحية، الضمانات القانونية لمعالجة المعطيات ذات الطابع الشخصي، دراسة على ضوء القانون رقم 18-07، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد 8، عدد 4، السنة 2019، ص 292.

[3] قارة، آمال (2007)، الحماية الجزائية للمعلوماتية في التشريع الجزائري، ط 2، دار دومة، للطباعة والنشر والتوزيع، الجزائر، ص 100.

فيحدث الدخول بشكل مباشر من خلال استخدام أحد الأجهزة الخاصة بالإخراج لجهاز الكمبيوتر، كالشاشة، أو الطابعة، وقد يتم الدخول بصورة غير مباشرة كما هو الحال بالنسبة للدخول غير المصرح به لشبكات الاتصال والمعالجة التي تتم عن بعد، الذي يتم من خلال التقاط المعلومات المتواجدة في النظام المعلوماتي[1].

وبالنسبة لفعل البقاء فيقصد به تواجد المعتدي داخل النظام الخاص بالمعالجة الآلية ضد إرادة المسيطر على هذا النظام، وقد يتم هذا الفعل بصورة مستقلة عن الفعل الخاص بالدخول إلى النظام وقد يجتمعان في آن واحد.

ويتمثل الركن المادي لهذه الجريمة بالبقاء غير المشروع وغير المصرح به داخل النظام المعلوماتي سواء أتم ذلك عن طريق الخطأ، أو بالصدفة، والحد الفاصل بين مشروعية الفعل من عدمها، يتمثل بقطع الاتصال، فقد يتواجد الشخص في النظام المعلوماتي، ولكنه يرجع عن هذا التواجد فلا جرمة في هذه الحالة، أما إذا قرر التواجد وقطع الاتصال فيكون مرتكباً لفعل جرمي يحاسب عليه القانون[2].

ثانياً: جريمة جمع أو معالجة بيانات شخصية بدون ترخيص: تقع هذه الجريمة عندما يتولى الشخص القائم على معالجة البيانات الشخصية بممارسة الأنشطة الخاصة بالمعالجة في الأحوال غير المرخص له فيها بذلك بموجب أحكام القانون، وكذلك يشكل الفعل الخاص بالمعالجة جريمة في حالة المعالجة إلغاء الترخيص، أو انتهاء مدته لعدم وجود مبرر قانوني يسمح بالبقاء والمعالجة للبيانات[3].

ثالثاً: جريمة الانحراف عن الغرض أو الغاية: تتمثل هذه الجريمة بانحراف المعالج للبيانات عن الغرض أو الغاية من المعالجة، سواء من ناحية التسجيل، أو التصنيف، أو النقل، فكل فعل يخالف الغرض من المعالجة الإلكترونية هو جريمة يحاسب عليها القانون[4].

الفرع الثاني: الجرائم المرتكبة ضد سلامة البيانات الشخصية

أولاً: جريمة الحفظ غير مشروع للبيانات الشخصية: يتم السلوك الاجرامي في هذه الجريمة عبر الاحتفاظ بالبيانات الشخصية لمدة أكثر من المدة التي سبق طلبها أو التي تضمنها الإخطار المسبق، بحيث تتم

---

(1) محمود، مروان محمود صالح، الحماية الجنائية للبيانات الشخصية الإلكترونية، مجلة كلية القانون للعلوم القانونية والسياسية، المجلد 14، العدد 52، 2025، ص 291.

(2) أيوب، بولين أنطونيوس (2009)، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، دراسة مقارنة، ط 1، منشورات الحلبي الحقوقية، لبنان، ص 414.

(3) نعيم، مغبغب (2006)، حماية برامج الكمبيوتر الأساليب والثغرات، دراسة في القانون المقارن، ط1، منشورات الحلبي الحقوقية، بيروت، لبنان، ص 201.

(4) الرزازي، محمد عطية محمد علي (2013)، الحماية القانونية لقواعد البيانات في القانون المصري والتشريعات المقارنة، دار الجامعة الجديدة، الإسكندرية، مصر، ص 49.

المعالجة في وقت أكثر مما هو مخصص له، وهنا تظهر أهمية المدة الزمنية الخاصة بحفظ البيانات والمعلومات ومعالجتها، وحق الشخص المعني بمحو البيانات الخاصة به بعد انتهاء الغاية من التخزين لعدم وجود مبرر للاحتفاظ بها لأن ذلك يشكل انتهاك لحق الإنسان في المحافظة على خصوصياته[1].

وهذه الجريمة من الجرائم العمدية، فلا يوجد مبرر للاحتفاظ بالبيانات بعد معالجتها إلا لغرض غير مشروع، بشرط توافر العلم لدى الجاني بأن ما يقوم به يشكل جريمة يحاسب عليها القانون، وأنه تسبب بالحاق الضرر بالغير[2].

ثانياً: جريمة التلاعب بالبيانات الشخصية: تتكون هذه الجريمة من عدة عناصر يمكن تفصيلها فيما يلي:

1. **الإدخال:** يعني به ان يقوم الجاني بإضافة معطيات جديده على الدعامة التي تتضمن المعلومات والمعالجة لها، ويتحقق هذا الفعل من خلال إضافة فايروسات مثل حصان طروادة، ليعمل على إضافة معطيات جديدة.
2. **المحو:** أي محو جزء من البيانات والمعطيات الموجودة على الدعامة، أو نقل جزء منها على المنطقة الخاصة بالذاكرة، أو تحطيم الدعامة.
3. **التعديل:** هو عبارة عن التغيير الذي يحدثه الجاني في البيانات والمعطيات داخل نظام المعالجة الآلية للمعطيات، أي استبدالها بمعطيات أخرى، ويستخدم الجاني من أجل الوصول إلى النتيجة الجرمية وتحقيق الهدف الذي يسعى إليه برامج خاصة[3].

الفرع الثالث: الجرائم المرتكبة ضد توافر البيانات الشخصية وإساءة استخدامها

أي الجرائم التي تستهدف تعطيل الوصول إلى البيانات الشخصية أو منع استخدامها بشكل مشروع، أو استغلالها بطرق غير قانونية، مثل حجب البيانات أو حذفها أو تعطيل الأنظمة التي تتيح الوصول إليها، أو استخدامها في غير الأغراض المصرح بها. ويُعد هذا النوع من الجرائم من أخطر صور الاعتداء، لما له من تأثير مباشر على حقوق الأفراد والمؤسسات، وإعاقة سير العمل في الأنظمة الإلكترونية. ويُعد هذا النوع من الجرائم من أخطر صور الاعتداء، لما له من تأثير مباشر على حقوق الأفراد والمؤسسات، وإعاقة سير العمل في الأنظمة الإلكترونية. كما قد يؤدي إلى خسائر مادية ومعنوية جسيمة، خاصة إذا تعلّق الأمر ببيانات حيوية أو حساسة، مثل البيانات الصحية أو المالية أو الإدارية، التي يعتمد عليها الأفراد والجهات في اتخاذ قراراتهم.، وتتخذ هذه

---

[1] طه، صابرين ناجي، دور القانون الجنائي في حماية البيانات الرقمية، مجلة النهرين للعلوم القانونية، العدد3، المجلد 26، 2024، ص 230.

[2] الموسوي، منى تركي، الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة عليها، مركز بحوث السوق وحماية المستهلك، جامعة بغداد، مجلة كلية بغداد للعلوم الاقتصادية، العدد الخاص بمؤتمر الكلية، 2013، ص 20.

[3] عفيفي، أحمد طارق (2014)، الجرائم الإلكترونية، جرائم الهاتف المحمول، دراسة مقارنة بين القانون المصري والإماراتي والنظام السعودي المركز القومي للإصدارات القانونية، مصر، ص70.

الجرائم صورًا متعددة، من أبرزها الهجمات الإلكترونية التي تستهدف تعطيل الأنظمة أو حجب الخدمات، مثل هجمات حجب الخدمة(Denial of Service) ، أو إتلاف البيانات أو حذفها بشكل متعمد، أو تشفيرها ومنع أصحابها من الوصول إليها، فضلًا عن إساءة استخدام البيانات من قبل الجهات المخوّلة بمعالجتها، من خلال تجاوز الأغراض المحددة لاستخدامها أو إفشائها دون سند قانوني.

كما تتجلى خطورة هذه الأفعال في أنها لا تقتصر على الإضرار بالفرد فحسب، بل قد تمتد آثارها إلى المساس بالأمن المعلوماتي للدولة ومؤسساتها، خاصة في حال استهداف قواعد البيانات الحكومية أو البنى التحتية الرقمية. ومن هنا، تبرز أهمية إقرار حماية جنائية فعالة تجرّم هذه الأفعال وتضع لها عقوبات رادعة، بما يضمن الحفاظ على توافر البيانات وسلامتها، ويعزز الثقة في البيئة الرقمية.

المبحث الثاني: موقف التشريعات المختلفة من حماية البيانات الالكترونية

تُعد الحماية الجنائية من الوسائل التي يكفلها القانون الجنائي بقسميه: قانون العقوبات وقانون أصول المحاكمات الجزائية، حيث يتم من خلالها تقرير جزاءات على الأفعال التي تشكل اعتداءً على مختلف المصالح المحمية قانونًا، ومنها المعلومات والبيانات، وذلك عند وقوع أي سلوك غير مشروع يلحق الضرر بها. ويقوم التجريم أساسًا على حماية المصالح الجديرة بالحماية، إذ يحدد المشرّع الأفعال التي تستحق العقاب بالنص عليها في القانون، بحيث يدور النص القانوني وجودًا وعدمًا مع المصلحة التي يسعى إلى حمايتها، ويتغير نطاق الحماية تبعًا لمدى توافر علة التجريم. وفي هذا الإطار، يمكن التمييز بين نوعين من الحماية الجنائية[1]:

أولًا: الحماية الجنائية الموضوعية: وينظمها قانون العقوبات، وتتمثل في تجريم الأفعال التي تمس المصلحة محل الحماية، كحماية المعلومات والبيانات من الاعتداء عليها، وذلك من خلال النصوص القانونية التي تضفي صفة عدم المشروعية على الأفعال الضارة، سواء وردت في القوانين العقابية العامة أو في القوانين الخاصة ذات الصلة.

ثانيًا: الحماية الجنائية الإجرائية: وتنظمها قواعد قانون أصول المحاكمات الجزائية، وتهدف إلى بيان الإجراءات الواجب اتباعها في مرحلة التحقيق والمحاكمة وصدور الأحكام وطرق الطعن وتنفيذ العقوبات، إضافة إلى تنظيم تشكيل المحاكم وتحديد اختصاصاتها. وتشمل هذه الحماية أيضًا القوانين والإجراءات التي نص عليها المشرّع لحماية المعلومات، ومنها ما ورد في قانون قوى الأمن الداخلي، بما يضمن سلامة الإجراءات وتحقيق العدالة الجنائية.

---

[1] محمود، سيد أحمد، (2024)، حماية البيانات الشخصية الرقمية وفقًا لأحكام القانون المصري رقم 151 لسنة 2020 (حماية البيانات الشخصية المعالجة الكترونياً)، مجلة العلوم القانونية والاقتصادية، ع1، السنة 66، ص 1442.

المطلب الأول: موقف التشريعات المقارنة من الحماية الجنائية للبيانات الإلكترونية.

حرصت مختلف التشريعات على تجريم المساس بالبيانات الشخصية، حيث يعتبر ذلك جريمة مخالفة للقانون توجب معاقبة مرتكبها،

الفرع الأول: موقف المشرّع القطري من حماية البيانات الإلكترونية

أولى المشرّع القطري اهتمامًا واضحًا بحماية البيانات الشخصية في البيئة الرقمية، حيث عرّف البيانات الشخصية في المادة (1) من القانون رقم (13) لسنة 2016 بشأن حماية خصوصية البيانات الشخصية بأنها: "بيانات عن الفرد الذي تكون هويته محددة أو يمكن تحديدها بصورة معقولة، سواء من خلال هذه البيانات أو عن طريق الجمع بينها وبين أية بيانات أخرى". كما عرّف معالجة البيانات الشخصية بأنها مجموعة العمليات التي تُجرى على البيانات، مثل الجمع والتسجيل والتنظيم والتخزين والاسترجاع والاستخدام والإفشاء والنقل والحجب والمحو وغيرها من صور المعالجة[1].

وقد وسّع المشرّع نطاق الحماية من خلال النص في المادة (16) من ذات القانون على فئات خاصة من البيانات الشخصية ذات الطبيعة الحساسة، مثل البيانات المتعلقة بالأصل العرقي، والصحة، والحالة الجسدية أو النفسية، والمعتقدات الدينية، والعلاقة الزوجية، والبيانات الجنائية، مع منح الوزير المختص صلاحية إضافة فئات أخرى إذا كان من شأن سوء استخدامها إلحاق ضرر جسيم بالفرد. كما اشترط القانون عدم جواز معالجة هذه البيانات إلا بعد الحصول على تصريح مسبق، وفقًا للضوابط والإجراءات المحددة، مع إمكانية فرض احتياطات إضافية لتعزيز حمايتها[2].

ومن الجانب الجنائي، أكد المشرّع القطري على حماية الحق في الخصوصية من خلال نص المادة (333) من قانون العقوبات المعدل بالقانون رقم (4) لسنة 2017، حيث جرم الاعتداء على حرمة الحياة الخاصة للأفراد بغير رضاهم، ومن ذلك تسجيل أو نقل المحادثات التي تتم في مكان خاص باستخدام أي وسيلة تقنية، وهو ما يشمل الوسائل الإلكترونية الحديثة، ويعكس توجه المشرّع إلى تجريم الأفعال التي تمس البيانات والمعلومات الشخصية في صورتها الرقمية وقد نصت المادة على " يعاقب بالحبس مدة لا تجاوز سنتين وبالغرامة المالية التي لا تزيد على (10000) عشرة آلاف ريال، أو بإحدى هاتين العقوبتين، كل من اعتدى على حرمة الحياة الخاصة الأفراد، بغير رضائهم في غير الأحوال المصرح بها قانونا وذلك بارتكاب أحد الأفعال الآتية : ... 3 .سجل أو نقل، محادثات جرت في مكان خاص، عن طريق جهاز أيا كان نوعه [(3)] .. بالإضافة إلى نص المادة 371عقوبات القطري يجرم الدخول غير المشروع إلى نظام المعالجة الآلية للبيانات المحفوظة في الحاسب الآلي سواء كان ذلك عن

---

[1] أنظر المادة الأولى من القانون القطري بشأن حماية خصوصية البيانات الشخصية رقم 13 لسنة 2016

[2] أنظر المادة 16ا من القانون القطري بشأن حماية خصوصية البيانات الشخصية رقم 13 لسنة 2016

[(3)] المادة 333 من قانون العقوبات القطري رقم 11 لسنة 2004، المعدلة بالقانون رقم 4 لسنة 2017، الصادر في 9 مارس 2017 .

طريق التحايل أو كان بدون وجه حق، ن قانون العقوبات على "انه يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة المالية التي لا تزيد على عشرة آلف ريال، أو بإحدى هاتين العقوبتين[1]

وبذلك يتضح أن المشرّع القطري قد تبنى نهجًا مزدوجًا في حماية البيانات الإلكترونية، يجمع بين الحماية التشريعية المدنية/الإدارية والحماية الجنائية، بما يعزز من صيانة الخصوصية ومواجهة الاعتداءات الواقعة على البيانات الشخصية في البيئة الرقمية.

الفرع الثاني: موقف المشرّع المصري في توفير الحماية الجنائية للبيانات الإلكترونية

يهدف قانون حماية البيانات الشخصية المصري رقم (151) لسنة 2020، ولا سيما المواد (7) و(44)، إلى وضع إطار قانوني شامل يوفر للمستخدم حماية بياناته التي تخضع للمعالجة الإلكترونية. ويكفل القانون عدة حقوق أساسية للمستخدم، منها الحق في معرفة طبيعة البيانات التي يمتلكها، وحقوق الحائز على البيانات والمعالج لها، كما يمنح الحق في تقديم الشكاوى ضد المخالفين ومقاضاتهم عند الضرورة. ويخاطب القانون أيضًا الشركات والمؤسسات التجارية التي تتعامل مع قواعد البيانات الخاصة بالمستخدمين، ويحدد المعايير التي تنظم العلاقة بين المستخدمين وهذه الشركات الرقمية. ومن أجل تنفيذ أحكام القانون بشكل فعال، نص القانون على إنشاء مركز لحماية البيانات الرقمية تكون مهامه الرقابة على تنفيذ القانون، وإصدار التراخيص والتصاريح للشركات التي تقوم بمعالجة البيانات الشخصية، وتقديم الإرشادات اللازمة لضمان الالتزام بأحكامه. ويُعد هذا التوجه مهمًا ومرحبًا به، إذ يواكب التطور التكنولوجي المتسارع ويعزز حماية البيانات الشخصية في الحياة العامة والخاصة[2].

وفقًا لنص المادة (57) من الدستور المصري لسنة 2014، فإن للحياة الخاصة حرمة، وهي مصونة لا تُمس. كما تُعد المراسلات البريدية والبرقية والإلكترونية، والمحادثات الهاتفية، وغيرها من وسائل الاتصال، ذات حرمة، وسريتها مكفولة، ولا يجوز مصادرتها أو الاطلاع عليها أو رقابتها إلا بأمر قضائي مُسبب ولمدة محددة، وفي الأحوال التي يبينها القانون[3]. وبناء على ذلك فيعد نص المادة (57) من الدستور المصري لسنة 2014 من الركائز الدستورية الأساسية التي أرست مبدأ حماية الخصوصية، حيث أكد بشكل صريح على حرمة الحياة الخاصة وسرية وسائل الاتصال بمختلف صورها، بما في ذلك الوسائل الإلكترونية الحديثة. ويُفهم من هذا النص أن

---

[1] اللمعي، ياسر محمد، مرجع سابق ذكره، ص 159

[2] محمود، سيد أحمد، (2024)، حماية البيانات الشخصية الرقمية وفقاً لأحكام القانون المصري رقم 151 لسنة 2020 (حماية البيانات الشخصية المعالجة الكترونياً)، مجلة العلوم القانونية والاقتصادية، ع1، السنة 66، ص 1442.

[3] صالح، سلمي محسن حسن، (2023)، جهود منظمات مكافحة الجريمة المعلوماتية في تحقيق الأمن السيبراني، مجلة دراسات في الخدمة الاجتماعية، العدد 63، الجزء الثالث، ص 815.

المشرّع الدستوري قد تبنى مفهومًا واسعًا للخصوصية، يمتد ليشمل البيانات والمعلومات المتداولة عبر البيئة الرقمية، وهو ما يُشكل أساسًا دستوريًا لحماية البيانات الإلكترونية

الفرع الثالث: دور المشرّع الجزائري في توفير الحماية الجنائية للبيانات الإلكترونية.

اعترفت غالبية التشريعات، إن لم يكن جميعها، بالحق في حماية الخصوصية باعتباره حقًا أصيلًا من حقوق الإنسان، وقد كفل المشرّع الجزائري هذا الحق من خلال إقراره وحمايته للأفراد. وفي هذا السياق، عبّر عن الأنظمة المعلوماتية بمصطلح "منظومة المعالجة الآلية للمعطيات"، إلا أن قانون العقوبات الجزائري لم يتضمن نصوصًا صريحة تتعلق بحماية البيانات الشخصية، وإنما تناول صورًا غير مباشرة للحماية من خلال تجريم بعض الأفعال المرتبطة بالاعتداء على الأنظمة المعلوماتية[1]

ومن بين هذه الأفعال، جريمة الولوج غير المصرح به إلى نظام معلوماتي، حيث يُقصد بها كل نشاط يتم عمدًا ودون إذن من صاحب النظام، بما يتيح للجاني إمكانية الاتصال بالنظام أو التحكم فيه بشكل كلي أو جزئي، الأمر الذي قد يؤدي إلى الوصول إلى البيانات المخزنة داخله واستغلالها بطرق غير مشروعة. وقد أولى المشرّع الجزائري اهتمامًا بهذه المخاطر، من خلال تجريم الأفعال التي تستهدف الأنظمة المعلوماتية وما تتضمنه من بيانات ذات طابع شخصي، وذلك بالنص عليها في المادة (394 مكرر) من قانون العقوبات[2]. وبموجب هذا النص، عُدّ الدخول عن طريق الغش إلى منظومة المعالجة الآلية للمعطيات جريمة يعاقب عليها القانون، حيث تقررت لها عقوبات تتراوح بين الحبس والغرامة المالية، كما شدد المشرّع العقوبة في حال ارتكاب أفعال إضافية مثل إدخال أو تعديل أو حذف المعطيات بطرق غير مشروعة. ويُظهر ذلك توجه المشرّع الجزائري نحو إضفاء الحماية الجنائية على البيانات الإلكترونية من خلال تجريم الأفعال التي تمس سلامة الأنظمة والمعطيات المرتبطة بها. كما لم يقتصر المشرّع الجزائري على قانون العقوبات، بل عزز هذه الحماية من خلال إصدار تشريعات خاصة، مثل القانون رقم (04-09) المتعلق بالقواعد الخاصة بتكنولوجيا الإعلام والاتصال، والقانون رقم (18-05) المتعلق بالتجارة الإلكترونية، والتي أسهمت في تنظيم استخدام البيانات وحمايتها في البيئة الرقمية، بما يعكس سعي المشرّع إلى مواكبة التطورات التقنية وتوفير حماية جنائية فعالة للبيانات الإلكترونية.[3]

---

[1] مباركية، مفيدة،(2018)،الحماية الجنائية للحق في الخصوصية الرقمية في القانون الجزائري، مجلة كلية الشريعة والاقتصاد، العدد السابع، الاصدار الأول، ص 470 .

[2] المادة رقم 394 من قانون 2004 المعدل

[3] معزوز، دليلة، (2021)، حماية المعطيات الشخصية في البيئة الافتراضية في التشريع الجزائري: الواقع والتحديات، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد العاشر، العدد الأول، ص 135 .

المطلب الثاني: موقف التشريع العراقي من الحماية الجنائية للبيانات الإلكترونية.

وهذا ما دأب عليه المشرع العراقي، حيث أولى هذا البيانات أهمية كبيرة وجرم المساس بها وذلك بموجب احكام دستور سنه 2005 النافذ، حيث أعطى الفرد الحق في خصوصيته بشرط عدم تعارض ذلك مع حقوق الآخرين والآداب العامة، بالإضافة إلى كفالته لحرمة المسكن حيث أكد على عدم جواز دخولها وتفتيشها إلا بموجب قرار قضائي، فذلك يعد مبرراً لدخول المساكن وتفتيشها دون الحصول على إذن من أصحابها باعتبارها ضرورة قانونية لا تحتمل الحصول على إذن أو موافقات رسمية من أجل الدخول إلى المنازل [1].

فقد أكد المشرع العراقي على سرية المراسلات الشخصية وعدم جواز انتهاكها، إلا للضرورة القانونية أو بموجب قرار قضائي، وقد كان الأجدر به أن يسن تشريع خاص بحماية البيانات الشخصية فهو وإن وفر الحماية لها بموجب احكام الدستور إلا أنها حماية غير مباشرة باعتبارها إحدى صور الحق في الخصوصية [2].

وعلى صعيد قانون العقوبات العراقي المرقم 111 لسنة 1969 المعدل حيث نصت المادة (328) 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"[3]، كما نصت المادة (438) على أن "يعاقب بالحبس مدة لا تزيد على سنة وبغرامة أو بإحدى هاتين العقوبتين، كل من نشر بإحدى طرق العلانية أخباراً أو صوراً أو تعليقات تتصل بأسرار الحياة الخاصة أو العائلية أو الإفراد، ولو كانت صحيحة، إذا كان من شأنها الإساءة إليهم، ومن اطلع من غير من ذكروا في المادة (328) من قانون العقوبات العراقي على رسالة أو برقية أو مكالمة هاتفية، فأفشاها لغير من وجهت إليه إذا كان من شأن ذلك إلحاق الضرر بأحد".

ويتضح مما سبق ان المشرع العراقي حمّى البيانات الإلكترونية في العديد من نصوص الدستور العراقي، وكذلك الحال في مواد قانون العقوبات العراقي الذي وأن كان تشريعه في عام 1969 أي قبل اختراع الشبكة المعلوماتية، فهو تضمن عددا من النصوص التقليدية التي يمكن تطويعها في إطار حماية البيانات الرقمية عن طريق التفسير الواسع لتلك النصوص، ويجب سن تشريع قانون مكافحة الجرائم المعلوماتية وسد الفراغ التشريعي بخصوص تلك الجرائم المستحدثة ضد البيانات الإلكترونية [4].

---

[1] نصت المادة (17) أولً و(ثانياً) من دستور جمهورية العراق النافذ لسنة 2005 على ما يلي:

أولاً: لكل فرد الحق في الخصوصية الشخصية بما لا يتنافى مع حقوق الآخرين الآداب العامة.

ثانياً: حرمة المساكن مصونة ولا يجوز دخولها أو تفتيشها أو التعرض لها إلا بقرار قضائي ووفقاً للقانون.

[2] رمضان، مدحت عبد الحليم (2000)، جرائم الاعتداء على الأشخاص والإنترنيت، دار النهضة العربية القاهرة، ط 1، ص 39.

[3] المادة 328 من قانون العقوبات العراقي رقم 111 لسنة 1969.

[4] عياد، سامي علي حامد (2007)، الجريمة المعلوماتية وجرائم الانترنيت، دار الفكر الجامعي، الاسكندرية، ص 66.

الفرع الأول: الأساليب غير التقليدية في حماية البيانات الرقمية

ينبغي وجود نظام كفء لإدارة المعلومات وأمن المعلومات والاتصالات ويشمل ذلك:

أ. يقتضي تطبيق إجراءات أمن المعلومات وأمن الاتصالات اعتماد مجموعة من التدابير الأساسية، من أبرزها ما يأتي[1]:

1. تبني سياسة أمنية واضحة ومرنة تواكب التطورات التقنية والمخاطر المستجدة.
2. تحديد المسؤوليات والصلاحيات بدقة، منعًا لشيوع المسؤولية، مع إلزام جميع المستويات الإدارية بالتقيد بالنظام المعتمد.
3. توفير وسائل فنية آلية لرصد وتسجيل محاولات الاختراق غير الناجحة، مع توثيق تاريخ ووقت حدوثها وتحديد الوحدة الطرفية التي تمت من خلالها، بما يتيح تعقب الفاعل.
4. تحليل ومراجعة جميع محاولات الاختراق الفاشلة واتخاذ الإجراءات اللازمة لتعزيز حماية النظام وسد الثغرات.
5. تشفير وترميز المعلومات والبيانات الحساسة لضمان سريتها وحمايتها من الوصول غير المصرح به.
6. تغيير مفاتيح التشفير بصورة دورية وغير منتظمة للحد من احتمالات اختراقها أو إساءة استخدامها.
7. إسناد مسؤولية إدارة مفاتيح التشفير إلى شخصين وفق نظام ثنائي، منعًا لانفراد شخص واحد بالتحكم بها وضمان تعزيز الرقابة والأمان.
8. فصل خطوط الاتصالات غير الضرورية عن نظم الحاسبات والمعلومات للحد من فرص الدخول غير المصرح به.
9. قصر تداول المعلومات والبيانات المشفرة والحساسة على عدد محدد ومعلوم من الأشخاص المرخص لهم، وفي الحدود اللازمة لأداء مهامهم.
10. حصر توزيع المعلومات على الأفراد أو الأقسام التي تستلزم طبيعة عملها الاطلاع عليها، دون تجاوز ذلك إلى جهات لا تقتضي وظائفها هذا الاطلاع.
11. حفظ البيانات ضمن بنك معلومات أو قاعدة بيانات محددة تتوافر لها وسائل الحماية المناسبة لضمان سلامتها وسريتها.
12. اعتماد نظام متعدد الطبقات لتحديد مستويات الولوج أو الدخول إلى النظم، بحيث تُمنح الصلاحيات وفقًا لطبيعة المهام والمسؤوليات.

ب- الوسائل الفنية لتوفير أمن المعلومات والاتصالات، ومنها على سبيل المثال[2]:

---

[1] الغافري، حسن (2009)، السياسة الجنائية في مواجهة جرائم الانترنيت، دار النهضة العربية، القاهرة، ص 65.

[2] المضحكي، حنان ريحان (2014)، الجرائم المعلوماتية "دراسة مقارنة"، ط 1، منشورات الحلبي الحقوقية، بيروت، ص 34.

1. اعتماد تقنية التوقيع الرقمي أو الإلكتروني في المراسلات الإلكترونية للتحقق من هوية مُنشئ المستند ومرسله وضمان نسبته إليه.
2. الاستعانة بخدمات التحقق والتصديق الإلكتروني المقدمة من جهات مختصة، كهيئات البريد أو الدوائر المرخص لها، بهدف التأكد من هوية أطراف التعامل في التجارة والعلاقات التعاقدية الإلكترونية.
3. استخدام تقنيات العلامات المائية أو الأختام الإلكترونية الخاصة على الوثائق الإلكترونية لضمان سلامتها وحمايتها من التزوير أو التعديل غير المشروع.

الفرع الثاني: تقييم الكفاية التشريعية في ضوء الو اقع العملي

في العصر الرقمي، ساهمت تكنولوجيا الاتصالات بشكل كبير في تعزيز قدرة الحكومات والمؤسسات والأفراد على مراقبة واعتراض الاتصالات وجمع البيانات. وقد تبين أن فعالية الدولة في تنفيذ عمليات المراقبة لم تعد مقيدة من حيث النطاق أو المدة الزمنية، بل تمتلك الدول الآن إمكانيات أكبر من أي وقت مضى لتنفيذ عمليات مراقبة متزامنة، شديدة التدخل، وموجهة بدقة، على نطاق واسع. (1).

في التشريع العراقي، نصّ قانون العقوبات رقم (11) لسنة 1969 في المادة (363) على تجريم الاعتداء على وسائل الاتصال السلكي واللاسلكي، إلا أن هذا النص جاء بصيغة عامة ولم يتناول الجرائم الحاسوبية بصورة مباشرة أو تفصيلية. كما صدر القانون رقم (31) لسنة 2013 الخاص بتصديق الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، في إطار تعزيز التعاون الإقليمي في هذا المجال. كذلك صدر قانون التوقيع الإلكتروني والمعاملات الإلكترونية رقم (78) لسنة 2012 لتنظيم التعاملات الإلكترونية وإضفاء الحجية القانونية على التوقيع والمستندات الإلكترونية.

أولاً: قصور النصوص على استيعاب التطور التقني لحماية البيانات الإلكترونية في التشريع العراقي

لم يشير المشرع العراقي إلى حماية البيانات الشخصية بموجب أحكام القانون الأساسي لعام 1925، وكذلك الحال بالنسبة لدستور عام 1958 وهو أول دستور للجمهورية العراقية بعد تحول العراق من الحكم الملكي إلى الجمهوري، وكذلك دستور عام 964، بل أشارت هذه الدساتير بصورة غير مباشرة لحرمة الحياة الخاصة[2].

أما بالنسبة لدستور سنه 2005 النافذ فقد أعطى الحق للأشخاص بالتمتع بحرمة حياتهم الخاصة، بشرط عدم منافاة ذلك مع النظام العام والآداب العامة[3].

---

(1) المضحكي حنان ريحان، مرجع سابق، ص 76.

(2) التميمي، قيس لطيف (2019)، شرح قانون العقوبات العراقي رقم 111 لسنة 1969 بقسميه العام والخاص معززا بالقرارات التميزية دار النهضة العربية، بيروت، ص 128.

(3) نصت المادة (17) أولاً و(ثانياً) من دستور جمهورية العراق النافذ لسنة 2005 على ما يلي:

وما يمكن ملاحظته على نص المشرع الدستوري العراقي أنه وإن وفر حماية قانونية للبيانات الشخصية إلا أنها بصورة غير مباشر، فقد جاءت بصورة غير مباشرة باعتباره جزء من الحق بالخصوصية، وذلك بخلاف العديد من الدساتير العربية التي نصت بشكل مباشر على حماية حرمة المراسلات والاتصالات .

وكذلك عمل المشرع العراقي على توفير الحماية القانونية لحرمة الحياة الخاصة عن طريق النشر، حيث منع نشر الأخبار أو الصور أو التعليقات الخاصة بأسرار الحياة الخاصة للأفراد أو العائلة، وفرض عقوبة الحبس أو الغرامة على الجاني حتى وإن كانت تلك المعطيات صحيحة، إذا كان من شأن نشرها الإساءة إلى ذوي الشأن، وكذلك الحال بالنسبة للشخص الذي اطلع على الرسائل أو البرقيات، أو المكالمات الهاتفية، وأفشاها لغير الشخص الذي وجهت إليه، إذا كان من شأن ذلك الفعل إلحاق الضرر بأحد[1].

ولم يصدر المشرع العراقي أي تشريع جديد يعالج مواضيع جرائم المعلوماتية إنما اكتفى بالرجوع الى القواعد العامة المنصوص عليها في قانون العقوبات العراقي رقم 111 لسنة 1969 المعدل، وعلى أدق تقدير عدم كفاية هذه النصوص للإحاطة بالجرائم المعلوماتية لأنها جرائم تقنية خاصة ومتشعبة ومتطورة، لذا كان الأحرى على المشرع العراقي سن قانون خاص بجرائم تقنية المعلومات لما له من أثر في تقليل الاستخدام السيئ للوسائل التقنية.

كما ان بعض الجرائم التقنية لا حدود جغرافية لها كما في حالة نشر موقع إباحي او معلومات مخلة بالآداب العامة او التحريض العام على الفجور وجرائم القرصنة والقذف والتشهير وسرقة الأموال عبر الشبكة المعلوماتية[2].

إن النصوص التقليدية التي أوردها المشرّع العراقي، والتي تُطبّق حاليًا على الجرائم التقنية، لا تُعد كافية لمكافحة هذا النوع من الجرائم، لاسيما أنها تتسم بخصائص خاصة تستوجب معالجة تشريعية متميزة من حيث التجريم والعقاب. فمن ناحية التجريم، توجد بعض صور السلوك التي ينبغي النص عليها صراحةً باعتبارها جزءًا من الركن المادي للجريمة، كما في حالة إعداد برامج مخصّصة لكسر الشفرات، إذ لا يصح اعتبارها مجرد

أولاً: لكل فرد الحق في الخصوصية الشخصية بما لا يتنافى مع حقوق الآخرين الآداب العامة.

ثانياً: حرمة المساكن مصونة ولا يجوز دخولها أو تفتيشها أو التعرض لها إلا بقرار قضائي ووفقاً للقانون.

[1] نصت المادة (4238) من قانون العقوبات العراقي رقم (111) لسنة 1969 المعدل على ما يلي:

يعاقب بالحبس مدة لا تزيد على سنة وبغرامة لا تزيد على مائة دينار أو بإحدى هاتين العقوبتين:

1. من نشر بإحدى طرق العلانية أخباراً أو صوراً أو تعليقات تتصل بأسرار الحياة الخاصة أو العائلية أو للأفراد ولو كانت صحيحة إذا كان من شأن نشرها الإساءة إليهم.
2. من اطلع من غير الذين ذكروا في المادة 328 على رسالة أو برقية أو مكالمة تلفونية فأفشاها لغير من وجهت إليه إذا كان من شأن ذلك الحاق ضرراً بأحد.

[2] البياتي، هلال، الكبيسي، عبد الستار (1999)، عوني الفخري ندوة القانون والحاسوب، سلطة المائدة الحرة رقم (37)، بيت الحكمة، بغداد، ص 23.

أعمال تحضيرية تحتمل أكثر من تفسير، بما يصعّب إثبات القصد الجرمي ويفضي إلى إفلات الجاني من المسؤولية. أما من ناحية العقاب، فإن العقوبات المقررة في القواعد العامة تبدو محدودة الأثر مقارنة بخطورة هذه الأفعال وطبيعتها التقنية المعقدة، والتي لا يُتصور وقوعها على سبيل المصادفة أو العفوية. فضلاً عن ذلك، فإن غياب قانون خاص ينظم الجرائم التقنية يمنح القاضي مساحة واسعة للاجتهاد في تكييف النصوص العامة وتطبيقها، وهو ما قد يمس بمبدأ الشرعية في الجرائم والعقوبات القائم على وضوح النص وتحديده.

وتعتبر الجرائم الماسة بسلامة البيانات الشخصية وسريتها من الجرائم الخطيرة التي تطال الفرد في سمعته، وشرفة واعتباره وتنتهك خصوصيته وتقتحمها بدون استئذان أو مقدمات، وما زاد من سهولة ارتكاب هذه الجريمة انتشار تكنولوجيا الإنترنت وكثرة الحواسيب، وسهولة ربطها على الشبكة العنكبوتية للإنترنت، بالإضافة إلى سهولة الحصول على المعلومات والبيانات الشخصية فجميع هذه الظروف والعوامل سهلت من ارتكاب الجريمة، بالإضافة إلى النظام المعلوماتي الذي يسهل اختراقه والدخول إليه وسرقة المعلومات والبيانات منه، ونقلها من مكان إلى آخر داخل أو خارج الدولة، مما استوجب التدخل التشريعي في هذا المجال باعتبار المشرع الحارس والحامي الحقيقي لحقوق الأفراد في المحافظة على خصوصياتهم، لكي يهنؤوا وينعموا باستخدام مشروع للإنترنت وفي المقابل كبح جماح أي سلوك خارج عن القانون ويتعارض مع النظام العام والآداب العامة، وذلك من خلال تشريع القوانين الخاصة في هذا المجال التي تحدد الفعل الجرمي والعقوبة المناسبة على الجاني.

وتتضمن الحماية الجنائية للبيانات الإلكترونية في القانون العراقي نصوصاً متفرقة في قانون العقوبات رقم 111 لسنة 1969، وقانون التوقيع الإلكتروني والمعاملات الإلكترونية رقم 78 لسنة 2012، بهدف مكافحة الجرائم المعلوماتية، وحماية الخصوصية، وضمان أمن البيانات من الاختراق أو التزوير. تركز الحماية على معاقبة الدخول غير المشروع التخريب، أو التداول غير القانوني للبيانات.

الفرع الثالث: الحلول المقترحة لتعزيز الحماية التشريعية للبيانات الإلكترونية

عمدت معظم الدول إلى إحداث تعديلات تشريعية بهدف حماية الحياة الخاصة للأفراد ومواجهة جميع أشكال وصور الإجرام المعلوماتي وتأكيد حماية الحق في الخصوصية والحيلولة دون الاعتداء عليه أو المساس به نتيجة للتطورات في عالم التقنية، مما يدلل ذلك على أن الحماية الجزائية للبرامج والأجهزة الإلكترونية لها أهميتها في الحفاظ على حياة الأفراد وخصوصياتهم[1]، ولذا فإن التوسع في استخدام أجهزة الحاسب الآلي يستلزم حماية تشريعية فعالة لأسرار الأفراد مع ضرورة النص على تجريم كافة أشكال التجريم التي تمس بسمعة الأفراد أو حرمة الحياة الخاصة.

[1] المضحكي حنان ريحان، مرجع سابق، ص 76.

اولاً- على الصعيد الفني التقني:

1. تتطلب الدعوة إلى إنشاء أجهزة متخصصة للتحقيق في الجرائم السيبرانية والجرائم التي تشمل أدلة إلكترونية اهتمامًا كبيرًا، وذلك بالنظر إلى التحديات التي تبرز جراء العدد المحدود من أفراد الشرطة المتخصصين مقارنةً بالعدد الضخم لمستخدمي الإنترنت. من الضروري أيضًا تفعيل استخدام تقنيات التحليل الجنائي التي تشمل إنشاء نسخ مطابقة للأصل من المعلومات المخزنة والمحذوفة، بالإضافة إلى تطبيق برامج "منع الكتابة" لضمان عدم تعديل المعلومات الأصلية. كما يجب الاعتماد على الخوارزميات لفك تشفير الملفات أو استخدام التوقيعات الرقمية للكشف عن أي تعديلات قد تطرأ على البيانات.

2. ضرورة اتباع القواعد التي تحكم أمن المعلومات من خلال تحديد المعلومات المهمة وتحليل المخاطر والتهديدات وتحليل القابلية للعدوان وتطبيق الإجراءات المضادة ومرحلة التقييم والاهتمام بوجود أنظمة الاستكشافات والاقتحام داخل المنشآت أو المؤسسات من خلال دوائر الحماية وحدة الضبط جهاز الاشارة، وسيلة ارسال جهاز إنذار، إضاءة كافية.

3. الاهتمام بتطبيق أنظمة 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.

4. وجوب 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، وتكوين فريق لمواجهة الجرائم الإلكترونية بداية من المدير ومشغل النظام والمراقب والمراجع والمحقق الجنائي والمستشار الفني وأفراد الحماية، تحديد اختصاص كل عضو بالفريق، واتباع عناصر التدريب للحد من الاختراقات الأمنية.

ثانياً- على الصعيد القانوني:

1. من الضروري تحديد المتطلبات اللازمة للتعامل الدولي وفقاً للأسس التي ينص عليها القانون الدولي، وذلك لأن العديد من التشريعات الجنائية لا تملك الأطر القانونية المناسبة للتعامل مع هذه القضايا. خاصة وأنه في كثير من الأحيان، لا يتطلب الأمر أن تحدث جميع عناصر الجريمة السيبرانية داخل حدود الدولة من أجل تأكيد ولايتها القضائية الإقليمية. بدلاً من ذلك، يمكن تحديد الولاية القضائية بناءً على موقع الأنظمة والبيانات الحاسوبية التي تم استخدامها في ارتكاب الجريمة.

2. 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.

3. يقتضي الأمر سدّ الفراغ التشريعي في مجال مكافحة الجريمة الإلكترونية، من خلال سنّ قانون متكامل يتضمن القواعد الموضوعية والإجرائية على حدّ سواء. وعلى وجه الخصوص، ينبغي النص صراحةً على تجريم الدخول غير المصرح به إلى الحاسبات الآلية وشبكات الاتصال (الإنترنت) والبريد الإلكتروني، وبيان الأفعال المكوِّنة للركن المادي لهذه الجرائم بصورة واضحة ومحددة. كما يتعين اعتبار البرامج والمعلومات أموالًا منقولة ذات قيمة، مع تحديد طبيعتها القانونية، بما يسمح بإخضاع الاعتداءات الواقعة عليها لأحكام التجريم المناسبة. فضلًا عن ذلك، ينبغي الاعتراف بالحجية القانونية للأدلة الرقمية، ومنحها ذات القوة الثبوتية التي تتمتع بها المحررات المقبولة قانونًا كوسيلة من وسائل الإثبات، بما يواكب التطور التقني ويعزز فعالية العدالة الجنائية في مواجهة الجرائم الإلكترونية.

4. يجب على المشرع العراقي التدخل لإصدار قانون لمكافحة الجرائم المعلوماتية، شريطة أن لا يتعارض هذا القانون مع الحقوق والحريات المقررة دستورياً في العراق. ويجب أن يتضمن النصوص التي تسمح للجهات المعنية بالقبض على مرتكبي الجرائم المتعلقة بانتهاك الحق في الخصوصية ومحاكمتهم.

5. ضرورة التنسيق وتوحيد الجهود بين الجهات التشريعية والقضائية، بالإضافة إلى الأجهزة الضبطية والفنية، بهدف سد الثغرات التي قد تتيح ارتكاب جريمة انتهاك الحق في الخصوصية والاتصالات الشخصية. كما يجب العمل على ضبط هذه الجرائم وتوثيقها بالوسائل القانونية والفنية المناسبة.

الخاتمة:

في ختام هذا البحث سنحاول إجمال أهم النتائج التي توصلنا إليها مع عرض أهم التوصيات التي يمكن الاستفادة منها.

أولاً: النتائج:

1. عدم وجود تشريعات خاصة في العديد من الدول تعالج سرية البيانات الشخصية الإلكترونية، كما هو الحال بالنسبة للتشريع العراقي، حيث يعالج هذه الإشكالية من خلال نصوص متفرقة في قانون العقوبات وقانون التوقيع الالكتروني والمعاملات الإلكترونية وغيرها.

2. عدم وجود هيئة مستقلة خاصة بالرقابة والاشراف على تطبيق القانون الخاص بانتهاك حرمة البيانات السرية الإلكترونية.

3. إن جريمة الاعتداء على سرية البيانات الإلكترونية هي جريمة مرنه تتطور بتطور التكنولوجيا واستحداث الوسائل العلمية في هذا المجال.

4. محدودية سياسة أمن المعلومات في الحد من الاختراقات الامنية وذلك لعدة 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.

ثانياً: التوصيات:

1. ندعو المشرع العراقي إلى صدور تشريع قانون خاص بحماية سرية البيانات الإلكترونية كما هو الحال بالنسبة للمشرع المصري والأردني.

2. ضرورة إنشاء هيئة مستقلة تتولى مهمة الرقابة والإشراف على تطبيق القانون والتنسيق مع الجهات المختصة والعمل على وضع السياسة المشتركة لحماية الحق في الخصوصية.

3. اصدار اللوائح والضوابط التي تحدد الأوجه الخاصة للبيانات والجهات الإدارية التي تتعامل مع البيانات الإلكترونية، ويجب أن تتوافق التشريعات الداخلية مع مبادئ وتوجهات المنظمات والاتفاقيات الدولية في مجال حماية الحق في الخصوصية.

4. نوصي المشرّع العراقي بضرورة سدّ الفراغ التشريعي في مجال مكافحة الجريمة الإلكترونية، من خلال إصدار تشريع متكامل يشمل القواعد الموضوعية والإجرائية معًا، وبوجه خاص النص صراحةً على تجريم الدخول غير المصرح به إلى الحاسبات الآلية وشبكات الاتصال (الإنترنت) والبريد الإلكتروني، بما يضمن توفير حماية قانونية فعالة للأنظمة والمعلومات الرقمية.

5. ينبغي على المشرع العراقي التدخل لإصدار قانون خاص بمكافحة الجرائم المعلوماتية، مع الحرص على أن يتوافق هذا القانون مع الحقوق والحريات المنصوص عليها في الدستور العراقي. ويجب أن يتضمن النصوص القانونية التي تمنح الجهات المعنية الصلاحية في القبض على مرتكبي جرائم انتهاك الخصوصية ومحاكمتهم، بما يضمن حماية حقوق الأفراد في هذا المجال.

المصادروالمراجع:

أولاً: القرآن الكريم.

ثانياً: الكتب:

1) التميمي، قيس لطيف (2019)، شرح قانون العقوبات العراقي رقم 111 لسنة 1969 بقسميه العام والخاص معززا بالقرارات التميزية دار النهضة العربية، بيروت.

2) الجبوري، سليم عبد الله (2011)، الحماية القانونية لمعلومات شبكة الانترنيت، ط 1، منشورات الحلبي الحقوقية.

3) جعفر، علي، (2013(، *جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة – دراسة مقارنة*، منشورات زين الحقوقية، بيروت.

4) الرزازي، محمد عطية محمد علي (2013)، الحماية القانونية لقواعد البيانات في القانون المصري والتشريعات المقارنة، دار الجامعة الجديدة، الإسكندرية، مصر.

5) الزعبي، جلال محمد (2010)، وأحمد محمد المناعسة، جرائم تقنية المعلومات الإلكترونية، ط 1، دار الثقافة للنشر والتوزيع، عمان.

6) الغافري، حسن (2009)، السياسة الجنائية في مواجهة جرائم الانترنيت، دار النهضة العربية، القاهرة.
7) الكعبي، محمد عبيد (2009)، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، الطبعة الثانية، دار النهضة العربية
8) الموسوي، منى تركي، الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة عليها، مركز بحوث السوق وحماية المستهلك، جامعة بغداد.
9) رستم، هشام فريد (1993)، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة لآلات الحديثة.
10) رمضان، مدحت عبد الحليم (2000)، جرائم الاعتداء على الأشخاص والإنترنيت، دار النهضة العربية القاهرة، ط 1.
11) طه، صابرين ناجي، دور القانون الجنائي في حماية البيانات الرقمية، مجلة النهرين للعلوم القانونية، العدد3، المجلد 26، 2024.
12) عياد، سامي علي حامد (2007)، الجريمة المعلوماتية وجرائم الانترنيت، دار الفكر الجامعي، الإسكندرية.
13) كاظم، صالح جواد (1991)، ملاحظات حول مفهوم علوية حقوق الإنسان مباحث في القانون الدولي، دار الشؤون الثقافية العامة، بغداد، ط1.
14) قارة، آمال (2007)، الحماية الجزائية للمعلوماتية في التشريع الجزائري، ط 2، دار دومة، للطباعة والنشر والتوزيع، الجزائر.

ثالثاً: المجلات والرسائل العلمية:

1) الشاذلي، فتوح، وعفيفي، كامل عفيفي (2003)، جرائم الكومبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون دراسة مقارنة، منشورات الحملي الحقوقية، لبنان.
2) المضحكي، حنان ريحان (2014)، الجرائم المعلوماتية "دراسة مقارنة"، ط 1، منشورات الحلبي الحقوقية، بيروت.
3) اللمعي، ياسر محمد، (2022)، السياسة الجنائية المعاصرة في حماية خصوصية البيانات الشخصية الإلكترونية – دراسة تحليلية مقارنة، مجلة روح القوانين، العدد السابع والتسعون .
4) سويلم، خالد سويلم محمد، (2022)، الحماية القانونية للبيانات الشخصية الإلكترونية – دراسة مقارنة، المجلة القانونية، المجلد 14، العدد 6.
5) جدي، صبرينة، الحماية القانونية للحق في الخصوصية المعلوماتية، مجلة التواصل في الاقتصاد والإدارة والقانون، المجلد 24، العدد 2.
6) الخضر، أبو بكر سلطان محمد، وكروم، عفاف مصطفى حامد، (2021)، وصف البيانات الرقمية بمواقع مصادر الوصول الحر، المجلة العربية للمعلوماتية وأمن المعلومات، مج2، ع4.
7) محمود، سيد أحمد، (2024)، حماية البيانات الشخصية الرقمية وفقًا لأحكام القانون المصري، مجلة العلوم القانونية والاقتصادية، ع1، السنة 66.
8) صالح، سلمي محسن حسن، (2023)، جهود منظمات مكافحة الجريمة المعلوماتية، مجلة دراسات في الخدمة الاجتماعية، العدد 63.

9) مباركية، مفيدة، (2018)، الحماية الجنائية للحق في الخصوصية الرقمية في القانون الجزائري، مجلة كلية الشريعة والاقتصاد.
10) معزوز، دليلة، (2021)، حماية المعطيات الشخصية في البيئة الافتراضية في التشريع الجزائري، مجلة الاجتهاد للدراسات القانونية والاقتصادية.
11) أيوب، بولين أنطونيوس (2009)، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، دراسة مقارنة، ط 1، منشورات الحلبي الحقوقية، لبنان
12) حزام فتحية، الضمانات القانونية لمعالجة المعطيات ذات الطابع الشخصي، دراسة على ضوء القانون رقم 18-07، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد 8، عدد 4، السنة 2019.
13) عبد الله، أحمد كيلاني، ومحمود، بلال عبد الرحمن (92019)، سياسة استبدال الصفة الجنائية للعقوبة، دراسة مقارنة، المركز العربي للنشر والتوزيع، مصر.
14) عفيفي، أحمد طارق (2014)، الجرائم الإلكترونية، جرائم الهاتف المحمول، دراسة مقارنة بين القانون المصري والإماراتي والنظام السعودي المركز القومي للإصدارات القانونية، مصر.
15) مجيد، سوز حميد، الحماية القانونية للحق في خصوصية البيانات الشخصية في العراق، دراسة تحليلية مقارنة، مجلة دراسات قانونية وسياسية، العدد11، السنة 6، 2018.
16) محمود، مروان محمود صالح، الحماية الجنائية للبيانات الشخصية الإلكترونية، مجلة كلية القانون للعلوم القانونية والسياسية، المجلد 14، العدد 52، 2025.
17) نعيم، مغبغب (2006)، حماية برامج الكمبيوتر الأساليب والثغرات، دراسة في القانون المقارن، ط1، منشورات الحلبي الحقوقية، بيروت، لبنان.

رابعاً: قوانين وقرارات:

1) دستور العراق الدائم لعام 2005.
2) القانون المصري رقم (151) لسنة 2020 بشأن حماية البيانات الشخصية.
3) القانون المصري رقم (175) لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات.
4) القانون القطري رقم (13) لسنة 2016 بشأن حماية خصوصية البيانات الشخصية.
5) القانون القطري رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية.
6) قانون العقوبات القطري رقم (11) لسنة 2004 المعدل بالقانون رقم (4) لسنة 2017.
7) قانون العقوبات العراقي رقم 111 لسنة 1969.
8) قانون التوقيع الإلكتروني والمعاملات الإلكترونية رقم (78) لسنة 2012.

خامسا: المواقع الإلكترونية.

الزيدي، كاظم عبد جاسم، (2022)، الحماية القانونية للبيانات الشخصية في القانون العراقي:
https://dcc-iq.com/?p=41826

القاضي، أريج خليل، (2023)، جريمة سرقة واختلاس البيانات الإلكترونية للدولة:
/https://www.sjc.iq/view.71508