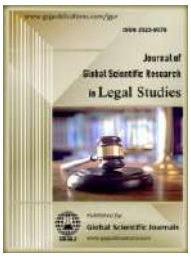
Journal of Global Scientific Research in Legal Studies
Vol.10, Issue 9/ pp. 3965-3983/ September 2025

Contents lists available at www.gsjpublications.com

Journal of Global Scientific Research in Legal Studies

journal homepage: www.gsjpublications.com/jourgsr



Judicial Mechanisms in Public Law to Confront Cyber Threats to Information

Hussein Ali Dakman Shammaran

Middle Technical University, Al-Suwaira Technical Institute, Wasit, Iraq.

ARTICLE INFO

Received: 7 Aug 2025,
Revised: 17 Aug 2025,
Accepted: 19 Sep 2025,
Online: 9 Sep 2025

Keywords:
Information Security, Cybersecurity, Public Law, Cyber Threats, Legal Oversight, Remote Litigation.

ABSTRACT

Amidst the rapid technological momentum and the expansive proliferation of digital information, information security has risen to become one of the most complex and vital legal and social challenges in the digital age. This study addresses the conceptual and general legal framework of information security, highlighting the cyber threats that endanger critical public utilities. It examines the effectiveness of public law tools in confronting these risks through modern legislation, specialized regulatory bodies, and effective oversight mechanisms. The research also emphasizes the role of remote litigation as an innovative mechanism that enhances the speed and efficiency of legal responses, reflecting the pivotal position of public law tools in organizing the relationship between the state and individuals within a complex digital space. Here, precise rules are formulated to balance cyber security protection with the preservation of digital freedoms, while ensuring principles of transparency and accountability. The study underscores the urgent need to update these legal tools, especially in countries like Iraq, aiming to build an integrated system combining advanced legislation, independent authorities, and coherent national strategies. The research confirms that cyber security cannot be reduced to a purely technical dimension but requires a comprehensive legal and social vision, positioning public law as the fundamental framework that guarantees the public interest and protects essential digital rights. The study concludes with strategic recommendations to enhance the efficiency of legal and regulatory tools, enabling them to address the complex challenges of the digital era while maintaining a delicate balance between security and freedom, thereby consolidating the concept of digital sovereignty and safeguarding individual rights simultaneously.

Corresponding author:
E-mail address: hussein.ali@mtu.edu.iq
doi: 10.5281/jgsr.2025.17073647

الآليات القضائية في القانون لمواجهة التهديدات السيبرانية لأمن المعلومات

حسين علي دكمان شمران

الجامعة التقنية الوسطى، المعهد التقني، الصويرة، واسط، العراق.

E-mail address: hussein.ali@mtu.edu.iq

الملخص

في ظل الزخم التكنولوجي المتسارع والتمدّد الواسع للمعلومات الرقمية، ارتقى أمن المعلومات ليصبح أحد أكثر التحديات القانونية والاجتماعية تعقيدًا وحيوية في العصر الرقمي، يتناول هذا البحث الإطار المفاهيمي والقانوني العام لأمن المعلومات، مسلطًا الضوء على التهديدات السيبرانية التي تهدد المرافق العامة الحيوية، مستعرضًا فاعلية أدوات القانون العام في مواجهة هذه المخاطر من خلال التشريعات الحديثة، الهيئات التنظيمية المتخصصة، وآليات الرقابة الفعّالة، كما يبرز دور التقاضي عن بُعد كآلية مبتكرة تعزز سرعة وكفاءة الاستجابة القانونية، لما تتبوأه أدوات القانون العام من مكانة محورية في تنظيم العلاقة بين الدولة والأفراد داخل فضاء رقمي معقد، حيث تُصاغ قواعد دقيقة توازن بين حماية الأمن السيبراني وصون الحريات الرقمية، مع ضمان مبادئ الشفافية والمساءلة، ويبرز البحث الحاجة الملحة لتحديث هذه الأدوات القانونية، خاصة في دول كالعراق، بهدف بناء منظومة متكاملة تجمع بين تشريعات متطورة، هيئات مستقلة، واستراتيجيات وطنية متماسكة، حيث تؤكد الدراسة أن الأمن السيبراني لا يمكن اختزاله في بعد تقني بحت، بل يتطلب رؤية قانونية واجتماعية شاملة تجعل من القانون العام الإطار الضامن لتحقيق الصالح العام وحماية الحقوق الرقمية الأساسية، وفي ختام البحث، تُقدم توصيات استراتيجية لتعزيز كفاءة الأدوات القانونية والتنظيمية، تمكّن من مواجهة تحديات العصر الرقمي المعقدة، مع الحفاظ على التوازن الدقيق بين الأمن والحرية، مما يرسخ مفهوم السيادة الرقمية ويصون الحقوق الفردية في آنٍ معًا.

الكلمات المفتاحية: أمن المعلومات، الأمن السيبراني، القانون العام، التهديدات السيبرانية، الرقابة القانونية، التقاضي عن بُعد.

المقدمة

أضحى العالم المعاصر يعيش في قلب ثورة رقمية غير مسبوقة، قلبت موازين الحياة اليومية، وفرضت واقعًا جديدًا على الأفراد والدول على حد سواء، ففي ظل التحول المتسارع نحو الإدارة الإلكترونية والاعتماد المتزايد على البيانات الرقمية، برزت قضية أمن المعلومات بوصفها أحد أكثر التحديات إلحاحًا، حيث لم تعد الهجمات السيبرانية مجرد محاولات تخريبية معزولة، بل أصبحت ظاهرة ممنهجة تهدد سيادة الدول، واستقرار مؤسساتها، وسلامة مصالحها الحيوية، وفي خضم هذا المشهد، تظهر أهمية القانون العام كأداة مركزية يفترض بها أن تواجه هذه التحديات؛ باعتباره الحارس التقليدي للنظام العام، والمُنظم للعلاقة بين السلطة الإدارية والمجتمع. غير أن التهديدات السيبرانية لا تعترف بالحدود الجغرافية أو بالضوابط القانونية الكلاسيكية، فهي تنفذ في فضاء مفتوح، وتحمل طابعًا متغيرًا ومتطورًا باستمرار، الأمر الذي يفرض على القانون العام بمكوناته الدستورية والإدارية أن يعيد النظر في أدواته، ويبحث عن آليات جديدة قادرة على التعامل مع واقع رقمي بالغ التعقيد، ولأن حماية أمن المعلومات لم تعد حكرًا على التقنيين، بل أصبحت مسؤولية مشتركة بين المؤسسات التقنية والهيئات القانونية، فإن القانون العام، بوصفه الإطار الحاكم للعلاقة بين السلطة والمجتمع، يدخل اليوم على خط المواجهة، مع ما يتطلبه ذلك من تحديث قواعده، وتوسيع وظائفه، وتطوير أدواته الرقابية والتنظيمية لتلائم بيئة متغيرة لا تخضع للحدود الجغرافية أو النمط القانوني الكلاسيكي.

في هذا السياق، تتناول الدراسة الحالية الإطار النظري والتطبيقي لتفاعل القانون العام مع هذه التحديات الرقمية، وتبحث في مدى قدرته على مواكبة التهديدات السيبرانية التي تطال أمن المعلومات داخل البنية الإدارية للدولة، من خلال خطة بحثية تتناول المفهوم، والوسائل، والتشريعات، وأوجه القصور، وآفاق التطوير.

أهمية البحث:

تكتسب هذه الدراسة أهميتها من طبيعة الموضوع الذي تتناوله، إذ تمثل التهديدات السيبرانية واحدة من أبرز المخاطر التي تواجه أمن الدول في العصر الرقمي، وخصوصًا ما يتعلق بأمن المعلومات داخل المؤسسات العامة. وفي هذا السياق، يبرز دور القانون العام – سواء من حيث التشريعات أو الوظائف الإدارية والرقابية – كأداة ضرورية لتنظيم هذا الفضاء وضمان سلامته.

وتزداد أهمية البحث نظرًا لكون القانون العام قد نشأ في بيئة تقليدية قائمة على مفاهيم السيادة والمرفق العام، بينما تظهر التهديدات السيبرانية في بيئة متغيرة، عابرة للحدود، يصعب إخضاعها للأطر القانونية الكلاسيكية. من هنا، فإن محاولة فهم كيفية استجابة قواعد القانون العام لهذا النوع من التهديدات، وكيفية تكيّفها مع التغيرات الرقمية المتسارعة، تمثل إسهامًا مهمًا في سد فجوة معرفية قائمة في هذا المجال، كما تسلط الدراسة الضوء على الحاجة إلى أدوات قانونية جديدة أو محدثة، تساعد الجهات العامة على حماية أمنها الرقمي بكفاءة، وتضع أطرًا واضحة للمساءلة والرقابة الإدارية، بما يحول دون وقوع الخلل أو التقصير عند مواجهة الهجمات السيبرانية، وتكمن أهمية هذه الدراسة أيضًا في توقيتها، إذ تتزايد الهجمات الرقمية على مؤسسات الدولة، في ظل تطور أدوات الجريمة الإلكترونية، وتوسّع استخدام التكنولوجيا في تقديم الخدمات العامة، وهو ما يجعل من القانون العام خط الدفاع الأول في ضبط وتنظيم هذا الواقع الجديد.

إشكالية البحث:

مع تسارع التحول الرقمي في المؤسسات العامة، لم تعد التهديدات السيبرانية مسألة فنية بحتة، بل تحولت إلى معضلة قانونية وتنظيمية تمس جوهر السيادة الإدارية للدولة ومشروعية أدائها، ففي ظل توسّع الفضاء المعلوماتي واعتماد الجهات الرسمية على الأنظمة الإلكترونية في معالجة البيانات وتقديم الخدمات، باتت الهجمات السيبرانية تهدد ليس فقط سرية المعلومات، بل أيضًا استمرارية المرافق العامة وسلامة القرارات الإدارية.

وقد نشأ القانون العام، بمفاهيمه الكلاسيكية، لتنظيم العلاقة بين الإدارة والأفراد، وضمان حماية النظام العام، لكنه اليوم يواجه واقعًا جديدًا تفرضه البيئة الرقمية، بكل ما تحمله من تحديات عابرة للحدود، وغموض تشريعي، وحاجة متزايدة إلى آليات مرنة وفعالة. وهنا تطرح الإشكالية نفسها بإلحاح:

ما مدى فاعلية أدوات القانون العام في التصدي للتهديدات السيبرانية لأمن المعلومات، وهل يملك هذا الفرع القانوني الوسائل الكافية لحماية المصالح الرقمية العامة في ظل تطور التهديدات وتبدل صورها؟

فرضيات البحث:

1. يمتلك القانون العام، بمكوناته الدستورية والإدارية، إطارًا نظريًا يسمح بالتدخل لحماية أمن المعلومات، إلا أن فعاليته محدودة بسبب بطء التكيّف مع مستجدات البيئة الرقمية.
2. الرقابة الإدارية والقضائية على أداء الجهات المختصة بأمن المعلومات ما زالت غير كافية لضمان الحماية الفعلية من التهديدات السيبرانية، مما يؤدي إلى فجوة بين النصوص القانونية والتطبيق العملي.
3. يمكن تعزيز دور القانون العام في التصدي للتهديدات السيبرانية من خلال تحديث التشريعات وتبني سياسات وقائية مرنة، قائمة على التعاون بين الدولة والقطاع التكنولوجي، بما يضمن حماية الأمن السيبراني كمصلحة عامة عليا.

منهجية البحث:

يعتمد هذا البحث على المنهج الوصفي التحليلي، من خلال تحليل الإطار النظري والمفاهيمي للقانون العام وأمن المعلومات، واستقراء النصوص القانونية ذات الصلة على المستوى الوطني، بهدف تحديد مدى فاعلية القواعد الإدارية والدستورية في التصدي للتهديدات السيبرانية و الوقوف على أوجه القصور والإفادة من الممارسات الفضلى في هذا المجال، كما ستقوم الباحثة كذلك بتوظيف المنهج النقدي في تحليل السياسات العامة والتشريعات ذات العلاقة، للكشف عن الثغرات التشريعية والمؤسسية التي تعيق فاعلية القانون العام في هذا المجال، وذلك بهدف تقديم توصيات واقعية وقابلة للتطبيق تسهم في تطوير منظومة الحماية السيبرانية على المستوى الإداري والدستوري.

خطة البحث:

المبحث الأول: الإطار المفاهيمي والقانوني العام لحماية أمن المعلومات.

المطلب الأول: مفهوم مصطلح أمن المعلومات في السياق السيبراني.

المطلب الثاني: التهديدات السيبرانية لأمن المعلومات وأثرها على المرافق العامة.

المبحث الثاني: فاعلية أدوات القانون العام في التصدي للتهديدات السيبرانية.

المطلب الأول: القانون العام وحماية الأمن السيبراني_ آليات وتحديات.

المطلب الثاني: دور التقاضي عن بعد في تعزيز فعالية القانون العام في مواجهة التحديات السيبرانية.

الخاتمة

النتائج

التوصيات

قائمة المراجع

المبحث الأول:

الإطار المفاهيمي والقانوني العام لحماية أمن المعلومات

لم يعد أمن المعلومات مجرد مسألة تقنية محضة، بل غدا من أبرز التحديات التي تواجه البنى المؤسساتية للدول في العصر الرقمي، سواء من حيث طبيعة المعلومات المحمية، أو الوسائل المستخدمة في اختراقها، أو من حيث حجم الأضرار المترتبة على انتهاكها، وبالتزامن مع تصاعد التهديدات السيبرانية وتطور أدوات الجريمة الرقمية، برزت الحاجة إلى مراجعة شاملة للإطار القانوني الناظم لأمن المعلومات، خاصة على مستوى القانون العام، الذي يقع عليه عبء حماية النظام العام الرقمي وصيانة المصالح الحيوية للأفراد والدولة، حيث إن فهم طبيعة أمن المعلومات وحدوده القانونية يشكل الخطوة الأولى لتحديد مدى فاعلية القواعد القانونية في الوقاية من الاعتداءات السيبرانية وردع مرتكبيها، وتتداخل هذه المسألة مع التعريفات التقنية، والضوابط التشريعية، والضمانات المؤسسية، مما يجعل الحاجة إلى إطار مفاهيمي وقانوني متكامل أمراً لا غنى عنه، كما أن التهديدات السيبرانية باتت تشكّل مصدر قلق دائم للمؤسسات العامة، نظرًا لما تحمله من إمكانيات التسلل إلى نظمها، والتأثير على قدرتها التشغيلية، أو حتى استهداف البنية التحتية للدولة، ولتحقيق ذلك، سيتم تناول هذا المبحث في مطلبين رئيسيين: يُعنى الأول بدراسة مفهوم مصطلح أمن المعلومات في السياق السيبراني، أما الثاني فنتناول فيه: التهديدات السيبرانية لأمن المعلومات وأثرها على المرافق العامة، كمايلي:

المطلب الأول:

مفهوم مصطلح أمن المعلومات في السياق السيبراني

في خضم التحولات الرقمية المتسارعة التي يعيشها العالم المعاصر، أصبح مصطلح "أمن المعلومات" أحد أكثر المفاهيم تداولًا، لما له من صلة مباشرة بحياة الأفراد والمؤسسات والدول، غير أن استيعاب هذا المفهوم الحديث لا يكتمل دون العودة إلى جذوره اللغوية التي تسهم في كشف دلالاته العميقة

وبنيته المفهومية الأساسية، حيث يتكون هذا المصطلح من عنصرين رئيسين هما: "الأمن" و"المعلومات"، ولكل منهما دلالته المتجذرة في اللغة العربية، والتي تُضيء لنا طريق الفهم المعاصر للمصطلح في ضوء الأصل اللغوي.

فكلمة "الأمن" في اللغة العربية ترتبط بالطمأنينة والسلام، وهي نقيض الخوف. وقد ورد هذا المعنى في القرآن الكريم في أكثر من موضع، من بينها قوله تعالى: {الذي أطعمهم من جوعٍ وآمنهم من خوف}[قريش: 4].

حيث يَرد الأمن كنعمة تُقابل الجوع والخوف، ويُمنّ الله بها على عباده، وكذلك قوله تعالى: {ادخلوها بسلام آمنين}[الحجر: 46]، والذي يبرز فيه الأمن كحالة من السلام النفسي والجسدي داخل الجنة.

وإذا ما رجعنا إلى المعاجم اللغوية، نجد أن الأمن يُفَسّر بأنه السكينة والاطمئنان وزوال القلق، [1]أي هو الحالة التي يعيش فيها الإنسان خاليًا من الخوف، سواء كان ذلك الخوف على النفس أو المال أو العرض أو أي مصلحة أخرى، وهو عدم توقع مكروه في الزمن الآتي، وأصله طمأنينة النفس وزوال الخوف،[2] ويقال: "أمن من الشيء" إذا سلم منه، و"أمن على ماله" إذا ائتمن غيره عليه، فالأمن هنا يتضمن جانبين: الوقاية من الخطر، والضمان للحقوق،[3] وعلى هذا الأساس، فإن "الأمن" في اللغة لا يُعنى فقط بالحماية من الخطر الفعلي، بل يتسع ليشمل الشعور بالثقة والاطمئنان في النفس، وهو ما يتوافق تمامًا مع المقصود بـ"أمن المعلومات"، الذي لا يعني فقط منع التهديد، بل تعزيز الشعور بالثقة الرقمية لدى الأفراد والمؤسسات في بيئة التعامل الإلكتروني.[4]

أما فيما يخص العنصر الثاني، وهو "المعلومات"، فهي جمع "معلومة"، والمعلومة مشتقة من الجذر "ع ل م"، وهو أصل يدل على الإدراك والمعرفة واليقين، فالعلم في اللغة هو "إدراك الشيء بحقيقته"،[5] والمعلومة هي "البيان الذي تم إدراكه وتوثيقه وأصبح قابلاً للتداول والفهم"،[6] وقد تطور هذا المصطلح في العصر الحديث ليعني كل محتوى معرفي يُخزَّن ويُنقل ويُستخدم، سواء كان رقميًا أو ورقيًا، بسيطًا أو معقدًا، خاصًا أو عامًا. إذًا، حين نتحدث عن أمن المعلومات، فنحن بصدد الحديث عن حالة الطمأنينة والثقة في التعامل مع البيانات، من حيث سرّيتها وسلامتها وتوافرها، وهي عناصر ثلاثة تقوم عليها جميع النظريات الأمنية الحديثة في علم المعلومات.[7]

لكن التطور التكنولوجي الهائل في العقود الأخيرة أضاف بعدًا جديدًا لهذا المفهوم، يتمثل في الفضاء السيبراني، وهو ما يحيلنا إلى مصطلح ثالث مرتبط: السيبرانية، [8]وهو من يقود السفينة ويوجّهها بحكمة في البحر، وهو تشبيه ينطبق تمامًا على من يوجه الأنظمة الرقمية الحديثة ويحميها من الانزلاق أو الاصطدام. [9]

ومع ولادة الإنترنت، بدأت كلمة "Cyber" تأخذ معنى "الفضاء الرقمي"، أي البيئة غير الملموسة التي تنشأ نتيجة الترابط بين الأجهزة والشبكات وقواعد البيانات والمستخدمين والتحكم الآلي.[10]

---

[1] روحي البعلبكي، قاموس المورد، ط7، دار العلم للملايين، بيروت، 1995، ص777.

[2] الزبيدي، مرتضى بن محمد. تاج العروس من جواهر القاموس، تحقيق مجموعة من العلماء، إشراف عبد الستار أحمد فراج، الكويت: وزارة الأوقاف والشؤون الإسلامية، 1399هـ / 1979م، ج34، ص184.

[3] ابن منظورمحمد بن مكرم، لسان العرب، ط1 دار صادر، ج1، بيروت، لبنان،2000، ص163.

[4] م. م. رعد خضير صليبي، تعزيز الأمن السيبراني في العراق: التحديات والفرص، مجلة دراسات دولية، العدد تسعة وتسعون، 2024، ص 509.

[5] انظر الرابط: ص3 – كتاب تفسير القرآن الكريم أسامة سليمان – تعريف العلم لغة واصطلاحا – المكتبة الشاملة تاريخ الاطلاع 2025/7/10.

[6] محمد السعيد خشبة، نظم المعلومات الإدارية، دار النشر للجامعات، القاهرة، 2008، ص 22.

[7] انظر الرابط الآتي: أمن المعلومات: مفهومه وأهميته وعناصره تاريخ الاطلاع 2025/7/11.

[8] إن لفظ "السيبر" (Cyber) مأخوذ من الكلمة اليونانية "Kybernetes"، والتي تعني "قائد الدفّة" أو "الموجه".

[9]شعبان عبد العاطي عطية واخرون، المعجم الوسيط، ط 4، مكتب الشروق الدولية" مجمع اللغة العربية"، مصر، 2004، ص28.

[10]ج. رضوان، الأمن السيبراني، أولوية في استراتيجيات الدفاع، مجلة الجيش، مؤسسة المنشورات العسكرية، الجزائر، العدد 603، جانفي، 234، ص 14.

وبذلك، ظهر مفهوم "الأمن السيبراني" ليشير إلى مجموعة الإجراءات التقنية والتنظيمية التي تُتخذ لحماية هذا الفضاء من التهديدات المختلفة، بما يشمل الفيروسات، والهجمات الإلكترونية، والاختراقات، والتجسس الرقمي، وغير ذلك من صور الجرائم الحديثة، وفي ضوء هذا التحول، بات من الواضح أن الحديث عن "أمن المعلومات" لم يعد قاصرًا على حماية الأوراق أو الوثائق، بل أصبح يعني حماية الكيان الرقمي الذي تُنتج فيه المعلومات وتُخزّن وتُنقل، وهو فضاء لا يخضع للحدود الجغرافية، ويحتاج إلى أطر لغوية وقانونية وتنظيمية جديدة تتناسب مع خصائصه المعقدة.[11]

من هنا، فإن المفهوم اللغوي لأمن المعلومات، وإن كان يستند إلى الجذور الأصيلة لكلمتي "الأمن" و"المعلومة"، إلا أنه في السياق الحديث قد تمدّد وتطور ليعبر عن حالة متقدمة من الحماية الرقمية، تعتمد على الذكاء الاصطناعي، والتحليل السلوكي، والأنظمة الوقائية، وترتبط ارتباطًا وثيقًا بالسيادة الوطنية والسياسة العامة للدول.

وقد انعكس هذا التوسع المفاهيمي على التشريعات المعاصرة، التي بدأت تُدرك أن أمن المعلومات لم يعد شأنًا تقنيًا فقط، بل أصبح جزءًا من الأمن القومي، ومجالًا يحتاج إلى تدخل تشريعي، وتخطيط استراتيجي، وتعاون دولي، ويُفهم أمن المعلومات – في سياقه العام – على أنه مجموعة الإجراءات والوسائل الفنية والتنظيمية التي تهدف إلى حماية المعلومات والأنظمة الرقمية من الوصول غير المصرح به، أو التغيير، أو الإتلاف، أو الاستخدام أو الكشف غير المشروع، وتتضمن هذه الحماية جوانب متعددة كسلامة البيانات، وسرية المعلومات، وتوافرها عند الحاجة، مما يجعلها محوراً أساسياً لأي بنية تحتية تقنية موثوقة.[12]

وجدير بالذكر أنه وعلى الصعيد القانوني، فإن مفهوم أمن المعلومات لا يزال في العراق يفتقر إلى تقنين شامل ومتكامل، إذ لا يوجد قانون موحد خاص بالأمن السيبراني، بل نجد النصوص القانونية المتعلقة به موزعة على قوانين جزائية أو تنظيمية عامة، ما يخلق نوعاً من الفجوة القانونية في التعامل مع التهديدات الرقمية المعاصرة،[13] فبالرغم من إدراك الدولة التدريجي لأهمية هذا المجال، إلا أن البنية التشريعية القائمة ما زالت تعاني من التشتت، وضعف التحديث، وقلة المتابعة الواقعية لمخاطر الفضاء السيبراني، وتبرز الحاجة إلى تشريعات متخصصة تُعرّف بدقة مفهوم أمن المعلومات، وتحدد أركان الجريمة السيبرانية، وتُبيّن مسؤوليات الجهات الرسمية والخاصة، وتضع آليات للرقابة، والمتابعة، والاستجابة السريعة. وهذا ما يتطلب وجود قانون للأمن السيبراني يتسم بالشمولية والمرونة، ويواكب التطورات السريعة في مجال الجريمة الرقمية، ويعزز أدوات الردع والوقاية، ومن ناحية أخرى، يواجه بلدنا الحبيب العراق تحديات حقيقية في تطبيق الحماية القانونية لأمن المعلومات، فهناك ضعف في الوعي الأمني لدى الكثير من العاملين في المؤسسات العامة، بالإضافة إلى محدودية الكوادر المتخصصة في مجال الأمن السيبراني، الأمر الذي يزيد من احتمالية تعرض الأنظمة للاختراق والتلاعب، كما أن البنية التحتية لتكنولوجيا المعلومات لا تزال في طور التطوير، وتعاني من ثغرات تجعل من الصعب تنفيذ إجراءات حماية متقدمة، لكن في المقابل، تتاح فرص حقيقية لتحسين واقع أمن المعلومات في العراق، سواء من خلال الاستفادة من التجارب الدولية في مجال التشريع السيبراني، أو عبر التعاون مع منظمات دولية متخصصة تقدم الدعم والخبرة، فضلاً عن إمكانية تطوير مهارات الكوادر الوطنية في هذا المجال الحيوي، مما يسهم في خلق جبهة وطنية قادرة على حماية الفضاء الرقمي العراقي.[14]

المطلب الثاني

التهديدات السيبرانية لأمن المعلومات وأثرها على المرافق العامة

في العقود الأخيرة، شهد العالم تحولًا رقميًا شاملًا غيّر ملامح الحياة اليومية، فأصبح الحاسوب والإنترنت عنصرين أساسيين في البنى الاجتماعية والاقتصادية، وفي تسيير شؤون الأفراد والمؤسسات على حدٍّ سواء، ولم تقتصر آثار هذا التحول على التعاملات الفردية أو المؤسسية فحسب، بل

---

[11] منى جبور الاشقر، السيبرانية هاجس العصر، المركز العربي للبحث القانونية والقضائية، بيروت، 2017، لبنان، ص25.

[12] أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، المجلد 8، العدد 4، كلية القانون، جامعة بابل، العراق 2016، ص 616.

[13] مصطفى ابراهيم سلمان الشمري، الأمن السيبراني وأثره في الأمن الوطني العراقي، مجلة العلوم القانونية والسياسية، كلية القانون والعلوم السياسية جامعة ديالى، المجلد 10، العدد 1، 2021، ص 152.

[14] زهراء عماد محمد كلنتر، تكييف الهجمات السيبرانية في ضوء القانون الدولي، مجلة الكوفة للعلوم القانونية والسياسية، 2020 المجلد 1، العدد 44/1، 2020، ص 52.

امتدت لتطال البنية العميقة لعمل الحكومات والإدارات العامة، حيث بات الاعتماد على النظم الرقمية والبنى التحتية المعلوماتية هو القاعدة في تسيير المرافق العامة، وتقديم الخدمات، واتخاذ القرارات، وحفظ البيانات السيادية.

لكن هذا الانفتاح الواسع على الفضاء الرقمي لم يكن خالياً من التحديات، بل أفرز نوعًا جديدًا من المخاطر غير التقليدية، عابرة للحدود، وغير مرئية، تُعرف اليوم بـ "التهديدات السيبرانية"، وقد تزايدت خطورة هذه التهديدات مع تعاظم الاعتماد على تقنيات المعلومات والاتصالات، حيث لم تعد مجرد احتمالات نظرية أو حوادث فردية، بل أصبحت واقعاً يومياً يهدد استقرار النظم المعلوماتية، وسلامة البيانات، واستمرارية أداء المرافق العامة، بل وأمن الدول ذاته.

وفي ظل هذا الواقع الجديد، باتت الهجمات السيبرانية تستهدف أهم الموارد الحيوية للدولة وبنيتها المعلوماتية ولم تعد تقتصر على مجرد إتلاف أجهزة أو تعطيل خدمات، بل تطورت لتشمل السرقة، والتجسس، والتشويه، والتخريب المنهجي لأنظمة الدولة الرقمية، وقد طالت هذه التهديدات المؤسسات الرسمية في قطاعات حساسة كالأمن، والطاقة، والتعليم، والصحة، والمالية، ما جعل من "أمن المعلومات" مكونًا جوهريًا من مكونات الأمن القومي.[15]

ويمكن تصنيف التهديدات السيبرانية وفق نطاق الاستهداف إلى ثلاث فئات رئيسية، تُبيّن بدقة طبيعة المخاطر ومواقع الخلل المحتملة:[16]

أولًا: التهديدات التي تطال مكونات الحاسوب المادية والمعنوية

تُشكّل مكونات الحاسوب – سواء كانت مادية ملموسة أو معنوية رقمية – الهدف الأول والأكثر عرضة للهجمات السيبرانية في العصر الرقمي، لا سيّما مع تزايد الاعتماد المؤسسي والإداري على البنية التحتية التكنولوجية في تشغيل المرافق العامة وإدارة المعلومات الحساسة، ويعكس هذا الاستهداف نزعة واضحة لدى القراصنة الرقميين إلى شلّ الأجهزة والأنظمة في مهدها، وحرمان المؤسسات من أدنى وظائفها التقنية، وتتجلى التهديدات الموجهة إلى المكونات المادية للحاسوب في محاولات تعطيل أو تدمير وحدات الإدخال مثل لوحة المفاتيح والماسحات الضوئية، أو وحدات الإخراج كالشاشات والطابعات، بالإضافة إلى الوسائط التخزينية كالأقراص الصلبة (Hard Drives) والذواكر المحمولة (USB)، وهي الوسائط التي تحفظ عليها المؤسسات العامة قواعد بياناتها ومراسلاتها ووثائقها الرسمية، إن مجرد عطب في هذه الوحدات قد يتسبب بشلل وظيفي تام لمرفق عام، أو تعطل تقديم خدمة حيوية للمواطنين، غير أن الأخطر من ذلك هو ما يصيب المكونات المعنوية، وهي تمثل جوهر عمل الحاسوب، وتتمثل بالبرمجيات، والأنظمة التشغيلية، وقواعد البيانات، والمعلومات المخزنة أو المتبادلة.[17] فالهجمات التي تطال هذه المكونات تُعد الأخطر، إذ لا تُرى بالعين المجردة ولا يُستدل عليها بسرعة، مما يُصعّب من عملية احتوائها أو منع انتشارها، وتُستخدم في هذه الهجمات أدوات رقمية معقدة تعرف بـ البرمجيات الخبيثة (Malware)، ومن بينها ما يُعرف بفيروسات الفدية (Ransomware)، وهي من أخطر البرمجيات الهجومية التي انتشرت في السنوات الأخيرة، إذ تقوم بتشفير الملفات الحساسة على الجهاز أو الشبكة، وتطالب الجهة المستهدفة بدفع مبلغ مالي – عادة ما يكون بعملة رقمية يصعب تتبعها – مقابل إعادة فك التشفير، ويتحول هذا النوع من الهجمات إلى أزمة مؤسسية حقيقية عندما يستهدف أنظمة المرافق العامة أو الأجهزة المرتبطة بخدمات المواطنين، كما حدث في عدة دول حين توقفت المستشفيات والموانئ أو شبكات توزيع الوقود عن العمل لساعات أو أيام بسبب اختراق مماثل.[18]

وفي هذا السياق، لا تمثل خسارة الأجهزة أو البيانات مجرد خلل تقني، بل تمتد آثارها إلى البعد السيادي للدولة، خصوصًا إذا كانت المعلومات المسروقة تتعلق بوزارات سيادية، أو مؤسسات أمنية، أو ملفات تخص الأمن القومي أو العلاقات الدبلوماسية، فكل عطب تقني يطال أجهزة الدولة، أو فقدان معلومات رقمية، قد يؤدي إلى تهديد مباشر لمفهوم المصلحة العامة، وتعطيل سير المرافق العامة، وتقويض ثقة المواطن بمؤسساته، ومن جهة أخرى، تبرز التحديات أمام القانون العام، الذي لا يزال في كثير من الدول – ومنها العراق – غير مهيّأ تشريعيًا أو إداريًا بما يكفي لمواجهة هذه الأنواع

[15] رزق أحمد سمودي، حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون الدولي العام، مجلة جامعة الشارقة للعلوم القانونية، المجلد 15، العدد 2، ديسمبر 2018، ص346.

[16] العيداني محمد، التهديدات السيبرانية وجرائم المعلومات، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد 13، العدد 01، 2024، ص20.

[17] إسراء شريف جيجان، الأمن السيبراني الصيني_ دراسة في الدوافع والتحديات، قضايا سياسية، العدد 56، ص 35.

[18] إبراهيم أحمد عبد السامرائي، الجريمة الالكترونية السيبرانية في القانون الدولي، مجلة جامعة جيهان أربيل للعلوم الإنسانية والاجتماعية، المجلد 6، العدد 2، 2022، ص .146

من الجرائم المعقدة، فبينما تتطوّر أدوات القراصنة بوتيرة عالية، تبقى نظم الحماية القانونية والإجرائية بطيئة في الاستجابة، مما يفتح المجال أمام المتسللين لإحداث أضرار واسعة دون وجود نصوص واضحة تجرّم أفعالهم أو تحدد مسؤولية الجهات الرسمية في حال وقوع الخرق.

ثانيًا: التهديدات التي تطال الشبكات والبنى التحتية المعلوماتية

مع التقدم المتسارع في رقمنة العمل الإداري وتوسّع استخدام الشبكات الداخلية والخارجية في تشغيل مرافق الدولة، أصبحت البنى التحتية المعلوماتية – وعلى رأسها شبكات الاتصال وتبادل البيانات – عصبًا حيويًا يربط بين مختلف الجهات الرسمية، من الوزارات والمؤسسات المركزية، إلى المديريات والفروع الميدانية. وفي ظل هذا الاعتماد المتزايد على الشبكات الرقمية، أضحت هذه الأخيرة عرضةً لهجمات سيبرانية معقدة تستهدف قدرتها على العمل، وسلامة محتواها، وموثوقية الخدمات التي تمرّ من خلالها.[19]

تتمثل هذه التهديدات في أعمال هجومية موجهة إلى البنية الشبكية للدولة، وتتخذ أشكالًا متعددة، منها تعطيل الخوادم (Servers) أو الضغط عليها من خلال هجمات الحرمان من الخدمة (DDoS)، والتي تُغرق الشبكة بسيلٍ من الطلبات الوهمية، مما يؤدي إلى إبطاء عملها أو توقفها التام. ويستهدف هذا النوع من الهجمات بشكل خاص المواقع الحكومية التي تقدم خدمات مباشرة للمواطنين، كأنظمة تسجيل الولادات أو إصدار الهويات أو الخدمات الضريبية، وهو ما يؤدي عمليًا إلى شلل إداري واسع وتعطيل سير المرفق العام.

ويستخدم المهاجمون السيبرانيون أدوات معقدة في اختراق البنى الشبكية، مثل استغلال الثغرات الأمنية في برامج الإدارة، أو انتحال الهويات الرقمية، أو زرع برمجيات تجسسية تتيح لهم التحكم عن بُعد بأجزاء من الشبكة، أو التجسس على حركة البيانات المتدفقة فيها. وتكمن الخطورة في أن هذه الشبكات غالبًا ما تكون مترابطة، مما يجعل اختراق جزءٍ منها مدخلًا للوصول إلى وحدات أخرى داخل المنظومة الإدارية للدولة، بما في ذلك أجهزة حساسة، أو شبكات ذات طابع أمني أو سيادي.[20]

ولا تقتصر هذه التهديدات على البنية التقنية بحد ذاتها، بل تشمل كذلك تشويش أو تعديل محتوى المواقع الرسمية، من خلال استهداف واجهاتها الإلكترونية لتغيير الرسائل أو بثّ معلومات مضللة، أو نشر بيانات ملفقة قد تمس بهيبة الدولة أو تثير البلبلة في الرأي العام، ففي الكثير من الحالات، يتم استغلال اختراق الشبكة ليس فقط لتعطيلها، بل لاستخدامها منصةً لنشر محتوى معادٍ أو توجيه رسائل دعائية لمهاجميها، ويُعدّ هذا النوع من الهجمات تهديدًا مباشرًا لسيادة الدولة الرقمية، إذ يُفقد الجهات الرسمية سيطرتها على أدوات التواصل، ويشوّش على مصداقيتها، ويجعلها عُرضة للتشكيك في كفاءتها التقنية والإدارية. كما أن هذه الهجمات قد تؤدي إلى تسريب بيانات مرور الشبكة (Traffic Data)، وهي بيانات حساسة تكشف عن طبيعة الاتصالات، وأوقات العمل، وعناوين المستخدمين، وهو ما يُسهّل للمهاجمين تحليل السلوك المؤسسي، ورسم خطط هجوم أكثر دقة في المستقبل.[21]

وفي ضوء هذه المخاطر، تتجلى أهمية تدخل القانون العام، سواء من خلال الرقابة الإدارية على البنية التحتية الرقمية، أو عبر تحديث الإطار التشريعي بما يضمن تحديد مسؤوليات واضحة للجهات المختصة بتأمين الشبكات، ووضع ضوابط صارمة لإدارة المعلومات، واعتماد بروتوكولات أمنية إلزامية، وفق المعايير العالمية للأمن السيبراني، كما يُفترض أن تواكب أجهزة الدولة تطور هذه الهجمات، من خلال بناء وحدات متخصصة في رصد التهديدات، والاستجابة السريعة لها، وتمكين القضاء الإداري من مساءلة الجهات المقصّرة أو المتهاونة في صيانة البنية الشبكية العامة.

ثالثًا: التهديدات التي تستهدف البيانات والمعلومات الرقمية

في قلب الثورة الرقمية التي تشهدها المؤسسات العامة، تمثل البيانات والمعلومات الرقمية العنصر الأثمن والأكثر عرضة للاستهداف من قبل المهاجمين السيبرانيين، فهذه المعلومات – التي تشمل الوثائق الرسمية، والمعاملات الإدارية، وبيانات المواطنين، ومراسلات الجهات الحكومية – أصبحت هي

[19] بن عربية رياض التهديدات اللاتماثلية في الفضاء السيبراني: حروب الجيل الرابع نموذجا، دفاتر البحوث العلمية، المجلد 10، العدد 1، 2022، ص 463.

[20] زهراء عماد محمد كلنتر، تكييف الهجمات السيبرانية في ضوء القانون الدولي، المرجع السابق، ص 52.

[21] شيخه حسين الزهراني، التعاون الدولي في مواجهة الهجوم السيبراني، مجلة جامعة الشارقة للعلوم القانونية، المجلد 17 ، العدد 1 يونيو 2020، ص 753-755

المادة الحيوية التي تُبنى عليها السياسات، وتُدار بها الشؤون العامة، وتتخذ على أساسها القرارات. ومن ثمّ، فإن أي تهديد يطال هذه البيانات، يُعد في حقيقته تهديدًا مباشرًا لأمن الدولة الإداري والسيادي.

تتنوع الهجمات التي تستهدف المعلومات بين السرقة الرقمية، والاعتراض غير المشروع للاتصالات، وتغيير أو إتلاف البيانات، بل وقد تصل إلى نشرها علنًا أو بيعها عبر شبكات مظلمة (Dark Web). وغالبًا ما يتم تنفيذ هذه الهجمات عبر وسائل تقنية متطورة، تشمل استغلال ثغرات أمنية في نظم التشغيل أو تطبيقات الإدارة، أو عبر زرع برامج تجسس داخل الأنظمة المؤسسية، أو حتى من خلال الخداع الإلكتروني (Phishing) الذي يستهدف الموظفين أنفسهم للحصول على كلمات المرور وبيانات الدخول، وتكمن خطورة هذه التهديدات في أنها تمسّ جوهر عمل الإدارة العامة، إذ أن اختراق قاعدة بيانات جهة حكومية واحدة يمكن أن يؤدي إلى تسرب كمّ هائل من المعلومات الحساسة، بما في ذلك ملفات المواطنين، أو قرارات إدارية داخلية، أو بيانات تتعلق بالأمن أو الاقتصاد، كما أن تعديل المعلومات أو محوها دون إذن قد يُنتج آثارًا قانونية باطلة، ويؤدي إلى تضليل الإدارات الأخرى التي تعتمد على هذه البيانات، مما يفتح الباب أمام الفوضى الإدارية والخلل التنظيمي.[22]

ومن أبرز الأمثلة على هذه التهديدات ما يُعرف بالهجمات الموجهة Targeted Attacks، والتي يتم فيها اختيار هدف محدد – كوزارة أو دائرة حيوية – وجمع معلومات أولية عنها، ثم شنّ هجوم رقمي مُحكم يستهدف التلاعب بسجلاتها أو سرقتها. وتزداد هذه الهجمات تعقيدًا عندما يُستخدم فيها الذكاء الاصطناعي في تحليل النمط السلوكي للعاملين داخل الجهة المستهدفة، لتحديد اللحظات المثلى للهجوم.

ومن الجدير بالذكر أن إحدى أخطر نتائج هذه التهديدات هي انتهاك خصوصية الأفراد وحقوقهم الرقمية، إذ يمكن للمهاجمين الاطلاع على معلومات طبية، أو مالية، أو قانونية، قد تُستخدم لاحقًا في الابتزاز أو التشهير أو التلاعب في الإجراءات القانونية، ما يحوّل الخرق الأمني من قضية تقنية إلى أزمة قانونية وإنسانية.

وهنا يبرز دور القانون العام بوصفه الضامن الأعلى لحماية الحقوق والحريات، في ضرورة أن ينظّم آليات التعامل مع البيانات الرقمية داخل الإدارات العامة، سواء من حيث تخزينها، أو تداولها، أو حمايتها، أو تحديد المسؤولية في حال تعرّضها للخطر، إذ ينبغي على النظام القانوني العام أن يفرض معايير دقيقة لحوكمة البيانات، ويُلزم الجهات العامة باعتماد بروتوكولات التشفير والتوثيق الرقمي، وتحديث أدوات الحماية بشكل دوري، كما يفترض أن يُخضع المخالفين للمساءلة الإدارية أو القضائية، سواء أكان الخطأ ناتجًا عن إهمال، أم عن خرق متعمّد.[23]

وفي السياق العراقي، ورغم بعض المبادرات الجزئية في تحديث البنية التقنية لبعض المؤسسات، إلا أن الحماية القانونية للبيانات لا تزال تعاني من قصور واضح في التشريع والرقابة، فلا يوجد قانون موحد يحدد طبيعة البيانات العامة، ولا جهة مركزية تشرف على أمنها، ما يجعل الكثير من الجهات عرضة للاختراق أو التسرب أو الضياع، كما أن ضعف الثقافة الرقمية لدى بعض العاملين، وعدم وضوح المسؤولية الإدارية عند وقوع الخرق، يُفرغ الإجراءات الأمنية من مضمونها، ويجعل القانون عاجزًا عن التفاعل الفعّال مع هذه الانتهاكات.

المبحث الثاني:

فاعلية أدوات القانون العام في التصدي للتهديدات السيبرانية

مع تعاظم الاعتماد على التكنولوجيا في مختلف مناحي الحياة، أصبح القانون العام يلعب دورًا محوريًا في وضع الإطارات القانونية والتنظيمية التي تحمي الفضاء السيبراني من التهديدات المتجددة والمعقدة، غير أن فاعلية هذه الأدوات القانونية لا تقتصر على مجرد سن التشريعات، بل تتعداها إلى مدى قدرتها على التطبيق العملي، والرقابة، وكذلك الاستفادة من التقنيات الحديثة التي تعزز من كفاءة التنفيذ، مثل آليات التقاضي عن بعد، لذلك، يهدف هذا المبحث إلى دراسة فاعلية أدوات القانون العام في التصدي للتهديدات السيبرانية من خلال مطلبين أساسيين، في المطلب الأول سيتم التركيز

[22] إبراهيم أحمد عبد السامرائي، الجريمة الالكترونية السيبرانية في القانون الدولي، المرجع السابق، ص 146.

[23] العيداني محمد، التهديدات السيبرانية وجرائم المعلومات، المرجع السابق، ص20.

على دور القانون العام في تنظيم وحماية الأمن السيبراني، مع بيان الآليات المتاحة والتحديات التي تواجه تطبيقها، مع تسليط الضوء على التجربة العراقية كمثال معاصر على ذلك، أما المطلب الثاني، فسيتناول دور التقاضي عن بعد كآلية حديثة تعزز من فعالية القانون العام، وتتيح سرعة الاستجابة والمرونة في مواجهة المخاطر السيبرانية، من خلال تيسير الوصول إلى العدالة وتحقيق الرقابة القضائية الفاعلة في بيئة رقمية متغيرة، كما يلي:

المطلب الأول:

القانون العام وحماية الأمن السيبراني_ آليات وتحديات

في العصر الرقمي، لم يعد القانون العام مجرد إطار تقليدي لتنظيم العلاقة بين الفرد والدولة أو لضبط سير المرافق العامة وفق مقتضيات المشروعية والمصلحة العامة، بل بات يواجه تحديًا مركبًا فرضته الطفرة التكنولوجية والتحولات السيبرانية التي تشق طريقها في صميم البنى الاجتماعية والاقتصادية والإدارية الحديثة. ولم يعد من الممكن مقاربة "الأمن" – ولا سيما في صورته السيبرانية – بمعزل عن الأسئلة الجوهرية التي تطرحها فلسفة القانون حول موقع الفرد من الدولة، وحدود السلطة، ومقدار ما ينبغي التضحية به من الحريات لصالح الحفاظ على النظام العام.[24]

إن جوهر القانون العام، في مبدئه الأصيل، ينبثق من فكرة الإرادة العامة التي تتجسد في القواعد التي تنظّم حياة الجماعة، وتضمن التوازن بين الحقوق والحريات، وتكرّس سيادة الدولة بوصفها الضامن الوحيد للأمن والاستقرار، غير أن هذا التوازن يهتز حين تدخل معادلة الأمن السيبراني على الخط، بوصفه أمنًا لا يتعلّق بالمجال الفيزيائي وحده، وإنما يشمل المجال المعلوماتي، أي فضاء البيانات والاتصالات والمعلومات الرقمية، وهو فضاء يتقاطع فيه الخاص والعام، الفردي والجماعي، المدني والسياسي، وهنا تبرز إشكالية قانونية وفلسفية معقدة: هل من حق الدولة أن تفرض إجراءات تشريعية وتنظيمية مشددة لضمان أمنها الرقمي، ولو على حساب حرية الأفراد في استخدام الفضاء السيبراني؟ وإذا كان القانون العام أداة الدولة في تنظيم الشأن العام، فهل يملك هذا القانون من المرونة والكفاءة ما يؤهله للتعامل مع تهديدات غير تقليدية، متحركة، ولا مادية بطبيعتها؟ وهل يبقى الفرد في هذه الحالة شريكًا في صياغة السياسات، أم مجرد موضوع للحماية والمراقبة؟

لا يمكن معالجة هذه الإشكاليات إلا من خلال فهم العلاقة الديناميكية بين مفهومي "القانون" و"الأمن". فكما تشير الدراسات القانونية المعاصرة، وخاصة تلك التي تنتمي إلى تيار "الدراسات النقدية للأمن"، فإن أمن الأفراد لا يتحقق بالضرورة من خلال تشديد السيطرة أو توسيع سلطة الدولة، بل من خلال تعزيز قدرتهم على التحكم في بياناتهم، وحماية خصوصيتهم، والمشاركة في صنع السياسات التي تمس حياتهم الرقمية. وفي المقابل، فإن القانون العام – الذي يستمد مشروعيته من مقولة تحقيق الصالح العام – ملزم بأن يُطوّع أدواته (القواعد، الهيئات، الإجراءات) لحماية المجال السيبراني الوطني من دون أن يتحول إلى أداة قمعية أو تقنية لتقييد الحريات باسم الأمن.[25]

وقد عرفت الدولة الحديثة – لا سيما في أطرها الغربية – تطورًا في فهم دور القانون العام بوصفه حارسًا للحقوق، وضابطًا للعلاقة بين الأمن والحرية. غير أن السياقات المختلفة، ومنها العراق والدول النامية، لا تزال تتأرجح بين مطلب الأمن السيبراني وبين هواجس الإفراط في ضبط الفضاء الرقمي بقوانين جزائية متشددة أو بهيئات تنفيذية تفتقر إلى الرقابة أو إلى الإطار القانوني الواضح، لا سيما في ظل إباحة التعامل القانوني الالكتروني بشكل واضح وصريح[26] وهنا يصبح القانون العام في حاجة إلى إعادة تعريف نفسه، لا بوصفه مجرد آلية لتنظيم الإدارة، بل كآلية لحوكمة المخاطر الجديدة في بيئة رقمية مفتوحة ومعقدة.[27]

---

[24] عزمي بشارة، مسألة الدولة: أطروحة في الفلسفة والنظرية والسياقات الدوحة / بيروت: المركز العربي للأبحاث ودراسة السياسات، 2023، ص 168–167.

[25] فايز محمد حسين، فلسفة القانون، دار المطبوعات الجامعية، القاهرة، 2007، ص 13

[26] نجد على سبيل المثال أن المشرع العراقي في المادة (88) من القانون المدني رقم (40) لسنة 1951 (34)، أجاز استعمال وسائل التكنلوجيا " يعتبر التعاقد (بالتلفون) أو بأية طريقة مماثلة كأنه تم بين حاضرين فيما يتعلق بالزمان وبين غائبين فيما يتعلق بالمكان"، كما نجد أن المشرع أجاز للقاضي الاستفادة من وسائل التقدم العلمي – دون حصرها – في استنباط القرائن القضائية، وهذا ما جاء واضحاً مباشراً كذلك في المادة (104) من قانون الأثبات رقم 107 لسنة 1979" للقاضي أن يستفيد من وسائل التقدم العلمي في استنباط القرائن القضائية"،

[27] عثمان سلمان غيلان العبودي، اثر التطور الالكتروني في مبادئ الوظيفة العامة، ط1، الناشر: صباح صادق جعفر الانباري، بغداد، ٢٠١١، ص ٧.

وعليه، فإن العلاقة بين القانون العام والأمن السيبراني ليست علاقة تبعية بل علاقة تأسيس وتفاعل. فالدولة لا تستطيع ضمان الأمن الرقمي من دون قاعدة قانونية صلبة وشفافة، تضع الحدود والحقوق، وتُعرّف بدقة نطاق السياسات السيبرانية، ومهام الهيئات المختصة، وحقوق الأفراد في المراقبة والمساءلة. بالمقابل، لا يمكن للأفراد الادعاء بحقوقهم الرقمية في فضاء غير منظّم، تسوده الفوضى التكنولوجية، أو يُترك فيه الأمن السيبراني رهينًا بالشركات الأجنبية ومراكز التحكم العالمية.

ومن هنا، تتحدد وظيفة القانون العام اليوم بوصفه الوسيط الأخلاقي والمؤسسي بين الأمن والحرية؛ فهو يسعى إلى تأمين بنية تحتية قانونية تشجع على تطوير تقنيات الحماية، من دون أن تسمح باستغلال هذه التقنيات في تقليص المجال العام، وهذا يتطلب رؤية جديدة تجعل من القانون العام أكثر انفتاحًا على المبادئ السيبرانية الحديثة: كالحق في التشفير، وحرية الوصول إلى المعلومات، وحماية البيانات الشخصية، والحوكمة المفتوحة.[28]

لقد أصبحت الدولة ملزمة – من خلال أدوات القانون العام – بأن تبني تصورًا جديدًا لمفهوم "السيادة"، لا يقتصر على الحدود الجغرافية، بل يشمل السيادة الرقمية، وهو مفهوم لا يمكن أن يتحقق من دون مشاركة المواطنين، وتحديث المنظومة التشريعية، وإنشاء هيئات متخصصة مستقلة، وربط الاستراتيجيات السيبرانية بالسياسات العامة لا بالأجهزة الأمنية فحسب، وفي هذا الإطار، تبدو التجربة العراقية مثالًا واضحًا على التحديات البنيوية التي تعوق فاعلية أدوات القانون العام في مجال الأمن السيبراني. فعلى الرغم من تزايد الوعي الرسمي بخطورة التهديدات الرقمية، إلا أن العراق ما يزال يفتقر إلى قانون وطني شامل ينظم أمن المعلومات وحماية الفضاء السيبراني، إذ يُعد غياب هذا القانون أحد أبرز مكامن الخلل التي تُفقد الدولة القدرة على التنظيم المسبق، وتُقيد حركتها في وضع استراتيجيات وقائية طويلة الأمد.[29]

فمشروع قانون الجرائم المعلوماتية، المطروح منذ أكثر من عقد، لا يزال يراوح مكانه في مجلس النواب دون أن يرى النور، مما يُبقي البيئة السيبرانية مفتوحة أمام الفوضى القانونية والتقنية، ويضعف الردع القانوني تجاه الجرائم الإلكترونية. كذلك، يلاحظ انعدام هيئة وطنية مستقلة للأمن السيبراني، ما يجعل التنسيق المؤسسي مشتتاً ومحدود الأثر، فالمحاولات القائمة مثل فريق الاستجابة السريعة التابع لمستشارية الأمن الوطني تفتقر إلى الاستقلالية القانونية، وتواجه تحديات تتعلق بالكفاءة والموارد والشرعية المؤسساتية، أما على المستوى التنظيمي، فتُعاني البنية الرقمية للدولة من ارتباطها بمنظومات وشبكات أجنبية، وضعف البنية التحتية السيادية، مما يُعقد عملية الحماية ويجعل السيادة السيبرانية معرضة للتدخل الخارجي، كما أن القطاع الخاص المحلي ومؤسسات الدولة ما تزال تفتقر إلى وعي تقني شامل حول ماهية التهديدات الرقمية، الأمر الذي يُعزز من هشاشة البيئة الرقمية ويُقلل من فرص التفاعل السريع مع الهجمات. [30]

ومع أن العراق أطلق ما يُعرف بـ"استراتيجية الأمن السيبراني" عام 2017 عبر فريق الاستجابة السريعة، فإن هذه الوثيقة ظلت نظرية الطابع، وعاجزة عن إحداث أثر مؤسسي حقيقي، فهي لم تتضمن توصيفاً عملياً واضحاً للجهات المسؤولة عن تنفيذ السياسات المقترحة، ولم تُرفق بخطط تنفيذية أو مؤشرات أداء قابلة للقياس، بل اكتفت بعبارات عمومية وصياغات فضفاضة، وهو ما يعكس بوضوح غياب الإرادة السياسية المؤطرة برؤية قانونية استراتيجية، كما أن الخلل لا يقف عند حدود البنية التشريعية أو التنظيمية، بل يمتد إلى ضعف القدرات البشرية المؤسسية في مجال الأمن السيبراني، فقلة الكوادر المتخصصة، وعدم دمج الأمن السيبراني ضمن الخطط التعليمية، ونقص البرامج التدريبية للموظفين الحكوميين، كلها تؤدي إلى تراجع الكفاءة الوقائية وضعف الاستجابة المؤسسية للأزمات.

ومن هنا، يتضح أن أدوات القانون العام في العراق رغم أهميتها النظرية ما تزال غير مفعّلة فعليًا، فالسياسات العامة تعاني من التجزئة، والتشريعات غائبة أو غير نافذة، والرقابة الإدارية لا تملك الأدوات الكافية لفرض الانضباط التقني، والبيئة المؤسسية تفتقر إلى التنسيق والاحترافية. وهذا ما يُبرز

[28] طارق بن عبد الله بن صالح العمر، احكام التقاضي الالكتروني، رسالة مقدمة لنيل درجة الدكتوراه في الفقه المقارن الى الجامعة الالمام محمد بن سعود الاسلامية – المعهد العالي للقضاء، قسم الفقه المقارن –١٤٣٠ – ص ٢

[29] مصطفى ابراهيم سلمان الشمري، الأمن السيبراني وأثره في الأمن الوطني العراقي، مجلة العلوم القانونية والسياسية، كلية القانون والعلوم السياسية جامعة ديالى ، المجلد 10 ، العدد 1، 2021 152

[30] باسم علي خريسان الامن في الفضاء السيبراني : دراسة في التهديدات واستراتيجية المواجهة مجلة كلية التراث الجامعة ، بغداد، المجلد 1 ، العدد 36 ، 2023، ص 23

الحاجة العاجلة إلى إصلاح شامل في منظومة الحوكمة السيبرانية من خلال مدونة تشريعية واضحة، وهيئات تنظيمية مستقلة، واستراتيجيات وطنية قابلة للتنفيذ، يكون فيها القانون العام أداة وقائية وتدبيرية أساساً، وليس مجرد استجابة لاحقة لوقوع الأذى.[31]

في إطار مواجهة التحديات التي تفرضها البيئة الرقمية، لا يمكن للقانون العام أن يظل جامدًا أو تقليديًا في أدواته، بل يجب أن يتخذ شكلاً ديناميكيًا يشمل منظومة متكاملة من التشريعات والإجراءات والمؤسسات التي تضمن حماية الفضاء السيبراني وتعزز أمنه، فالقانون العام يسعى إلى تنظيم الفضاء الرقمي عبر تشريعات متخصصة تتناول الجريمة الإلكترونية، وحماية البيانات الشخصية، وضبط عمل الهيئات السيبرانية الحكومية، إلى جانب تشريعات التوقيع الإلكتروني والمعاملات الرقمية، التي أصبحت حجر الأساس في المعاملات الرقمية المعاصرة. إلا أن الواقع العراقي يعكس حالة من النقص الواضح في هذا المجال، فبالرغم من وجود قانون التوقيع الإلكتروني رقم 78 لسنة 2012، إلا أن العراق يفتقر إلى قانون شامل للأمن السيبراني، ولا يزال مشروع قانون الجرائم الإلكترونية متوقفًا في البرلمان منذ عام 2011، مما يعكس ضعف الإرادة التشريعية في مواكبة التحديات الرقمية المتسارعة، ويترك البيئة القانونية هشة أمام التهديدات المتزايدة.[32]

أما على مستوى الهيئات والمؤسسات التنظيمية، فإن التجارب الدولية الناجحة تشير إلى أهمية وجود هيئات وطنية مستقلة وقوية تملك صلاحيات واضحة في إدارة الأمن السيبراني، كما هو الحال في "الهيئة الوطنية للأمن السيبراني" في المملكة العربية السعودية، أو "الوكالة الوطنية لأمن نظم المعلومات" في فرنسا، حيث تتمتع هذه الهيئات بالاستقلالية والموارد التي تمكنها من التصدي للتهديدات الرقمية بكفاءة. وعلى النقيض من ذلك، يشكو العراق من غياب مثل هذه الهيئات المستقلة، ويعتمد فقط على فريق الاستجابة السريعة التابع لمستشارية الأمن الوطني، وهو كيان يعاني من محدودية الغطاء القانوني وضعف الإمكانات وقلة الشفافية، مما يحول دون قيامه بدور فاعل وموثوق في حماية الأمن السيبراني الوطني.[33]

وبالانتقال إلى السياسات العامة والاستراتيجيات الوطنية، تُعد هذه الأدوات مرنة وضرورية لتوجيه الجهود الحكومية والمجتمعية نحو حماية الفضاء السيبراني، وقد أصدرت بعض الدول استراتيجيات سيبرانية واضحة المعالم تتضمن جداول زمنية محددة، وأهدافًا قابلة للقياس، وآليات تنفيذ واضحة، تعكس جدية الدولة في مواجهة التهديدات الرقمية. في المقابل، تكشف استراتيجية الأمن السيبراني العراقية الصادرة عام 2017 عن قصور كبير، إذ اقتصرت على 11 صفحة فقط، خالية من خطة تنفيذية أو إطار مؤسسي ملزم، بل وتم نشرها على موقع الاتحاد الدولي للاتصالات بدلاً من المنصات الرسمية العراقية، ما يثير تساؤلات مشروعة حول جديتها وفعاليتها، ويُظهر غياب التنسيق والتخطيط السليمين في هذا المجال الحيوي.[34]

ولا يقتصر دور القانون العام على سن التشريعات ووضع السياسات فحسب، بل يمتد إلى الرقابة الإدارية والشفافية، التي تُعد من أبرز أدوات الوقاية من التهديدات السيبرانية، فالرقابة الإدارية تفرض التزام المؤسسات الحكومية بتحديث نظمها وتأمين بياناتها بفعالية، كما تفرض مساءلة المسؤولين عند وقوع تسريبات أو خروقات رقمية ناجمة عن إهمال أو ضعف في إجراءات الحماية. وتكتمل هذه الصورة بالرقابة القضائية، وبخاصة عبر المحاكم الإدارية، التي يفترض أن تكون مؤهلة لمحاسبة الجهات المقصّرة في حماية البنى التحتية الرقمية، رغم أن هذا الدور لا يزال محدودًا في العراق، ويواجه عراقيل عديدة، منها ضعف الإطار القانوني وقلة التخصص القضائي في المجال السيبراني، حيث أن هذا الواقع المعقد لا يخلو من معوّقات عديدة تحدّ من فاعلية أدوات القانون العام في العراق، من بينها غياب الإرادة التشريعية لتمرير قوانين سيبرانية حديثة، وضعف التنسيق بين الجهات الأمنية والإدارية المختلفة، فضلاً عن قلة الوعي لدى الموظفين العموميين بمخاطر الفضاء الرقمي، وهو أمر يُضعف الجهود الوقائية ويزيد من فرص وقوع الخروقات،

---

[31] ظفر عبد مطر التميمي، العراق والأمن السيبراني ... الفرص والتحديات، مجلة واسط للعلوم الانسانية والاجتماعية، جامعة واسط العراق، المجلد 18 ، العدد 51 ، 2022 ، ص 11-12.

[32] وفي جلسته بتاريخ 21 نوفمبر / 2023 طرح البرلمان العراقي مشروع قانون جرائم المعلوماتية، بعد فشل دورات المجلس السابقة في إقراره خلال العقد المنصرم، وعلى الرغم من التعديلات المتكررة على مشروع القانون، ومع التأكيد على أهمية تنظيم عملية التواصل الالكتروني خصوصاً وأن العراق تأخر كثيراً في سن تشريع، ذلك القانون الذي تضمن 31 مادة يعود إلى عام 2011، فقد نصت المادة السادسة من القانون على يعاقب كل من حاول استخدام شبكة المعلومات لتكدير الأمن والنظام العام بالسجن المؤبد أو بغرامة تتراوح بين (25) و (50) مليون دينار عراقي، أما المادة الثانية والعشرون تنص على الحبس لمدة سنتين ودفع غرامة لا تقل عن مليوني دينار ولا تزيد على خمسة ملايين دينار، لمن نسب إلى الغير عبارات أو أصوات أو صوراً تنطوي على القذف والسب من خلال شبكة المعلومات، وقد تم سحب ذلك المشروع من قبل الحكومة، لغرض إضافة بعض التعديلات عليه . انظر : عمر العجلوني، لماذا يجب تعديل مشروع قانون الجرائم المعلوماتية في العراق على الموقع الالكتروني https://euromedmonitor.org/index.php/ar/article5498/ تاريخ الزيارة: 2025/7/14.

[33] مروان سالم العلي التحديات الاستراتيجية للأمن الوطني العراقي في ظل المتغيرات الدولية، مجلة تكريت للعلوم السياسية، العراق، المجلد 2، العدد 20، 2020، ص 57

[34] حازم حمد موسى الرؤيا الاستراتيجية للأمن الوطني العراقي في الفضاء السيبراني مقاربة بين المعضلة الأمنية والمكنة الأدائية، المجلة الجزائرية للعلوم القانونية والسياسية، الجزائر، المجلد 57 العدد 5 2020، ص557.

إلى جانب ذلك، يرتبط الإنترنت العراقي بشبكات خارجية، مما يقلل من قدرة الدولة على السيطرة الكاملة على مجالها السيبراني، ويعزز من مخاطر التدخل الخارجي. كما أن غياب الحوكمة الرقمية الفعالة للمؤسسات العامة يفاقم من هذه التحديات، إذ تظل المؤسسات رهينة لأنظمة غير متكاملة وممارسات غير منظمة، مما يُضعف من قدرتها على حماية بنيتها الرقمية الحيوية.[35]

بناءً على ذلك، يظهر أن تفعيل أدوات القانون العام في مواجهة التهديدات السيبرانية يتطلب رؤية شاملة ومتكاملة، تبدأ بتطوير تشريعات مرنة ومتطورة تلائم طبيعة التهديدات الرقمية، وتستمر بإرساء هيئات تنظيمية مستقلة ومؤهلة، ووضع استراتيجيات وطنية واضحة قابلة للتنفيذ والمتابعة، وصولاً إلى تعزيز الرقابة الإدارية والقضائية، وزيادة الوعي والتدريب في أوساط العاملين في القطاع العام. وهذا المسار لا يتحقق إلا بإرادة سياسية حقيقية ورؤية قانونية حديثة تعي أهمية السيادة الرقمية، وتحترم حقوق الأفراد الرقمية، وتوازن بين متطلبات الأمن والحرية في عالم معولم ومعقد.

المطلب الثاني:

دور التقاضي عن بعد في تعزيز فعالية القانون العام في مواجهة التحديات السيبرانية.

في إطار سعي الدول إلى تحديث نظمها الإدارية والقضائية لمواكبة متطلبات العصر الرقمي، برزت نماذج جديدة من الممارسات المؤسسية، لم تعد تقتصر على تقديم الخدمات الإدارية عبر الإنترنت، بل امتدّ أثرها إلى عمق العمل القضائي ذاته، ومن أبرز هذه النماذج نظام "التقاضي عن بُعد"، وقد فرض هذا النمط القضائي المستحدث واقعًا قانونيًا وتقنيًا جديدًا يتقاطع فيه المرفق العام مع البيئة الرقمية، ويتشابك فيه الحق في التقاضي مع التحديات السيبرانية.[36]

وجديرٌ بالذكر أن المرافق القضائية تُعد من أهم المرافق العامة التي ترتبط بمصير الأفراد وحقوقهم، ويتطلب إدارتها مستوى عالياً من الأمان والموثوقية، ومع انتقال هذه المرافق إلى النمط الرقمي، أصبحت أكثر عرضة لتهديدات مثل الهجمات على البنية التحتية القضائية، أو تسريب وثائق القضايا، أو التشويش على الجلسات، أو انتحال صفة أحد أطراف الدعوى، وتزداد الخطورة في القضايا الحساسة مثل القضايا الجنائية أو النزاعات الإدارية أو القضايا التي تمس الأمن القومي أو النظام العام، في هذا السياق، يطرح التقاضي عن بُعد إشكاليات جوهرية على مستوى القانون العام، تتصل بمفاهيم المشروعية، وضمانات المحاكمة العادلة، والرقابة على عمل المرافق العامة. فالدولة، بصفتها صاحبة السيادة، ملزمة دستوريًا بتوفير نظام قضائي يضمن حياد القاضي، وحقوق الدفاع، وسرية البيانات، وسلامة الإجراءات، وهو ما قد يتعرض للتقويض بفعل ثغرة إلكترونية أو خلل في النظام، الأمر الذي يفرض على الإدارة العامة – والسلطة التشريعية – مسؤولية مضاعفة في صياغة أطر قانونية مرنة ومواكبة، فلم يعد العمل القضائي، كما كان في السابق، مقصورًا على قاعات المحاكم، بل أصبح ينفَّذ جزئيًا أو كليًا عبر الوسائط الرقمية، من خلال جلسات تنعقد بالصوت والصورة، ومنصات إلكترونية تُستعمل لتقديم المرافعات، وتبادل المذكرات، وإصدار القرارات، وهذا التحوّل، وإن حمل وعودًا بتيسير الوصول إلى العدالة، وتقليص أمد النزاع، وتحقيق كفاءة مؤسسية، إلا أنه في الوقت ذاته كشف عن هشاشة رقمية كامنة في البنية القضائية للدول، لا سيما عندما تُفتقر إلى حماية قانونية وتقنية كافية تضمن سلامة هذه الإجراءات وعدالتها، كما أن التقاضي الإلكتروني، بوصفه مظهرًا من مظاهر رقمنة القضاء، يُمثّل في جوهره اندماجًا مباشرًا بين مرفق عام تقليدي – هو القضاء – وبيئة سيبرانية مفتوحة ومعرّضة للانتهاك، وهذا ما يجعل من أمن المعلومات القضائية تحديًا مزدوجًا، يتعلق من جهة بحماية حق الأفراد في الخصوصية والمشاركة الفعالة في إجراءاتهم، ومن جهة أخرى بالحفاظ على هيبة السلطة القضائية وضمان مشروعية وسلامة أحكامها.[37]

وتزداد أهمية هذه الإشكالية في ظل ما شهده العالم – والعراق من ضمنه – من محاولات لاعتماد التقاضي عن بُعد، خاصة في فترات الطوارئ (كجائحة كوفيد–19)، أو في مناطق تشهد ضعفًا في البنية القضائية المادية، فقد اتضح من التجربة أن البنية الرقمية وحدها لا تكفي، ما لم تُدعّم

---

[35] ظفر عبد مطر التميمي، العراق والأمن السيبراني _ الفرص والتحديات، المرجع السابق، ص 11–12.

[36] د. صفاء أوتاني، المحكمة الالكترونية المفهوم والتطبيق– بحث منشور في مجلة الجامعة دمشق للعلوم الاقتصادية والقانونية المجلد ٢٨ العدد الاول– ٢٠١٢ – ص ١٧٠.

[37] د. اكرم فاضل سعيد، حماية قواعد البيانات من مخاطر التنازل عنها والمنافسة غير المشروعة الواقعة عليها محاضرات غير مطبوعة القيت على طلبة الدراسات العليا (الماجستير) قسم القانون الخاص في كلية الحقوق جامعة النهرين للعام الدراسي ٢٠١٣–٢٠١٤.

بأطر قانونية واضحة تُنظّمها وتضع ضمانات ضد اختراقها والتلاعب ببياناتها، وتُحمّل الجهات العامة مسؤولياتها القانونية في حال وقوع خرق سيبراني يؤدي إلى إبطال إجراءات أو تسريب بيانات، من هنا، فإن التقاضي عن بُعد لا يُعدّ مجرد تجربة تقنية طموحة، بل هو نموذج واقعي يُجسّد طبيعة العلاقة المستجدة بين القانون العام ومخاطر الفضاء الرقمي، ويطرح تساؤلات جوهرية حول مدى نجاعة القواعد الإدارية والدستورية في التعامل مع هذا النمط الجديد من العمل القضائي، خاصة إذا ما وقعت هجمات إلكترونية تستهدف البنية التحتية القضائية، أو تم اعتراض مجريات المحاكمة، أو تم اختراق خصوصية المتقاضين، وهي ممارسة قضائية حديثة تنطوي على استخدام تقنيات الاتصال المرئي والصوتي، ومنصات إلكترونية لإدارة الدعوى القضائية، من تسجيلها حتى إصدار الحكم، دون الحاجة إلى حضور الأطراف فعليًا داخل قاعات المحاكم.

إلا أن هذا التطور، وإن كان يحمل مزايا إدارية وقانونية واضحة، يُمثّل في الوقت ذاته مدخلًا جديدًا للتهديدات السيبرانية، لا سيّما في البيئات التي لا تمتلك بنية معلوماتية مؤمّنة، أو تشريعات ناضجة تنظم هذا النوع من التقاضي الذي يتطلب تشغيل منظومة تقنية معقّدة، تشمل أدوات التصوير والبث، وإدارة البيانات القضائية، والتحقق من الهوية الرقمية، وضمان سرية الجلسات، وهي كلها عناصر قد تصبح هدفًا للقرصنة أو الاختراق أو العبث.

إن التقاضي عن بُعد، حتى وإن بدا خيارًا استراتيجياً في ظل الطوارئ الصحية أو الكوارث الطبيعية أو لتعزيز الوصول إلى العدالة في المناطق النائية، إلا أنه لا يجب أن يُختزل إلى مجرد حلّ تقني، بل لا بد أن يُؤسس له تشريعيًا وتنظيميًا، ويجب أن يتم بناء هذه القاعدة على ثلاثة أركان رئيسية: أولها، وجود تشريع واضح يُحدد نطاق هذا النوع من التقاضي، وشروط استخدامه، وضمانات صحته القانونية. ثانيها، توفير بنية تحتية رقمية مؤمّنة ومحمية من الاختراق، عبر اعتماد أنظمة تشفير قوية، وتحديث دوري للبرمجيات، وتدريب للكوادر الفنية. وثالثها، الرقابة القضائية والإدارية الفاعلة، لضمان عدم التلاعب في محتوى الجلسات أو نتائج المحاكمات.[38]

وفي هذا الإطار، يمكن القول إن تجربة العراق لا تزال في طور التأسيس في مجال التقاضي عن بعد، رغم إقرار بعض القوانين التي تمهد لهذا النمط من الإجراءات، فقد شرّع المشرّع العراقي قانون التوقيع الإلكتروني والمعاملات الإلكترونية رقم (78) لسنة 2012، والذي يُعدّ لبنة أولى في تمهيد الطريق نحو التحول الرقمي، كما أجاز في قوانين أخرى استخدام الوسائل الإلكترونية في العقود والمعاملات التجارية، وهو ما يؤشر إلى وجود وعي تشريعي تدريجي تجاه البيئة الرقمية، إلا أن المرفق القضائي لا يزال يفتقر إلى منظومة متكاملة تُمكنه من الانتقال الآمن والفعّال نحو التقاضي الإلكتروني الكامل، سواء من حيث التشريع، أو البنية التحتية، أو تدريب الكوادر القضائية والإدارية، وعلى المستوى الأمني، يمثل غياب قانون خاص بالأمن السيبراني في العراق فجوة كبيرة في حماية البيانات والمراسلات القضائية، ما قد يسمح بتدخلات غير مشروعة في النظام القضائي الرقمي، أو نشر بيانات حساسة، أو التأثير على مسار العدالة. إن التهديدات السيبرانية في هذا السياق لا تعني فقط التخريب التقني، بل تشمل أيضاً زعزعة ثقة المواطن في نزاهة القضاء، وهو أمر بالغ الخطورة في مجتمع يسعى إلى ترسيخ دولة القانون والمؤسسات.[39]

ومن ثم، فإن التقاضي عن بُعد يجب أن يُفهم في إطار أشمل، باعتباره ساحة تطبيقية تواجه فيها الدولة تحدياً حقيقياً في موازنة أمرين: تحديث خدماتها القضائية بما يواكب متطلبات العصر، وضمان عدم التنازل عن المبادئ الدستورية الراسخة، مثل ضمان حق الدفاع العادل، وحماية خصوصية البيانات، واستقلال القضاء. وتفرض هذه المعادلة تحديًا مزدوجًا على القانون العام: أن يُعطي الإدارة القضائية ما يكفي من المرونة لتبنّي الحلول التقنية، دون أن يُفرّط في آليات الرقابة والمساءلة.

وأخيرا يمكن لنا متابعة التشريعات العراقية من خلال منظومة قوانين صدرت في اوقات متفاوتة و كما يلي:

1 -اجازت المادة (88) من القانون المدني العراقي رقم 40 لسنة 1951 المعدل سالفة الذكر التعاقد بالتلفون او باي طريقة مماثلة وهو اعتراف صريح بالتعاقد الالكتروني والتعبير عن الارادة بتلك الوسيلة والاشارة ضمناً الى ما سيظهر من وسائل مماثلة ومتطورة لاحقاً .

[38] م نافع بحر سلطان، الاختصاص القضائي الالكتروني للمحاكم العراقية، بحث منشور في مجلة جامعة تكريت للعلوم القانونية و السياسية, العدد /3, السنة الأولى، ص16.
[39] مروان سالم العلي التحديات الاستراتيجية للأمن الوطني العراقي في ظل المتغيرات الدولية، المرجع السابق، ص 66.

2 -اجازت المادة (104) من قانون الاثبات العراقي رقم (107) لسنة 1979 المعدل بالقانون رقم (46) لسنة 2000 (للقاضي ان يستفيد من وسائل التقدم العلمي في استنباط القرائن القضائية) فنطاق الاثبات بالقرينة القضائية محدد بأثبات الوقائع المادية والتصرف القانوني الذي لا تزيد قيمته على خمسة الاف دينار (وهو مبلغ زهيد قياسا الى قيمة الدينار العراقي في ضوء التضخم النقدي) و وجود مبدأ الثبوت بالكتابة وقيام المانع من الحصول على دليل كتابي وفقدان السند الكتابي بسبب اجنبي , وأثبات الغش و الاحتيال في التصرف القانوني.

3 -أجازت المادة (19) من قانون التجارة رقم (30) لسنة 1983 المعدل الاستعانة بالأجهزة التقنية الحديثة عوضا عن الدفاتر التجارية الاختيارية. .

4 -أقر المشرع العراقي في قانون النقل رقم (80) لسنة 1983 المفهوم الواسع للتوقيع صراحة حيث أجازت المادة (142/ رابعا) من هذا القانون توقيع سند الشحن بخط اليد أو بأية طريقة أخرى مقبولة.

5 -أجازت المادة (2/38) من قانون المصارف رقم (40) لسنة 2003 ثم المادة (2/38) من قانون المصارف رقم (94) لسنة 2004 احتفاظ المصرف بالسجلات بصورة خطية ولأي مصرف ان يحتفظ بالدفاتر والسجلات والبيانات و المستندات و المراسلات و البرقيات و الإشعارات و المستندات الأخرى المتعلقة بأنشطته المالية بشكل مصغر الميكروفيلم أو خزن البيانات إلكترونيا او الوسائل التكنلوجية المعاصرة الأخرى بدلا من الاحتفاظ بشكلها الأصلي طيلة المدة المحددة في القانون بقدر ما تتوفر نظم و إجراءات وافية لاسترجاع نفس مفعول الأصل من حيث الأثبات وللبنك المركزي أن يصدر لائحة تحدد المتطلبات المفصلة لتلك النظم.

6 -المادة (21) من النظام الداخلي اكدت على ان لأجراء سير العمل في المحكمة الاتحادية العليا رقم (30) لسنة 2005 أجراء التبليغات بوساطة البريد الالكتروني والفاكس والتلكس اضافة لوسائل التبليغ الاخرى المنصوص عليها في قانون المرافعات المدنية (57) والمنشور في الوقائع العراقية بالعدد 3997 في 2005/5/20.

7 -عرفت المادة (68/ أولا) من مشروع قانون الملكية الفكرية المعدل عام 2006 الدائرة المتكاملة بأنها (كل منتج يؤدي وظيفة الكترونية ويتكون من مجموعة من العناصر المتصل بعضها ببعض أحدها في الأقل عنصر نشط بحيث تتشكل هذه العناصر فيما بينها من وصلات ضمن جسم مادي معين أو عليه سواء أكان المنتج مكتملا أو في أي مرحلة من مراحل انتاجه) ونصت المادة (68/ثانيا) من المشروع على أنه (يجوز استعمال الحاسوب لتسجيل التصاميم والبيانات المتعلقة بها وتكون البيانات و الوثائق المستخرجة منه المصدقة من المسجل حجة على الغير ما لم يثبت صاحب الشأن عكسها) وأجازت المادة (151/ثالثا) من المشروع استعمال الحاسوب الالي لتسجيل الأسماء والبيانات المتعلقة بها وتكون البيانات و الوثائق المستخرجة منه والمصدقة من المسجل حجة على الكافة ما لم يثبت صاحب الشأن عكسها (وبرامج الحاسوب المشمولة بالحماية هي المفاتيح أو الأدوات أو اللغات المستخدمة في أنتاج برامج الويب والعمليات الأخرى التي تصنف على اساس كونها برامج حاسوب (م163).

8 -صدر قانون التوقيع الإلكتروني والعاملات الإلكترونية رقم (78) لسنة 2012 ونشر في الجريدة الرسمية بعددها المرقم (4256) في 2012/11/5 , وعرف الكتابة الإلكترونية بأنها (كل حرف أو رقم او رمز أو أية علامة أخرى تثبت على وسيلة الكترونية أو رقمية أو ضوئية أو أية وسيلة أخرى مشابهة وتعطي دلالة قابلة للأدراك والفهم) (م1 خامسا) وعرفت المعاملات الإلكترونية بأنها (الطلبات والمستندات والمعاملات التيش تتم بوسائل الإلكترونية) (م1/ سادسا) والمستندات الإلكترونية بأنها (المحررات والوثائق التي تنشأ أو تدمج أو تخزن أو ترسل أو تستقبل كليا أو جزئيا بوسائل إلكترونية بما في ذلك تبادل البيانات الكترونيا أو البريد الإلكتروني أو البرق او التلكس أو النسخ البرقي ويحمل توقيعا إلكترونيا) (م1/تاسعا).

الخاتمة:

في ختام هذا البحث، يتضح جليًا أن أمن المعلومات في العصر الرقمي لم يعد قضية تقنية فحسب، بل تحول إلى موضوع قانوني واجتماعي مركب يتطلب تأطيرًا قانونيًا متطورًا يستجيب لتحديات الفضاء السيبراني المتسارعة. وفي هذا السياق، تبرز أهمية أدوات النظام العام كركيزة أساسية لضمان توازن فعال بين حماية الأمن السيبراني والحفاظ على الحقوق والحريات الأساسية للأفراد، فهذه الأدوات لا تقتصر على فرض الضوابط وتنظيم العلاقات

بين الدولة والمجتمع فحسب، بل تمتد لتشكل الإطار القانوني والمؤسسي الذي يمكن من خلاله مواجهة التهديدات الرقمية بكفاءة وشفافية، مع الحفاظ على السيادة الرقمية وضمان المساءلة والرقابة. وبذلك، يصبح النظام العام ليس مجرد قاعدة صلبة تفرض النظام، بل منظومة متكاملة تواكب التحولات التقنية والاجتماعية، وتعزز قدرة الدولة على حماية أمنها ومصالحها العامة في فضاء متغير ومتسارع.

وقد اتضح من الدراسة مجموعة من النتائج، نذكر منها:

1. إن مفهوم أمن المعلومات في البيئة الرقمية يمتد ليشمل أبعادًا تقنية وقانونية واجتماعية وإدارية، مما يفرض ضرورة تحديث القوانين والإجراءات لتواكب هذه الطبيعة المتعددة الأوجه للأمن السيبراني.
2. هناك قصور تشريعي واضح في العراق نتيجة غياب قانون شامل للأمن السيبراني وضعف الهيئات التنظيمية المستقلة، مما يعيق قدرة الدولة على مواجهة التهديدات الرقمية وحماية الفضاء السيبراني الوطني.
3. ثبت أن دمج التقاضي عن بعد في النظام القضائي يسهم بشكل فاعل في تعزيز سرعة وكفاءة معالجة القضايا المتعلقة بالأمن السيبراني، بشرط وجود أُطر قانونية متينة وبرامج تدريبية متخصصة للقضاة والفاعلين.
4. أكدت الدراسة أن حماية الحقوق الرقمية للأفراد مثل الخصوصية وحرية الوصول إلى المعلومات يجب أن تكون جزءًا لا يتجزأ من استراتيجية الأمن السيبراني، لتجنب تحوّل إجراءات الحماية إلى أدوات قمعية تحد من الحريات.
5. لوحظ ضعف في الموارد البشرية المؤهلة والتنسيق المؤسسي بين الجهات المعنية في العراق، مما ينعكس سلبًا على فاعلية أدوات القانون العام في التصدي للتهديدات السيبرانية ويبرز الحاجة إلى تعزيز القدرات المؤسسية والبشرية.

وفي الختام يوصي الباحث بمجموعة من التوصيات، أبرزها:

1. ضرورة إصدار قانون شامل للأمن السيبراني يواكب التطورات التقنية ويرسخ مبادئ حماية الحقوق الرقمية، مع وضع ضوابط واضحة للجهات المختصة وصلاحياتها.
2. هناك حاجة ماسة إنشاء هيئات تنظيمية مستقلة ذات صلاحيات واضحة وموارد كافية لإدارة الأمن السيبراني على المستوى الوطني، بما يضمن التنسيق الفعّال بين مختلف الجهات الحكومية والخاصة.
3. لزوم تطوير وتفعيل آليات التقاضي عن بعد في القضايا السيبرانية من خلال سن تشريعات داعمة، وبرامج تدريبية مستمرة للقضاة والعاملين في النظام القضائي لضمان التطبيق الأمثل.
4. ضرورة تعزيز الثقافة الأمنية والوعي لدى الموظفين العموميين والعاملين في القطاعين العام والخاص حول مخاطر الأمن السيبراني وأهمية اتباع أفضل الممارسات في حماية البيانات.
5. لا بد من اعتماد استراتيجية وطنية شاملة للأمن السيبراني تحتوي على خطط تنفيذية واضحة ومؤشرات أداء قابلة للقياس، مع إشراك مختلف القطاعات الحكومية والمجتمعية.
6. تعزيز التعاون بين العراق والدول والمنظمات الدولية المتخصصة في الأمن السيبراني لتبادل الخبرات ومواجهة التهديدات العابرة للحدود بفعالية، والاستثمار في بناء القدرات البشرية من خلال إدماج الأمن السيبراني في المناهج التعليمية، وتوفير برامج تدريب وتأهيل متقدمة للكوادر المختصة، مما يسهم في رفع مستوى الجاهزية المؤسسية.

ومن هنا، نأمل أن يكون هذا البحث قد أسهم في إلقاء الضوء على جوانب مهمة من هذه القضية المعاصرة، وأن يفتح آفاقًا جديدة للنقاش والتطوير في مجالات التشريع، والسياسات، والمؤسسات التي تعنى بحماية الأمن السيبراني، كما نرجو أن تساهم هذه الدراسة في دعم جهود الباحثين وصناع القرار والمهتمين، ليس فقط في المجال القانوني، بل في كل المجالات ذات الصلة، لما لها من أثر بالغ في تعزيز بيئة رقمية آمنة ومستقرة تُتيح للناس فرص الابتكار والتقدم، وتحميهم من المخاطر التي قد تهددهم في هذا العالم الافتراضي الواسع.

وفي النهاية، لا يسعنا إلا أن نتطلع إلى مستقبلٍ يزدهر فيه القانون والأمن السيبراني جنبًا إلى جنب، بحيث يُصاغ قانون عام حديث يواكب العصر، ويُبنى على أسس قوية من العدالة والشفافية، ويضمن بيئة رقمية تحترم حقوق الإنسان وتدعم التنمية المستدامة. وهذا هو الأمل الذي يحملنا لمزيد من البحث والعمل، لأن حماية أمن المعلومات ليست فقط مسألة تقنية أو قانونية، بل هي مهمة حضارية تتطلب تكاتف الجميع.

قائمة المراجع:

أولاً: القرآن الكريم

ثانياً: القوانين والتشريعات:

القانون المدني العراقي رقم (40) لسنة 1951.

قانون الأثبات رقم 107 لسنة 1979.

قانون التجارة رقم (30) لسنة 1983 المعدل.

قانون النقل رقم (80) لسنة 1983.

قانون المصارف رقم (40) لسنة 2003 .

قانون المصارف رقم (94) لسنة 2004 .

قانون المرافعات المدنية رقم (57) لعام 2005.

مشروع قانون الملكية الفكرية المعدل عام 2006.

قانون التوقيع الإلكتروني والعاملات الإلكترونية رقم (78) لسنة 2012.

ثالثاً: المراجع اللغوية:

1. ابن منظور، محمد بن مكرم، لسان العرب، ط1 دار صادر، ج1، بيروت، لبنان،2000.
2. روحي البعلبكي، قاموس المورد، ط7، دار العلم للملايين، بيروت، 1995.
3. الزبيدي، مرتضى بن محمد. تاج العروس من جواهر القاموس، تحقيق مجموعة من العلماء، إشراف عبد الستار أحمد فراج، الكويت: وزارة الأوقاف والشؤون الإسلامية، 1399هـ / 1979م، ج34.
4. شعبان عبد العاطي عطية واخرون، المعجم الوسيط، ط 4، مكتب الشروق الدولية" مجمع اللغة العربية"، مصر، 2004.

رابعاً: الكتب والدراسات القانونية:

1. اكرم فاضل سعيد، حماية قواعد البيانات من مخاطر التنازل عنها والمنافسة غير المشروعة الواقعة عليها محاضرات غير مطبوعة القيت على طلبة الدراسات العليا (الماجستير) قسم القانون الخاص في كلية الحقوق جامعة النهرين للعام الدراسي ٢٠١٣-٢٠١٤.
2. طارق بن عبد الله بن صالح العمر، احكام التقاضي الالكتروني، رسالة مقدمة لنيل درجة الدكتوراه في الفقه المقارن الى الجامعة الالمام محمد بن سعود الاسلامية – المعهد العالي للقضاء، قسم الفقه المقارن -١٤٣٠.
3. عثمان سلمان غيلان العبودي، اثر التطور الالكتروني في مبادئ الوظيفة العامة، ط1، الناشر: صباح صادق جعفر الانباري، بغداد، ٢٠١١.
4. عزمي بشارة، مسألة الدولة: أطروحة في الفلسفة والنظرية والسياقات الدوحة / بيروت: المركز العربي للأبحاث ودراسة السياسات، 2023.
5. فايز محمد حسين، فلسفة القانون، دار المطبوعات الجامعية، القاهرة، 2007.
6. محمد السعيد خشبة، نظم المعلومات الإدارية، دار النشر للجامعات، القاهرة، 2008.
7. منى جبور الاشقر، السيبرانية هاجس العصر، المركز العربي للبحث القانونية والقضائية، بيروت، 2017، لبنان.

خامساً: المجلات والدوريات:

1. إبراهيم أحمد عبد السامرائي، الجريمة الالكترونية السيبرانية في القانون الدولي، مجلة جامعة جيهان أربيل للعلوم الإنسانية والاجتماعية، المجلد 6، العدد 2، 2022.
2. أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، المجلد 8، العدد 4، كلية القانون، جامعة بابل، العراق 2016.
3. إسراء شريف جيجان، الأمن السيبراني الصيني_ دراسة في الدوافع والتحديات، قضايا سياسية، العدد 56.
4. باسم علي خريسان الامن في الفضاء السيبراني : دراسة في التهديدات واستراتيجية المواجهة مجلة كلية التراث الجامعة ، بغداد، المجلد 1 ، العدد 36 ، 2023.
5. بن عربية رياض التهديدات اللاتماثلية في الفضاء السيبراني: حروب الجيل الرابع نموذجا، دفاتر البحوث العلمية، المجلد 10، العدد 1، 2022.
6. ج. رضوان، الأمن السيبراني، أولوية في استراتيجيات الدفاع، مجلة الجيش، مؤسسة المنشورات العسكرية، الجزائر، العدد 603، جانفي.
7. حازم حمد موسى الرؤيا الاستراتيجية للأمن الوطني العراقي في الفضاء السيبراني مقاربة بين المعضلة الأمنية والمكنة الأدائية، المجلة الجزائرية للعلوم القانونية والسياسية، الجزائر، المجلد 57 العدد 5 2020.

8. رزق أحمد سمودي، حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون الدولي العام، مجلة جامعة الشارقة للعلوم القانونية، المجلد 15، العدد 2، ديسمبر 2018.
9. رعد خضير صليبي، تعزيز الأمن السيبراني في العراق: التحديات والفرص، مجلة دراسات دولية، العدد تسعة وتسعون، 2024.
10. زهراء عماد محمد كلنتر، تكييف الهجمات السيبرانية في ضوء القانون الدولي، مجلة الكوفة للعلوم القانونية والسياسية، 2020 المجلد 1، العدد 44/1، 2020.
11. شيخه حسين الزهراني، التعاون الدولي في مواجهة الهجوم السيبراني، مجلة جامعة الشارقة للعلوم القانونية، المجلد 17 ، العدد 1 يونيو 2020.
12. صفاء أوتاني، المحكمة الالكترونية المفهوم والتطبيق– بحث منشور في مجلة الجامعة دمشق للعلوم الاقتصادية والقانونية المجلد ٢٨ العدد الاول– ٢٠١٢.
13. ظفر عبد مطر التميمي، العراق والأمن السيبراني، الفرص والتحديات، مجلة واسط للعلوم الانسانية والاجتماعية، جامعة واسط العراق، المجلد 18 ، العدد 51 ، 2022.
14. العيداني محمد، التهديدات السيبرانية وجرائم المعلومات، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد 13، العدد 01، 2024.
15. مروان سالم العلي التحديات الاستراتيجية للأمن الوطني العراقي في ظل المتغيرات الدولية، مجلة تكريت للعلوم السياسية، العراق، المجلد 2، العدد 20، 2020.
16. مصطفى ابراهيم سلمان الشمري، الأمن السيبراني وأثره في الأمن الوطني العراقي، مجلة العلوم القانونية والسياسية، كلية القانون والعلوم السياسية جامعة ديالى، المجلد 10، العدد 1، 2021.
17. مصطفى ابراهيم سلمان الشمري، الأمن السيبراني وأثره في الأمن الوطني العراقي، مجلة العلوم القانونية والسياسية، كلية القانون والعلوم السياسية جامعة ديالى ، المجلد 10 ، العدد 1، 2021.
18. نافع بحر سلطان، الاختصاص القضائي الالكتروني للمحاكم العراقية، بحث منشور في مجلة جامعة تكريت للعلوم القانونية و السياسية, العدد /3, السنة الأولى.

سادساً: المراجع الالكترونية:

عمر العجلوني، لماذا يجب تعديل مشروع قانون الجرائم المعلوماتية في العراق على الموقع الالكتروني /https://euromedmonitor.org/index.php/ar/article5498 تاريخ الزيارة: 2025/7/14.

ص3 – كتاب تفسير القرآن الكريم أسامة سليمان – تعريف العلم لغة واصطلاحا – المكتبة الشاملة تاريخ الاطلاع 2025/7/10.

الرابط: أمن المعلومات: مفهومه وأهميته وعناصره تاريخ الاطلاع 2025/7/11.

References List:

First: The Holy Qur'an

Second: Laws and Legislation:

- Iraqi Civil Code No. (40) of 1951.
- Evidence Law No. 107 of 1979.
- Commercial Law No. (30) of 1983 (amended).
- Transport Law No. (80) of 1983.
- Banking Law No. (40) of 2003.
- Banking Law No. (94) of 2004.
- Civil Procedures Law No. (57) of 2005.
- Draft Amended Intellectual Property Law, 2006.
- Electronic Signature and Electronic Transactions Law No. (78) of 2012.

Third: Linguistic References:

1. Shaaban Abd al-Aati Atiya et al., *Al-Mu'jam Al-Waseet* (The Intermediate Dictionary), 4th ed., Shorouk International Office, Arabic Language Academy, Egypt, 2004.
2. Al-Zubaidi, Murtada ibn Muhammad, *Taj Al-'Arous min Jawahir Al-Qamus*, edited by a group of scholars under the supervision of Abdul Sattar Ahmad Faraj, Kuwait: Ministry of Awqaf and Islamic Affairs, 1399 AH / 1979 CE, vol. 34.
3. Ibn Manzur, Muhammad ibn Makram, *Lisan Al-Arab*, 1st ed., Dar Sader, vol. 1, Beirut, Lebanon, 2000.

Fourth: Legal Books and Studies:

1. Tariq ibn Abdullah ibn Saleh Al-'Umar, *Rules of Electronic Litigation*, doctoral dissertation submitted to Imam Muhammad ibn Saud Islamic University – Higher Institute of Judiciary, Comparative Jurisprudence Department, 1430 AH.
2. Othman Salman Ghilan Al-Aboudi, *The Impact of Electronic Development on the Principles of Public Service*, 1st ed., Publisher: Sabah Sadiq Jaafar Al-Anbari, Baghdad, 2011.
3. Azmi Bishara, *The Question of the State: A Thesis in Philosophy, Theory, and Contexts*, Doha/Beirut: Arab Center for Research and Policy Studies, 2023.

4. Faiz Muhammad Hussein, *Philosophy of Law*, University Publications House, Cairo, 2007.
5. Muhammad Al-Saeed Khashaba, *Management Information Systems*, University Publishing House, Cairo, 2008.
6. Mona Jbour Al-Ashqar, *Cybernetics: The Concern of the Age*, Arab Center for Legal and Judicial Research, Beirut, Lebanon, 2017.
7. Akram Fadel Saeed, *Protecting Databases from the Risks of Assignment and Unfair Competition: Unpublished Lectures Delivered to Graduate Students (Master's) in the Private Law Department, College of Law, Al-Nahrain University, Academic Year 2013-2014.*

Fifth: Journals and Periodicals:

1. J. Radwan, "Cybersecurity: A Priority in Defense Strategies," *Army Magazine*, Military Publications Foundation, Algeria, Issue 603, January.
2. Ibrahim Ahmad Abdul Samarai, "Cyber Crime in International Law," *Cihan University Erbil Journal of Humanities and Social Sciences*, Vol. 6, No. 2, 2022.
3. Ahmad Abis Nima Al-Fatlawi, "Cyber Attacks: Concept and International Responsibility in Light of Contemporary International Regulation," *Al-Muhaqiq Al-Hilli Journal of Legal and Political Sciences*, Vol. 8, No. 4, College of Law, University of Babylon, Iraq, 2016.
4. Israa Sharif Jejan, "Chinese Cybersecurity: A Study of Motivations and Challenges," *Political Issues*, Issue 56.
5. Basim Ali Khraisaan, "Security in Cyberspace: A Study of Threats and Confrontation Strategies," *Al-Turath University College Journal*, Baghdad, Vol. 1, No. 36, 2023.
6. Ben Arabia Riyad, "Asymmetric Threats in Cyberspace: Fourth Generation Warfare as a Model," *Scientific Research Notebooks*, Vol. 10, No. 1, 2022.
7. Hazem Hamad Musa, "Strategic Vision of Iraqi National Security in Cyberspace: A Study between the Security Dilemma and Performance Capacity," *Algerian Journal of Legal and Political Sciences*, Algeria, Vol. 57, No. 5, 2020.
8. Rizq Ahmad Samudi, "Right of Self-Defense Resulting from Cyber Attacks in Light of International Public Law," *University of Sharjah Journal of Legal Sciences*, Vol. 15, No. 2, December 2018.
9. Raad Khudair Salibi, "Enhancing Cybersecurity in Iraq: Challenges and Opportunities," *International Studies Journal*, Issue 99, 2024.
10. Zahraa Emad Muhammad Kalantar, "Classification of Cyber Attacks in Light of International Law," *Al-Kufa Journal of Legal and Political Sciences*, Vol. 1, No. 44/1, 2020.
11. Shaikha Hussein Al-Zahrani, "International Cooperation in Combating Cyber Attacks," *University of Sharjah Journal of Legal Sciences*, Vol. 17, No. 1, June 2020.
12. Safaa Otani, "The Electronic Court: Concept and Application," published research in *Damascus University Journal of Economic and Legal Sciences*, Vol. 28, No. 1, 2012.
13. Dhafar Abdul Muttalib Al-Tamimi, "Iraq and Cybersecurity: Opportunities and Challenges," *Wasit Journal of Humanities and Social Sciences*, University of Wasit, Iraq, Vol. 18, No. 51, 2022.
14. Al-Eidani Muhammad, "Cyber Threats and Information Crimes," *Al-Ijtihad Journal for Legal and Economic Studies*, Vol. 13, No. 01, 2024.
15. Marwan Salem Al-Ali, "Strategic Challenges of Iraqi National Security in Light of International Changes," *Tikrit Journal of Political Sciences*, Iraq, Vol. 2, No. 20, 2020.
16. Mustafa Ibrahim Salman Al-Shammari, "Cybersecurity and Its Impact on Iraqi National Security," *Journal of Legal and Political Sciences*, College of Law and Political Sciences, University of Diyala, Vol. 10, No. 1, 2021.
17. Nafeh Bahr Sultan, "Electronic Jurisdiction of Iraqi Courts," published research in *Tikrit University Journal of Legal and Political Sciences*, Issue 3, First Year.
18. Mohammed R. M., Zaid R. M., Mohammed I. D. (2023). Text Mining of Iraqi Law Using Clustering Technique. *Journal of Global Scientific Research in Multidisciplinary Studies*. 8(5); 3075-3084.

Sixth: Electronic References:

- Omar Al-Ajlouni, "Why the Draft Cybercrime Law in Iraq Must Be Amended," available at: https://euromedmonitor.org/index.php/ar/article/5498, visited on 14/7/2025.
- Page 3 - *Interpretation of the Holy Qur'an* by Osama Suleiman – Definition of 'Science' linguistically and technically – Al-Maktaba Al-Shamela, accessed 10/7/2025.
- Link: "Information Security: Concept, Importance, and Components," accessed 11/7/2025.