IRAQI Academic Scientific Journals

Sumer Journal of Legal Science
مجلة سومر للعلوم القانونية

P.ISSN: -3081-1082
https://sjls.edu.iq/index.php/su/ar/index

Vol. (1), No. (2) June 2026
Pages 189-214

المجلد (١) العدد (٢) حزيران ٢٠٢٦
الصفحة ١٨٩-٢١٤

Shared Responsibilities Among Authorities in National Cybersecurity Risk Management

Dr. Khaled Hammadi Hussein Al-Jubouri
Directorate General of Education in Nineveh / Legal Department

Abstract:
This research addresses the issue of the distribution of competencies among authorities in the field of cybersecurity in Iraq, through an analysis of the legal and institutional framework governing this distribution, with reference to some comparative experiences, It highlights the interaction between the executive, legislative, and judicial authorities, and reviews their roles in managing cybersecurity risks, whether in terms of regulation and legislation or in terms of oversight and implementation, It also discusses the reality of national bodies concerned with cybersecurity and analyzes the extent of their role integration in the absence of a comprehensive law that precisely regulates this field.

Keywords: Cybersecurity, Iraq, conjoint specializations, authorities, legislation, institutional coordination, digital threats.

https://doi.org/10.66734/dkca8810

1: Email khaled-1970@msn.com
2 : Email:

Submitted: -3-2026
Accepted: 17-3-2026
Published:2-6-2026

رقم الإيداع في دار الكتب والوثائق :2895 لسنة 2025م

الاختصاصات المشتركة بين السلطات في إدارة المخاطر السيبرانية الوطنية

م.د. خالد حمادي الجبوري
المديرية العامة للتربية في نينوى

المستخلص

يتناول هذا البحث مسألة توزيع الاختصاصات بين السلطات في مجال الأمن السيبراني في العراق، من خلال تحليل الإطار القانوني والتنظيمي الذي يحكم هذا التوزيع مع الإشارة إلى بعض التجارب المقارنة التي تسلط الضوء على التفاعل بين السلطات التنفيذية والتشريعية والقضائية، ويستعرض أدوارها في إدارة المخاطر السيبرانية، سواء من حيث التنظيم والتشريع أو من حيث الرقابة والتنفيذ، كما يناقش واقع الهيئات الوطنية المعنية بالأمن السيبراني ويحلل مدى تكامل أدوارها في ظل غياب قانون شامل ينظم هذا المجال بشكل دقيق.

الكلمات المفتاحية :الأمن السيبراني، العراق، الاختصاصات المشتركة، السلطات، التشريع، التنسيق التنظيمي، التهديدات الرقمية.

المقدمة

أولا/ التعريف بموضوع البحث:

يشهدُ العالم تحولات متسارعة في مجال التكنولوجيا والاتصالات، مما أدى إلى بروز الفضاء السيبراني كأحد الميادين الحيوية التي تَمسُ الأمن الوطني والسيادة الرقمية للدول، وفي هذا السياق بات من الضروري أن تتبني الدول نماذج قانونية متكاملة لإدارة المخاطر السيبرانية تقوم على توزيع واضح للاختصاصات بين السلطات المختلفة، وتضمن التنسيق والتكامل في مواجهة التهديدات الرقمية المتزايدة، يتناول هذا البحث مسألة الاختصاصات المشتركة بين السلطات في إدارة المخاطر السيبرانية الوطنية من خلال تحليل الإطار الدستوري والتنظيمي الذي يحكم توزيع هذه الاختصاصات في العراق، واستعراض أدوار الهيئات الوطنية المعنية مع الإشارة إلى بعض النماذج المقارنة التي يمكن أن تُسهِم في تطوير المنظومة العراقية الرقمية.

ثانياً/ أهمية الدراسة:

تنبع أهمية هذه الدراسة من الحاجة الملحة إلى بناء إطار قانوني ومؤسسي فعّال للأمن السيبراني في العراق في ظل تصاعد التهديدات الرقمية وتعدد الجهات المعنية وغياب قانون شامل يُنظم هذا المجال، كما تسعى الدراسة إلى تسليط الضوء على التحديات التي تعيق تفعيل الاختصاصات المشتركة، والفرص المتاحة لبناء

رقم الإيداع في دار الكتب والوثائق :2895 لسنة 2025م

منظومة وطنية متكاملة، بما يُسهم في تعزيز الأمن الرقمي وحماية المصالح الحيوية للدولة وضمان التوازن بين متطلبات الحماية واحترام الحقوق والحريات.

ثالثاً/مشكلة الدراسة

تتمثل الإشكالية القانونية لهذا البحث في التساؤل عن: هل يوجد تنازع أو تداخل في الاختصاصات بين السلطات (التنفيذية، التشريعية، القضائية) في مجال الامن السيبراني؟ وما هي مظاهر الفراغ التشريعي التي تعيق تحديد المسؤوليات بدقة؟

ويتفرع من هذا السؤال الرئيسي سؤالان فرعيان:

١ .ما مدى دستورية توزيع الصلاحيات السيبرانية في ضوء مبدأ الفصل بين السلطات؟ وهل هناك تعارض بين النصوص القانونية القائمة والصلاحيات الممنوحة للجهات التنفيذية؟

٢ .كيف يمكن تفعيل الاختصاصات المشتركة بين السلطات في العراق لضمان إدارة فعالة للمخاطر السيبرانية الوطنية؟

رابعاً/ منهجية الدراسة

تعتمد الدراسة على المنهج التحليلي القانوني من خلال تحليل النصوص الدستورية والتنظيمية ذات الصلة، واستقراء أدوار السلطات المختلفة في إدارة الأمن السيبراني بهدف الوقوف على مدى وضوح توزيع الاختصاصات وفعاليتها، كما تستند إلى المنهج المقارن من خلال استعراض تجارب بعض الدول في تنظيم الاختصاصات السيبرانية بهدف استخلاص الدروس التي يمكن الإستفادة منها في تطوير النموذج العراقي.

خامساً/ هيكلية الدراسة:

لمعالجة موضوع الدراسة المعنون " الاختصاصات المشتركة بين السلطات في إدارة المخاطر السيبرانية الوطنية" إرتأينا تقسيمه الى مبحثين رئيسيين:

المبحث الأول: الإطار القانوني والتنظيمي لتوزيع الاختصاصات في مجال الأمن السيبراني

المبحث الثاني: آليات التنسيق والتكامل بين السلطات في مواجهة التهديدات السيبرانية

رقم الإيداع في دار الكتب والوثائق :2895 لسنة 2025م

المبحث الأول

الإطار القانوني والتنظيمي لتوزيع الاختصاصات في مجال الأمن السيبراني

إن الإطار القانوني والتنظيمي لتوزيع الاختصاصات السيبرانية يمثل حجر الزاوية في بناء منظومة وطنية متماسكة للأمن السيبراني، حيث يحدد هذا الإطار الأدوار والمسؤوليات المنوطة بكل من السلطات التنفيذية والتشريعية والقضائية، ويؤسس لآليات التنسيق والتكامل فيما بينها[١]، كما يتيح هذا التوزيع المنهجي تفادي التداخل في الصلاحيات ويعزز من فعالية الاستجابة للتهديدات السيبرانية، ويضمن احترام المبادئ الدستورية وعلى رأسها مبدأ الفصل بين السلطات.

وفي ظل التحولات المتسارعة التي يشهدها العالم الرقمي، بات الأمن السيبراني يشكل أحد أبرز التحديات التي تواجه الدول الحديثة، نظراً لتزايد الاعتماد على الفضاء السيبراني في مختلف مناحي الحياة، من الاقتصاد والإدارة إلى الأمن والدفاع، وقد أفرز هذا الواقع الجديد حاجة ملحة إلى تطوير أطر قانونية ومؤسسية فعالة تضمن توزيعاً واضحاً ومنظماً للاختصاصات بين مختلف السلطات والجهات المعنية بإدارة المخاطر السيبرانية.[٢]

وتتفاوت النماذج القانونية والتنظيمية المعتمدة من دولة إلى أخرى، تبعاً للسياقات السياسية والدستورية والتقنية، إلا أن القاسم المشترك بينها يتمثل في السعي إلى تحقيق التوازن بين متطلبات الأمن السيبراني وضرورات الحوكمة الرشيدة، ومن هنا تبرز أهمية دراسة هذا الإطار لفهم كيفية تنظيم العلاقة بين الفاعلين السياديين والمؤسسات المتخصصة، واستكشاف أفضل الممارسات المقارنة التي يمكن الاستفادة منها في تطوير السياسات الوطنية في هذا المجال الحيوي.

بناءاً على ما سبق، سنعالج هذا المبحث في مطلبين، حيث نتناول في المطلب الأول: الأساس الدستوري والتنظيمي لتوزيع الاختصاصات، أما في المطلب الثاني سنتناول: الهيئات الوطنية المعنية بإدارة المخاطر السيبرانية.

رقم الإيداع في دار الكتب والوثائق :2895 لسنة 2025م

المطلب الأول

الأساس الدستوري والتنظيمي لتوزيع الاختصاصات

يُشكل تحديد الأساس الدستوري والتنظيمي لتوزيع الاختصاصات في مجال الأمن السيبراني خطوة محورية في بناء منظومة وطنية فعالة لمواجهة التهديدات الرقمية المتزايدة، فمع تعاظم أهمية الفضاء السيبراني كحيز استراتيجي يؤثر في الأمن القومي والاقتصاد والمجتمع، تبرز الحاجة إلى إطار قانوني ومؤسسي يضمن وضوح الأدوار وتكامل الجهود بين مختلف السلطات العامة.[٣]

ويُعنى هذا المطلب بتحليل المرتكزات الدستورية والتنظيمية التي تستند إليها عملية توزيع الاختصاصات السيبرانية، من خلال محورين رئيسيين: يتناول الأول مبدأ الفصل والتكامل بين السلطات في المجال السيبراني، بوصفه أحد المبادئ الدستورية التي تضمن التوازن بين السلطات وتمنع تداخل الصلاحيات أو احتكارها، أما المحور الثاني فيستعرض أبرز القوانين الوطنية المنظمة للأمن السيبراني في عدد من الدول بهدف الوقوف على النماذج المقارنة التي يمكن أن تسهم في بلورة تصور متكامل لتوزيع الاختصاصات في السياق الوطني[٤].

من خلال هذا الجزئية، يسعى المطلب إلى إبراز أهمية التأسيس القانوني والتنظيمي المنضبط في تحقيق الحوكمة السيبرانية الرشيدة، وضمان فعالية الاستجابة للتحديات الرقمية المعاصرة ضمن إطار يحترم المبادئ الدستورية ويعزز التعاون بين السلطات.

الفرع الأول

مبدأ الفصل والتكامل بين السلطات في المجال السيبراني

يُعدُّ مبدأ الفصل بين السلطات من الركائز الأساسية التي تقوم عليها النظم الدستورية الحديثة، إذ يهدف إلى توزيع الوظائف والصلاحيات بين السلطات التنفيذية والتشريعية والقضائية، بما يضمن منع الاستبداد وتحقيق التوازن والرقابة المتبادلة، غير أن تطبيق هذا المبدأ في المجال السيبراني يطرح تحديات خاصة نظراً للطبيعة المتداخلة والمعقدة لهذا المجال الذي يتطلب استجابة سريعة وفعالة لمخاطر متغيرة ومتعددة الأبعاد تتراوح بين التقنية والقانونية والأمنية.[٥]

في هذا السياق، لا يمكن الاكتفاء بفصل صارم بين السلطات، بل تبرز الحاجة إلى تكامل مؤسسي مرن يراعي خصوصية الفضاء السيبراني، فالسلطة التنفيذية بوصفها الجهة المسؤولة عن تنفيذ السياسات العامة، تضطلع بدور محوري في إدارة الأمن السيبراني من خلال الوزارات المختصة والهيئات الوطنية المعنية مثل الفرق الوطنية

رقم الإيداع في دار الكتب والوثائق :2895 لسنة 2025م

للاستجابة للحوادث السيبرانية، وتقوم هذه الجهات بوضع الاستراتيجيات وتنسيق الجهود والتعامل مع التهديدات في الوقت الفعلي، إلا أن هذا الدور لا يمكن أن يكون فعالاً دون إطار تشريعي واضح ومحدث، وهو ما تضطلع به السلطة التشريعية من خلال سَنْ القوانين التي تنظم الأمن السيبراني وتحدد صلاحيات الجهات التنفيذية وتضع الضوابط اللازمة لحماية الحقوق والحريات الرقمية(٦).

أما السلطة القضائية، فتضطلع بدور أساسي في ضمان سيادة القانون في الفضاء السيبراني، ويتمثل هذا الدور في وظيفتين رئيستين: الأولى، الفصل في المنازعات الناشئة عن الجرائم السيبرانية وما يتعلق بها من دعاوى حماية الخصوصية والثانية، تفسير النصوص القانونية ذات الصلة بما يضمن تكيف الأفعال الإلكترونية ضمن القواعد القانونية العامة مما يُسهم في ترسيخ الإجتهاد القضائي المتخصص في هذا المجال (٧).

إن التفاعل بين هذه السلطات لا ينبغي أن يُفهم على أنه تنازع أو تداخل في الصلاحيات، بل هو تعبير عن تكامل وظيفي يهدف إلى تحقيق الحوكمة الرشيدة في مجال الأمن السيبراني، فالتحديات السيبرانية لا تعترف بالحدود الإدارية أو القانونية التقليدية، بل تتطلب استجابة منسقة تتجاوز منطق التقسيم الصارم للسلطات، ومن هنا فإن مبدأ الفصل بين السلطات في المجال السيبراني يجب أن يُعاد تأويله في ضوء متطلبات العصر الرقمي، بحيث يُحافظ على استقلالية كل سلطة دون أن يُعيق التعاون والتنسيق الضروريين لمواجهة التهديدات السيبرانية بكفاءة وفعالية.(٨)

ففي العراق، لا يزال الإطار القانوني للأمن السيبراني في طور التشكّل، إلا أن المبادئ العامة للفصل بين السلطات تنعكس على كيفية تعامل كل سلطة مع القضايا السيبرانية، فالسلطة التشريعية ممثلة بمجلس النواب تضطلع بمهمة سَنْ القوانين التي تنظم الفضاء السيبراني مثل مشروع قانون الجرائم المعلوماتية، الذي يهدف إلى تجريم الأفعال الضارة عبر الوسائل الإلكترونية وتنظيم استخدام التكنولوجيا بما يضمن حماية الأمن الوطني وحقوق الأفراد، ورغم الجدل الذي أثاره هذا المشروع إلا أنه يمثل محاولة لتقنين المجال السيبراني ضمن إطار تشريعي(٩).

أما السلطة التنفيذية، فتتجسد مسؤولياتها في تنفيذ السياسات السيبرانية وتوفير البنية التحتية اللازمة لحماية الفضاء الرقمي، وقد أنشأت الحكومة العراقية جهات مختصة بهذا المجال، مثل مركز الأمن السيبراني التابع لوزارة الداخلية ووحدة مكافحة الجرائم الإلكترونية، بالإضافة إلى دور وزارة الاتصالات في تنظيم قطاع الإنترنت،

رقم الإيداع في دار الكتب والوثائق :2895 لسنة 2025م

هذه الجهات تعمل على تنفيذ السياسات، رصد التهديدات، والتنسيق مع الجهات الدولية، لكنها تحتاج إلى صلاحيات قانونية واضحة تُمنح من خلال التشريع البرلماني(١٠).

فالسلطة القضائية من جانبها تلعب دوراً حاسماً في تفسير وتطبيق القوانين السيبرانية والفصل في النزاعات المتعلقة بالجرائم الإلكترونية وحماية الحقوق الرقمية للمواطنين، ومع ذلك فإن غياب تشريعات متكاملة في هذا المجال يضع القضاء أمام تحديات كبيرة، خاصة فيما يتعلق بتكييف الأفعال الإلكترونية ضمن النصوص القانونية التقليدية وضمان العدالة في ظل تطور الجرائم الرقمية.(١١)

ورغم الفصل الوظيفي بين السلطات فإن التكامل بينها ضروري لضمان فعالية منظومة الأمن السيبراني، فالتشريع لا يكتمل دون مشورة فنية من الجهات التنفيذية والتطبيق لا يكون فعالًا دون رقابة قضائية تضمن احترام الحقوق والحريات، كما أن التنسيق بين هذه السلطات ضروري في حالات الطوارئ السيبرانية، حيث تتطلب الاستجابة الفعالة تعاوناً سريعاً بين الجهات الأمنية القضائية والتشريعية.(١٢)

في النهاية فإن مبدأ الفصل والتكامل بين السلطات في المجال السيبراني في العراق لا يزال في طور التبلور ويعتمد تطوره على مدى قدرة الدولة على تحديث تشريعاتها وبناء مؤسسات متخصصة وتعزيز ثقافة التعاون بين السلطات بما يضمن أمن الفضاء الرقمي وحماية الحقوق الدستورية للمواطنين.

الفرع الثاني

القوانين الوطنية المنظمة للأمن السيبراني (نماذج مقارنة)

تُعدُّ القوانين الوطنية المنظمة للأمن السيبراني من الركائز الأساسية التي تعتمد عليها الدول في حماية فضائها الرقمي وضمان أمن المعلومات وصون الحقوق والحريات في البيئة الإلكترونية، وقد أصبح من الضروري أن تمتلك كل دولة إطاراً قانونياً واضحاً وشاملاً ينظم هذا المجال، وفي ظل التوسع الهائل في استخدام التكنولوجيا وتزايد التهديدات السيبرانية التي تستهدف الأفراد والمؤسسات والبنى التحتية الحيوية.(١٣)

تسعى هذه القوانين إلى تحقيق جملة من الأهداف من أبرزها حماية البيانات الشخصية وضمان سرية المعلومات وتنظيم استخدام الوسائل الإلكترونية، إضافة إلى تجريم الأفعال التي تُرتكب عبر الفضاء السيبراني مثل الاختراق والابتزاز الإلكتروني ونشر البرمجيات الخبيثة والتجسس الرقمي، كما تهدف إلى تعزيز الثقة في التعاملات الإلكترونية وتوفير بيئة رقمية آمنة تشجع على الاستثمار والابتكار(١٤).

رقم الإيداع في دار الكتب والوثائق :2895 لسنة 2025م

في سبيل تحقيق هذه الأهداف، تتضمن القوانين الوطنية للأمن السيبراني عادةً أحكاماً تتعلق بتحديد الجهات المختصة بتنفيذ السياسات السيبرانية مثل الهيئات الوطنية للأمن السيبراني أو مراكز الاستجابة للطوارئ الرقمية، وتمنحها صلاحيات واسعة في مجالات الرصد والتحقيق والتنسيق مع الجهات الأخرى، كما تنص على التزامات تقع على عاتق الجهات الحكومية والخاصة مثل تبني معايير الحماية والإبلاغ عن الحوادث السيبرانية وتعيين مسؤولين مختصين بالأمن السيبراني(١٥).

وتُدرجْ هذه القوانين لتشمل العقوبات المقررة على منتهكي أحكامها، والتي قد تشمل الغرامات المالية أو السجن أو إغلاق المواقع الإلكترونية وذلك بحسب جسامة الفعل المرتكب، وتُراعى في صياغة هذه العقوبات مبادئ التناسب والعدالة مع الحرص على عدم المساس بحرية التعبير أو الاستخدام المشروع للتكنولوجيا.(١٦)

تختلف تفاصيل هذه القوانين من دولة إلى أخرى بحسب السياق القانوني والسياسي والتقني لكل بلد، فبعض الدول تعتمد قوانين شاملة ومحدثة، بينما تكتفي دول أخرى بتضمين أحكام الأمن السيبراني ضمن قوانين الجرائم الإلكترونية أو قوانين الاتصالات، كما أن بعض الدول تركز على حماية البنية التحتية الحيوية، في حين تُولي دول أخرى اهتماماً أكبر بحماية البيانات الشخصية أو مكافحة الإرهاب الرقمي.(١٧)

ومع ذلك فإن التحدي الأكبر الذي تواجهه هذه القوانين يتمثل في مواكبة التطورات السريعة في مجال التكنولوجيا والتغير المستمر في طبيعة التهديدات السيبرانية، ولذلك فإن تحديث هذه القوانين بشكل دوري وتعزيز التعاون بين السلطات الوطنية والدولية وتطوير القدرات البشرية والتنظيمية، إذ يُعدُّ أمراً ضرورياً لضمان فعاليتها واستجابتها للواقع المتغير(١٨).

بالتالي فإن القوانين الوطنية المنظمة للأمن السيبراني تمثل الإطار القانوني الذي تستند إليه الدولة في حماية فضائها الرقمي، وهي تعكس مدى وعيها بأهمية الأمن السيبراني كعنصر من عناصر الأمن القومي وكمجال حيوي يتقاطع مع مختلف جوانب الحياة المعاصرة.

وفي القوانين المقارنة تُعدُّ القوانين الوطنية المنظمة للأمن السيبراني في كل من العراق ومصر والأردن انعكاساً لمدى إدراك هذه الدول لأهمية حماية فضائها الرقمي في ظل التهديدات المتزايدة التي تستهدف البنى التحتية الحيوية والبيانات الشخصية والمؤسسات الحكومية والخاصة، ورغم أن هذه الدول تتقاطع في إدراكها لأهمية الأمن السيبراني، إلا أن مقاربتها القانونية تختلف من حيث النضج والهيكل التنظيمي ومدى شمولية التشريعات.(١٩)

رقم الإيداع في دار الكتب والوثائق :2895 لسنة 2025م

ففي العراق لا يزال الإطار القانوني للأمن السيبراني في طور التشكّل، إذ لم يُقَرّ حتى الآن قانون شامل خاص بالأمن السيبراني رغم وجود مسودات ومشاريع قوانين مثل مشروع قانون الجرائم المعلوماتية الذي أثار جدلاً واسعاً بسبب مخاوف تتعلق بحرية التعبير، ومع ذلك توجد جهود مؤسسية مثل تأسيس المركز الوطني للأمن السيبراني واستراتيجية وطنية للأمن السيبراني أطلقتها مستشارية الأمن الوطني، تسعى إلى بناء قدرات وطنية وتعزيز التعاون الدولي وتطوير البنية التحتية الرقمية، إلا أن غياب تشريع ملزم ومتكامل يَحدُّ من فعالية هذه الجهود ويجعل العراق أكثر عرضة للتهديدات السيبرانية خاصة في ظل ضعف التنسيق بين الجهات المعنية ونقص الكوادر المتخصصة.[٢٠]

أما في مصر فقد قطعت الدولة شوطاً متقدماً في تنظيم الأمن السيبراني، حيث أطلقت الاستراتيجية الوطنية للأمن السيبراني ٢٠٢٣–٢٠٢٧، التي يُشرف عليها المجلس الأعلى للأمن السيبراني التابع لمجلس الوزراء، وتهدف هذه الاستراتيجية إلى حماية البنية التحتية الحيوية وتعزيز القدرات الوطنية وخلق صناعة سيبرانية وطنية، كما أن الجهاز القومي لتنظيم الاتصالات وضع إطاراً تنظيمياً لتقديم خدمات الأمن السيبراني الذي يحدد المعايير والضوابط التي يجب أن تلتزم بها الشركات العاملة في هذا المجال، وتُعدّ مصر من الدول التي تسعى إلى تحقيق التوازن بين حماية الأمن الرقمي وضمان الحقوق الرقمية من خلال تطوير تشريعاتها بشكل تدريجي وتوسيع نطاق الشراكات الإقليمية والدولية في هذا المجال.[٢١]

يُعدُّ قانون الأمن السيبراني رقم ١٦ لسنة ٢٠١٩ في الأردن من أبرز التشريعات في هذا المجال، حيث أنشأ بموجبه المركز الوطني للأمن السيبراني[٢٢]، الذي أُوكلت إليه مهام تنظيم القطاع ووضع السياسات والتنسيق بين الجهات المختلفة، كما أُقرت قوانين وأنظمة مكمّلة مثل قانون الجرائم الإلكترونية لسنة ٢٠٢٣[٢٣]، وقانون حماية البيانات الشخصية ونظام ترخيص مقدميّ خدمات الأمن السيبراني وتعليمات تصنيف الحوادث السيبرانية، وتُظهر هذه المنظومة القانونية تطوراً ملحوظاً في المقاربة الأردنية التي تسعى إلى بناء بيئة رقمية آمنة مع التركيز على حماية الحقوق والحريات وتطوير الكفاءات الوطنية وتعزيز الشفافية في التعامل مع الحوادث السيبرانية وقد تعاملت دول بما في ذلك دول عربية مثل العراق والإمارات وعمان والأردن وسوريا، مع الجرائم السيبرانية من خلال تشريعات عقابية وتنظيمية في تجريم الوصول غير القانوني إلى مواقع الويب وأنظمة المعلومات المملوكة من الغير[٢٤] .

رقم الإيداع في دار الكتب والوثائق :2895 لسنة 2025م

المطلب الثاني

الهيئات الوطنية المعنية بإدارة المخاطر السيبرانية

أصبحت إدارة المخاطر السيبرانية أولوية وطنية لا غنى عنها لضمان استقرار الدول وحماية مصالحها الحيوية، وذلك في ظل تصاعد التهديدات السيبرانية وتزايد الاعتماد على التكنولوجيا الرقمية في مختلف مناحي الحياة، ولمواجهة هذا التحدي المتنامي، برزت الحاجة إلى إنشاء هيئات وطنية متخصصة تُعنى بإدارة هذه المخاطر وتُشكل البنية التنظيمية التي تتولى مسؤولية التخطيط والتنفيذ والتنسيق بين مختلف الجهات المعنية بالأمن السيبراني.[٢٥]

تُعدُّ هذه الهيئات بمثابة الدرع الأول في مواجهة الهجمات الإلكترونية حيث تضطلع بمهام متعددة تشمل رصد التهديدات والاستجابة للحوادث ووضع السياسات الوطنية وتطوير القدرات الفنية والبشرية، فضلاً عن التنسيق مع الشركاء الإقليميين والدوليين، وتتنوع هذه الهيئات بين وزارات مختصة ووكالات وطنية ومراكز استجابة للطوارئ السيبرانية، ولكل منها دور محدد في منظومة الحماية الرقمية.[٢٦]

وبناءً على ما سبق، سندرس هذا المطلب في فرعين وفق الآتي:

الفرع الأول

دور السلطة التنفيذية (الوزارات، الوكالات، الفرق الوطنية للاستجابة للحوادث)

في ظل التوسع الرقمي المتسارع الذي يشهده العالم، لم تَعدّ التهديدات السيبرانية مجرد احتمالات نظرية بل أصبحت واقعاً ملموساً يهدد الأمن الوطني للدول، ويطال مؤسساتها الحيوية واقتصاداتها وخصوصية مواطنيها[٢٧]، وفي هذا السياق تبرز أهمية الدور الذي تضطلع به السلطة التنفيذية في إدارة المخاطر السيبرانية من خلال أجهزتها المختلفة، كالمؤسسات الحكومية والوزارات والوكالات المتخصصة والفرق الوطنية للاستجابة للحوادث السيبرانية، ويُعدُّ هذا دوراً محورياً في بناء منظومة وطنية متماسكة للأمن السيبراني قادرة على الوقاية من التهديدات والاستجابة الفعالة لها والتعافي من آثارها.[٢٨]

ففي العراق ورغم غياب قانون شامل ومُقرّ خاص بالأمن السيبراني حتى الآن، إلا أن السلطة التنفيذية بدأت تتخذ خطوات مؤسسية مهمة لمواجهة التحديات الرقمية، فقد أُنشئ المركز الوطني للأمن السيبراني التابع لهيئة الإعلام والاتصالات، ليكون الجهة الفنية المسؤولة عن تنسيق الجهود الوطنية في مجال الأمن السيبراني وتقديم الدعم الفني للجهات الحكومية ورصد التهديدات السيبرانية وتطوير السياسات العامة في هذا المجال، كما

رقم الإيداع في دار الكتب والوثائق :2895 لسنة 2025م

تضطلع وزارة الداخلية من خلال مديرية مكافحة الجرائم الإلكترونية بدور مهم في التحقيق في الجرائم السيبرانية وملاحقة مرتكبيها والتعاون مع الجهات القضائية في تقديمهم للعدالة.

إلى جانب ذلك، تلعب وزارة الاتصالات دوراً تنظيمياً في إدارة البنية التحتية الرقمية وتنظيم عمل مزوديّ خدمات الإنترنت وضمان إلتزامهم بمعايير الأمان السيبراني، كما تسهم وزارة التعليم العالي والبحث العلمي في دعم البحث والتطوير في مجال الأمن السيبراني من خلال الجامعات والمراكز البحثية وتخريج كوادر متخصصة قادرة على سد الفجوة التقنية في هذا القطاع.[٢٩]

أما على صعيد الاستجابة للحوادث السيبرانية، فقد بدأت السلطة التنفيذية في العراق بتأسيس فرق وطنية للاستجابة للطوارئ الحاسوبية، تتولى مهام الرصد المبكر للهجمات وتحليل البرمجيات الخبيثة وتقديم الدعم الفني للجهات المتضررة وتنسيق الجهود مع الشركاء الإقليميين والدوليين، بالرغم أن هذه الفرق لا تزال في مراحلها الأولى من التأسيس، إلا أنها تمثل خطوة مهمة نحو بناء قدرة وطنية فعالة في مجال الاستجابة السريعة للحوادث السيبرانية[٣٠].

ومع ذلك، فإن فعالية هذه الأدوار تبقى مرهونة بوجود إطار قانوني واضح يُحدد الصلاحيات ويُعزز التنسيق بين الجهات المختلفة ويُرسّخ مبدأ المساءلة والشفافية، فغياب قانون شامل للأمن السيبراني يَحدُّ من قدرة السلطة التنفيذية على اتخاذ إجراءات حاسمة ويُضعف من قدرتها على التنسيق مع السلطات الأخرى، خاصة في ظل التداخل بين الاختصاصات وتعدد الجهات المعنية[٣١].

في المحصلة النهائية، فإن السلطة التنفيذية في العراق تمثل حجر الزاوية في إدارة المخاطر السيبرانية، من خلال أجهزتها المختلفة التي تتوزع أدوارها بين التنظيم والرصد والتحقيق والاستجابة، غير أن تعزيز هذا الدور يتطلب استكمال الإطار التشريعي وتطوير البنية التنظيمية وبناء القدرات الوطنية، بما يضمن حماية فعالة للفضاء السيبراني العراقي في مواجهة التحديات المتزايدة.

الفرع الثاني

مساهمة السلطة التشريعية والقضائية في الرقابة والتنظيم

في إطار بناء منظومة وطنية متكاملة للأمن السيبراني، لا يقتصر الدور على السلطة التنفيذية فحسب، بل تتعاظم أهمية مساهمة السلطتين التشريعية والقضائية في إرساء قواعد الرقابة والتنظيم، بما يضمن التوازن بين حماية الأمن الرقمي وصون الحقوق والحريات الأساسية، فالسلطة التشريعية تضطلع بمهمة وضع الإطار

رقم الإيداع في دار الكتب والوثائق :2895 لسنة 2025م

القانوني الذي يُنظم الفضاء السيبراني ويُحدد مسؤوليات الجهات المختلفة ويُرسّخ المبادئ الدستورية في بيئة رقمية تتسم بالتغير السريع والتعقيد المتزايد، ومن خلال سن القوانين ومراجعتها وتحديثها، تضمن هذه السلطة أن تكون التشريعات مواكبة للتطورات التقنية وقادرة على التصدي للجرائم الإلكترونية وتنظيم استخدام البيانات، وضمان الشفافية والمساءلة في أداء المؤسسات المعنية بالأمن السيبراني.[٣٢]

أما السلطة القضائية، فتُشكل الضمانة الأساسية لتطبيق هذه القوانين بعدالة وفعالية، إذ تتولى مهمة الفصل في النزاعات الناشئة عن الجرائم السيبرانية وتفسير النصوص القانونية ذات الصلة وحماية الحقوق الرقمية للأفراد والمؤسسات، كما تلعب دوراً مهماً في ترسيخ مبدأ سيادة القانون في الفضاء الرقمي من خلال إصدار الأحكام التي تُراعي التوازن بين متطلبات الأمن وحرية التعبير وخصوصية الأفراد، وتُسهم هذه السلطة كذلك في تطوير الاجتهاد القضائي في مجال الجرائم الإلكترونية، وهو ما يُعدُّ ضرورياً في ظل حداثة هذا النوع من الجرائم وتعدد أشكاله وأساليبه.[٣٣]

إن مساهمة السلطتين التشريعية والقضائية في الرقابة والتنظيم لا تقتصر على الجانب القانوني فحسب، بل تمتد إلى تعزيز الثقة المجتمعية في منظومة الأمن السيبراني من خلال ضمان أن تكون الإجراءات المتخذة في هذا المجال خاضعة للرقابة البرلمانية ومحمية بضمانات قضائية تكفل العدالة والإنصاف، ومن هنا فإن التكامل بين هذه السلطات يُعدُّ شرطاً أساسياً لنجاح أي استراتيجية وطنية للأمن السيبراني، ويُجسد هذا التوازن المطلوب بين الفعالية الأمنية والشرعية القانونية.[٣٤]

تكتسب مساهمة السلطتين التشريعية والقضائية في الرقابة والتنظيم في العراق ضمن مجال الأمن السيبراني أهمية متزايدة، خاصة في ظل التحديات التي يفرضها الواقع الرقمي المتسارع وغياب قانون وطني شامل ينظم هذا المجال بشكل دقيق، فالسلطة التشريعية ممثلة بمجلس النواب تتحمل المسؤولية في وضع الإطار القانوني الذي يُنظم الفضاء السيبراني ويُحدد صلاحيات الجهات التنفيذية ويُرسّخ المبادئ الدستورية المتعلقة بحماية الحقوق والحريات في البيئة الرقمية، وقد شهد العراق محاولات متعددة لصياغة قانون للجرائم المعلوماتية، إلا أن هذه المحاولات واجهت انتقادات واسعة من قبل منظمات المجتمع المدني والناشطين، لما تضمنته بعض المسودات من مواد اعتُبرت فضفاضة أو قابلة للتأويل، مما قد يهدد حرية التعبير وتُستخدم لتقييد الحريات العامة، ورغم ذلك فإن وجود تشريع متوازن يراعي متطلبات الأمن من جهة ويصون الحقوق من جهة أخرى، يظل ضرورة ملحة في ظل تصاعد الهجمات السيبرانية التي تستهدف مؤسسات الدولة والبنية التحتية الحيوية[٣٥].

رقم الإيداع في دار الكتب والوثائق :2895 لسنة 2025م

أما السلطة القضائية، فإن دورها يتجلى في تطبيق القوانين ذات الصلة بالأمن السيبراني والفصل في القضايا المتعلقة بالجرائم الإلكترونية وتفسير النصوص القانونية بما يتلائم مع طبيعة الجرائم الرقمية التي غالباً ما تتسم بالتعقيد والتطور التقني، ويواجه القضاء العراقي تحديات كبيرة في هذا المجال، من بينها نقص الخبرات المتخصصة في الجرائم السيبرانية وصعوبة تكييف بعض الأفعال الإلكترونية ضمن النصوص القانونية التقليدية، فضلاً عن الحاجة إلى تطوير أدوات التحقيق الرقمي، وتعزيز التعاون مع الجهات الفنية المختصة، ومع ذلك فإن السلطة القضائية تبقى الضامن الأساسي لحماية الحقوق الرقمية من خلال الرقابة على مشروعية الإجراءات التي تتخذها الجهات التنفيذية وضمان عدم تجاوزها للصلاحيات الممنوحة لها بموجب القانون[٣٦].

إن التفاعل بين السلطتين التشريعية والقضائية في العراق يُعدُّ عنصراً جوهرياً في بناء منظومة قانونية فعالة للأمن السيبراني، حيث تُسهم الأولى في سَنْ القوانين وتحديثها بما يتماشى مع المستجدات التقنية، بينما تضمن الثانية تطبيق هذه القوانين بعدالة وحيادية، ويُعدُّ هذا التوازن ضرورياً لضمان أن تكون السياسات السيبرانية منسجمة مع المبادئ الدستورية ومبنية على أسس قانونية واضحة وقابلة للتنفيذ القضائي، بما يعزز ثقة المواطنين في قدرة الدولة على حماية فضائهم الرقمي دون المساس بحقوقهم الأساسية.[٣٧]

المبحث الثاني

آليات التنسيق والتكامل بين السلطات في مواجهة التهديدات السيبرانية

لم يَعدُّ بالإمكان الاكتفاء بجهود منفردة أو معزولة من قبل جهة واحدة لمواجهتها، في ظل تصاعد التهديدات السيبرانية التي باتت تَمسُ أمن الدول واستقرارها، بل أصبح من الضروري اعتماد نهج مؤسسي قائم على التنسيق والتكامل بين مختلف السلطات الوطنية، فالطبيعة المعقدة والمتغيرة للهجمات الرقمية والتي قد تستهدف البنية التحتية الحيوية أو المؤسسات الحكومية أو حتى الأفراد، تفرض على الدولة أن تُوحِد جهودها من خلال منظومة متكاملة تتوزع فيها الأدوار بوضوح وتتكامل فيها الصلاحيات دون تداخل أو تضارب.[٣٨]

إنّ آليات التنسيق والتكامل بين السلطات، سواء كانت تشريعية أو تنفيذية أو قضائية، تمثل الإطار العملي الذي يضمن استجابة فعالة وسريعة للتهديدات السيبرانية ويَحول دون استغلال الثغرات التنظيمية أو القانونية، فالتشريعات وحدها لا تكفي ما لم تُترجم إلى سياسات تنفيذية واضحة، وهذه السياسات بدورها تحتاج إلى رقابة قضائية تضمن التزامها بالقانون وحماية الحقوق[٣٩]، كما أن التنسيق بين الجهات الأمنية والتقنية والقانونية يُعدُّ شرطاً أساسياً لتبادل المعلومات وتحديد المسؤوليات وتفادي الازدواجية في المهام، كما إن بناء منظومة وطنية

رقم الإيداع في دار الكتب والوثائق :2895 لسنة 2025م

فعالة للأمن السيبراني لا يتحقق إلا من خلال ترسيخ ثقافة التعاون التنظيمي وتطوير قنوات اتصال دائمة بين السلطات، وتحديد آليات واضحة لتقاسم الأدوار والمهام في حالات الطوارئ السيبرانية، ومن هنا فإن الحديث عن آليات التنسيق والتكامل بين السلطات لا يُعدُّ ترفاً تنظيمياً، بل هو ضرورة استراتيجية لضمان أمن الدولة الرقمي وتعزيز قدرتها على الصمود في وجه التحديات المتزايدة في الفضاء السيبراني.[٤٠]

بناءاً على ما سبق، سندرس هذا المبحث في مطلبين، نتناول في المطلب الأول: صور التعاون التنظيمي بين السلطات، أما في المطلب الثاني نتناول فيه التحديات والفرص في تفعيل الاختصاصات المشتركة.

المطلب الأول

صور التعاون التنظيمي بين السلطات

تزايد الاعتماد على الفضاء السيبراني في مختلف مناحي الحياة فرض على الدول تحديات غير مسبوقة تتطلب استجابات مؤسسية منسقة تتجاوز حدود الاختصاصات التقليدية، إذ أن التهديدات الرقمية لم تَعدُّ تستهدف فقط البنية التحتية أو المؤسسات الأمنية، بل امتدت لتشمل قطاعات الاقتصاد، التعليم، الصحة، والخصوصية الفردية، ما يستدعي تفعيل آليات تعاون فعّالة بين السلطات المختلفة لضمان استجابة وطنية شاملة .[٤١]

فالتعاون التنظيمي بين السلطات لا يُعدُّ خياراً تنظيمياً بل ضرورة استراتيجية تفرضها طبيعة التهديدات السيبرانية التي تتسم بالتعقيد والتطور المستمر، وهذا التعاون يتجسد في صور متعددة منها التنسيق بين الجهات التشريعية والتنفيذية والقضائية، وتبادل المعلومات والخبرات وتوحيد الجهود في صياغة السياسات العامة، فضلاً عن العمل المشترك في إدارة الأزمات السيبرانية والتحقيق في الجرائم الرقمية[٤٢].

بناءاً على ما تقدم سندرس هذا المطلب في فرعين وذلك وفق الاتي:

الفرع الأول

التنسيق بين الأجهزة الأمنية والمدنية في إدارة الأزمات السيبرانية

يُشكل التنسيق بين الأجهزة الأمنية والمدنية في إدارة الأزمات السيبرانية أحد المرتكزات الأساسية لضمان استجابة فعالة وشاملة للتهديدات الرقمية التي قد تطال البنية التحتية الحيوية للدولة أو تَمسُ الأمن العام والمصالح الاقتصادية والاجتماعية، وهذا التنسيق لا يُعدُّ مجرد إجراء تنظيمي، بل هو ضرورة استراتيجية تفرضها طبيعة الأزمات السيبرانية التي تتسم بالمباغتة والتعقيد والتأثير المتعدد الأبعاد، ما يجعل من غير الممكن لأي جهة بمفردها أن تتصدى لها بكفاءة دون تعاون وتكامل مع الأطراف الأخرى.[٤٣]

رقم الإيداع في دار الكتب والوثائق :2895 لسنة 2025م

في هذا الإطار تتقاطع مهام الأجهزة الأمنية التي تمتلك الخبرة في التحقيقات الجنائية والتعامل مع التهديدات الموجهة للأمن الوطني مع مهام الجهات المدنية التي تدير قطاعات الاتصالات والخدمات والطاقة والمعلومات، في حين عندما تقع أزمة سيبرانية، كاختراق شبكة حكومية أو هجوم على نظام مصرفي أو تسريب بيانات حساسة، فإن الاستجابة تتطلب تفعيل قنوات اتصال فورية ومباشرة بين هذه الجهات لتبادل المعلومات وتحديد طبيعة التهديد وتقدير مدى انتشاره ووضع خطة استجابة مشتركة تتضمن إجراءات العزل والتحقيق والتعافي(٤٤).

غالباً ما تتولى الأجهزة الأمنية مثل وحدات مكافحة الجرائم الإلكترونية أو أجهزة الاستخبارات، مسؤولية تتبع مصدر الهجوم وتحليل نواياه، بينما تضطلع الجهات المدنية كوزارات الاتصالات أو مراكز الطوارئ الرقمية بمهمة احتواء الأثر الفني للهجوم واستعادة الأنظمة المتضررة وضمان استمرارية الخدمات، هذا التداخل في الأدوار يتطلب وجود بروتوكولات واضحة للتنسيق تُحدد بموجبها المسؤوليات، وآليات اتخاذ القرار وتبادل البيانات، دون أن يؤدي ذلك إلى تضارب في الصلاحيات أو تأخير في الاستجابة.(٤٥)

كما أن التنسيق بين هذه الجهات لا يقتصر على لحظة وقوع الأزمة، بل يبدأ من مرحلة الوقاية من خلال إعداد خطط وطنية مشتركة وتنفيذ تدريبات دورية لمحاكاة الهجمات السيبرانية وتقييم الجاهزية التنظيمية وتطوير أنظمة الإنذار المبكر، كذلك يُعدُّ التنسيق ضرورياً في مرحلة ما بعد الأزمة لتقييم الأداء واستخلاص الدروس وتحديث السياسات والإجراءات بما يعزز مناعة الدولة الرقمية.(٤٦)

إن نجاح هذا التنسيق يعتمد على عدة عوامل، من بينها وجود إرادة سياسية واضحة تدعم العمل المشترك وتوفر بنية تشريعية تُنظم العلاقة بين الجهات المعنية وتُعزز ذلك بتبادل المعلومات دون المساس بالخصوصية أو السيادة، كما يتطلب الأمر بناء ثقافة قانونية تؤمن بأهمية التعاون وتُشجع على تجاوز الحواجز البيروقراطية وتُكرّس مفهوم الأمن السيبراني كمسؤولية وطنية جماعية.

في المحصلة النهائية، فإن التنسيق بين الأجهزة الأمنية والمدنية في إدارة الأزمات السيبرانية يُعدُّ ركيزة لا غنى عنها في أي استراتيجية وطنية للأمن الرقمي، وهو ما يضمن للدولة القدرة على الصمود أمام التهديدات المتزايدة وحماية مصالحها الحيوية وتعزيز ثقة المواطنين في قدرتها على تأمين فضائهم الرقمي.(٤٧)

يشهد العراق في هذا السياق في السنوات الأخيرة تنامياً في الوعي بأهمية الأمن السيبراني، خاصة مع تصاعد الهجمات الرقمية التي استهدفت مؤسسات حكومية وخدمية، مما برزت الحاجة إلى تنسيق فعّال بين الأجهزة الأمنية والمدنية في إدارة الأزمات السيبراني، ورغم أن الإطار القانوني العراقي لا يتضمن حتى الآن قانوناً

رقم الإيداع في دار الكتب والوثائق :2895 لسنة 2025م

شاملاً ومُقرّاً خاصاً بالأمن السيبراني، إلا أن بعض الجهود التنظيمية بدأت تتبلور ضمن صلاحيات السلطة التنفيذية، مما أتاح مجالاً لتفعيل التنسيق بين الجهات المعنية، وإن كان ذلك لا يزال يفتقر إلى الغطاء القانوني الكامل.(٤٨)

في الواقع تتوزع المهام بين عدد من الجهات، فوزارة الداخلية من خلال مديرية مكافحة الجرائم الإلكترونية تتولى التحقيق في الحوادث السيبرانية ذات الطابع الجنائي، بينما تضطلع هيئة الإعلام والاتصالات بدور تنظيمي فيما يخص البنية التحتية الرقمية، وتُشرف على المركز الوطني للأمن السيبراني الذي أُنشئ ليكون نقطة الارتكاز الفنية في رصد التهديدات وتنسيق الاستجابة، وهذا التوزيع في المهام يفرض ضرورة وجود تنسيق مؤسسي واضح، خاصة في حالات الطوارئ السيبرانية التي تتطلب استجابة سريعة ومتكاملة بين الجهات الأمنية التي تملك أدوات التحقيق والتحليل الجنائي الرقمي والجهات المدنية التي تدير الأنظمة المتضررة وتتحكم بالبنية التحتية التقنية.(٤٩)

إن غياب قانون خاص بالأمن السيبراني يُضعف من فعالية هذا التنسيق، إذ لا توجد نصوص قانونية تُحدد بدقة آليات التعاون أو تُلزم الجهات المختلفة بتبادل المعلومات أو تُنظم إجراءات الاستجابة المشتركة، ونتيجة لذلك غالباً ما يتم التعامل مع الأزمات السيبرانية وفقاً لاجتهادات إدارية أو تعليمات داخلية، ما قد يؤدي إلى تضارب في الصلاحيات أو تأخر في اتخاذ القرار، خاصة في الحالات التي تتطلب تدخلاً فورياً لاحتواء الأثر ومنع انتشاره.(٥٠)

مع ذلك، هناك مؤشرات على تطور تدريجي في هذا المجال، حيث أطلقت مستشارية الأمن الوطني استراتيجية وطنية للأمن السيبراني تهدف إلى تعزيز التنسيق بين الجهات المعنية وتطوير البنية التحتية القانونية والتنظيمية، وبناء قدرات وطنية قادرة على إدارة الأزمات الرقمية بكفاءة، كما أن بعض مشاريع القوانين مثل مشروع قانون الجرائم المعلوماتية، وإن كان لا يزال مثيراً للجدل، إذ يُعدُّ خطوة نحو تنظيم العلاقة بين الجهات الأمنية والمدنية، خاصة إذا ما أُعيدت صياغته بما يضمن التوازن بين متطلبات الأمن وحماية الحقوق.(٥١)

إن إدارة الأزمات السيبرانية في العراق تظل رهينة بمدى قدرة الدولة على تجاوز حالة التشتت التنظيمي، وتفعيل التنسيق بين الأجهزة الأمنية والمدنية ضمن إطار قانوني واضح، يضمن سرعة الاستجابة ووضوح المسؤوليات وتكامل الأدوار، وهو ما يُعدُّ شرطاً أساسياً لبناء منظومة وطنية فعالة للأمن السيبراني في مواجهة التهديدات المتزايدة.(٥٢)

رقم الإيداع في دار الكتب والوثائق :2895 لسنة 2025م

الفرع الثاني

تبادل المعلومات والإنذارات المبكرة بين السلطات

تبادل المعلومات والإنذارات المبكرة بين السلطات يُعدُّ من أبرز عناصر الفعالية في منظومة الأمن السيبراني، إذ يشكل الأساس الذي تُبنى عليه الاستجابة السريعة والمنسقة للتهديدات الرقمية في بيئة تتسم بالتغير المستمر والتعقيد التقني، إذ تصبح القدرة على مشاركة البيانات والتحذيرات في الوقت المناسب بين الجهات المعنية أمراً حاسماً في احتواء الهجمات السيبرانية والحد من آثارها، وهذا التبادل لا يقتصر على المعلومات التقنية البحتة فحسب، بل يشمل أيضاً التحليلات الاستخبارية والتقارير الجنائية والمؤشرات الفنية للهجمات ونقاط الضعف المكتشفة في الأنظمة، ما يتيح للسلطات المختلفة بناء صورة متكاملة عن طبيعة التهديد واتجاهه المحتمل.(٥٣)

في هذا السياق الوطني، يتطلب هذا النوع من التعاون وجود قنوات اتصال مؤسسية وآمنة تتيح للجهات الأمنية والهيئات التنظيمية والمؤسسات المدنية تبادل المعلومات دون تأخير أو تعقيد بيروقراطي، كما أن فعالية هذا التبادل تعتمد على وجود ثقة متبادلة بين الأطراف وإطار قانوني يُنظم عملية المشاركة، ويُحدد المسؤوليات ويضمن حماية المعلومات الحساسة من التسريب أو سوء الاستخدام في حالات الأزمات السيبرانية التي قد يكون حدوثها في دقائق معدودة وهي كفيلة بتحديد مصير شبكة كاملة، ولذلك فإن الإنذار المبكر المبني على معلومات دقيقة ومحدثة، يُعدُّ من أهم أدوات الوقاية والاستجابة.(٥٤)

إن الإنذارات المبكرة التي تصدرها عادة مراكز الاستجابة للحوادث السيبرانية أو الجهات الاستخبارية، تُرسل إلى الجهات المعنية لاتخاذ التدابير الوقائية مثل تحديث الأنظمة أو تعطيل بعض الخدمات مؤقتًا أو تفعيل خطط الطوارئ، وتزداد أهمية هذه الإنذارات عندما تكون الهجمات ذات طابع منسق أو عابر للحدود، حيث يتطلب الأمر تنسيقاً داخلياً بين السلطات إلى جانب التعاون مع الشركاء الإقليميين والدوليين، كما أن تبادل المعلومات لا يقتصر على أوقات الأزمات بل يمتد إلى مراحل ما قبل الهجوم من خلال مشاركة نتائج تقييمات المخاطر والتقارير الدورية والتوصيات الفنية، ما يُسهم في رفع مستوى الجاهزية الوطنية.(٥٥)

وفي العراق، لا تزال آليات تبادل المعلومات والإنذارات المبكرة في طور التأسيس في ظل غياب قانون وطني شامل للأمن السيبراني يُنظم هذه العملية بشكل واضح، ومع ذلك بدأت بعض الجهات مثل المركز الوطني للأمن السيبراني ومديرية مكافحة الجرائم الإلكترونية وهيئة الإعلام والاتصالات في تطوير قنوات اتصال داخلية لتبادل البيانات المتعلقة بالحوادث السيبرانية، وإن كانت هذه الجهود لا تزال محدودة وتعتمد على التنسيق الإداري

رقم الإيداع في دار الكتب والوثائق :2895 لسنة 2025م

أكثر من كونها مؤطرة قانونياً، إذ أن الحاجة إلى إطار تشريعي يُنظم هذا التبادل باتت ملحة، خاصة مع تزايد الهجمات التي تستهدف البنية التحتية الرقمية وضرورة وجود استجابة موحدة وسريعة.[٥٦]

إن بناء منظومة فعالة لتبادل المعلومات والإنذارات المبكرة بين السلطات لا يُعدُّ ترفاً تنظيمياً، بل هو ضرورة أمنية تفرضها طبيعة التهديدات السيبرانية، ويتطلب استثماراً في البنية التحتية التقنية من خلال تدريب الكوادر وتطوير السياسات وتعزيز الثقة بين الجهات المعنية، فكلما كانت المعلومات تُشارك بسرعة وبدقة، زادت قدرة الدولة على التصدي للهجمات وتقليص آثارها وحماية مصالحها الحيوية في الفضاء الرقمي.[٥٧]

المطلب الثاني

التحديات والفرص في تفعيل الاختصاصات المشتركة

يُشكل تفعيل الاختصاصات المشتركة بين السلطات في مجال الأمن السيبراني خطوة ضرورية لتعزيز فعالية الاستجابة الوطنية للتهديدات الرقمية، ومع أن هذا التفعيل يفتح آفاقاً واسعة للتكامل التنظيمي وتبادل الخبرات، إلا أنه يواجه في الوقت ذاته تحديات قانونية وإدارية وتقنية قد تعيق تحقيق التنسيق المنشود[٥٨]، إذ تتقاطع في هذا السياق فرص واعدة لبناء منظومة سيبرانية متماسكة مع صعوبات تتطلب حلولًا مبتكرة وإرادة سياسية واضحة، ما يجعل من دراسة هذا المطلب ضرورة لفهم الواقع التنظيمي وإمكانات تطويره.

بناءاً على ما سبق، سندرس هذا المطلب في فرعين وذلك وفق الآتي:

الفرع الأول

التحديات القانونية والتقنية في توزيع المسؤوليات

يُشكل توزيع المسؤوليات في مجال الأمن السيبراني تحدياً معقداً على المستويين القانوني والتقني، خاصة في الدول التي لا تزال في طور بناء منظومتها السيبرانية، كما هو الحال في العراق، فغياب قانون وطني شامل ينظم الأمن السيبراني يؤدي إلى حالة من التداخل في الصلاحيات بين الجهات المختلفة، ويخلق فراغات تنظيمية تعيق الاستجابة الفعالة للتهديدات الرقمية، من الناحية القانونية، يواجه العراق إشكالية في تحديد الجهة المخولة بوضع السياسات السيبرانية، والجهة المسؤولة عن تنفيذها، والجهة التي تملك صلاحية التحقيق والمساءلة، وهو ما ينعكس على بطء التنسيق، وتضارب القرارات، وضعف المساءلة القانونية.[٥٩]

إنَّ المشهد القانوني العراقي في هذا المجال لا يزال غير مكتمل، إذ لم يُقر حتى الآن قانون خاص بالأمن السيبراني، رغم وجود مسودات ومشاريع قوانين مثل مشروع قانون الجرائم المعلوماتية، الذي يركز في جوهره

رقم الإيداع في دار الكتب والوثائق :2895 لسنة 2025م

على تجريم الأفعال الإلكترونية دون أن يتناول بشكل شامل مسألة توزيع المسؤوليات أو تنظيم العلاقة بين الجهات الأمنية والمدنية، هذا القصور التشريعي ينعكس على الواقع العملي، حيث تعمل جهات متعددة مثل وزارة الداخلية وهيئة الإعلام والاتصالات ووزارة الاتصالات والمركز الوطني للأمن السيبراني دون وجود إطار قانوني يُحدد بدقة حدود اختصاص كل منها، أو يُنظم آليات التنسيق بينها، مما يؤدي إلى تكرار الجهود أحياناً أو إلى غياب الاستجابة الموحدة في أوقات الأزمات.(٦٠)

أما من الناحية التقنية، فإن التحديات لا تقل تعقيداً، إذ إن توزيع المسؤوليات يتطلب وجود بنية تحتية رقمية متكاملة وقواعد بيانات مشتركة ومنصات لتبادل المعلومات ونظم إنذار مبكر، وهي عناصر لا تزال في طور التطوير في العراق، كما أن تفاوت القدرات التقنية بين الجهات المختلفة يُضعف من فعالية التنسيق، حيث تمتلك بعض المؤسسات أدوات متقدمة للرصد والتحليل، في حين تفتقر أخرى إلى الحد الأدنى من الكوادر المؤهلة أو التجهيزات الفنية، ما يخلق فجوة في الأداء ويُعيق بناء استجابة وطنية موحدة(٦١).

إضافة إلى ذلك، فإن غياب المعايير الوطنية الموحدة في مجال الأمن السيبراني يؤدي إلى اختلاف في طرق التعامل مع التهديدات وتباين في تقييم المخاطر وتضارب في الإجراءات المتخذة، وهو ما يُبرز الحاجة إلى إطار تنظيمي يُلزم جميع الجهات باتباع سياسات ومعايير موحدة ويُحدد آليات تبادل المعلومات ويُرسّخ مبدأ التكامل القانوني، كما أن التحديات التقنية تتفاقم في ظل ضعف الاستثمار في البنية التحتية السيبرانية وغياب برامج تدريب وطنية مستدامة، مما يجعل من الصعب بناء منظومة متكاملة لتوزيع المسؤوليات على أسس مهنية وتقنية راسخة.(٦٢)

في المحصلة النهائية، فإن التحديات القانونية والتقنية في توزيع المسؤوليات داخل منظومة الأمن السيبراني في العراق تُعدُّ من أبرز العقبات التي تَحول دون بناء استجابة فعالة ومستدامة للتهديدات الرقمية، إذ أن تجاوز هذه التحديات يتطلب إرادة سياسية واضحة لإقرار تشريعات شاملة وتطوير البنية التحتية الرقمية وتعزيز القدرات التنظيمية، بما يضمن وضوح الأدوار وتكامل الجهود وفعالية الأداء في مواجهة المخاطر السيبرانية المتزايدة.(٦٣)

الفرع الثاني

فرص بناء منظومة وطنية متكاملة للأمن السيبراني

يمثل بناء منظومة وطنية متكاملة للأمن السيبراني فرصة استراتيجية للعراق لتعزيز أمنه الرقمي وحماية مصالحه الحيوية ومواكبة التحولات العالمية في مجال التكنولوجيا والمعلومات، إذ إن هذه الفرصة تنبع من إدراك متزايد

رقم الإيداع في دار الكتب والوثائق :2895 لسنة 2025م

لدى صناع القرار بأهمية الأمن السيبراني كجزء لا يتجزأ من الأمن القومي، والحاجة إلى تجاوز المعالجات الجزئية أو الظرفية نحو تأسيس بنية مؤسسية وتشريعية قادرة على الاستجابة للتحديات الرقمية المتصاعدة، ورغم أن العراق لا يمتلك حتى الآن قانوناً شاملاً ومُقرَّاً خاصاً بالأمن السيبراني، إلا أن هذا الفراغ التشريعي لا يُعدُّ عائقاً مطلقاً، بل يمكن إعتباره مساحة مفتوحة لإعادة البناء على أسس حديثة تستفيد من تجارب الدول الأخرى، وتُراعى فيها الخصوصية الوطنية.(٦٤)

الفرصة الحقيقية تَكمُن في إمكانية صياغة قانون وطني متكامل يُنظم الأمن السيبراني من منظور شمولي، لا يقتصر على تجريم الأفعال الإلكترونية، بل يمتد إلى تحديد الأدوار التنظيمية وتوزيع الصلاحيات ووضع آليات التنسيق وتحديد معايير الحماية وضمان التوازن بين متطلبات الأمن وحماية الحقوق والحريات، مثل هذا القانون يمكن أن يُشكل الإطار المرجعي الذي تنطلق منه السياسات الوطنية، ويُعزز من قدرة الدولة على بناء شراكات فعالة مع القطاع الخاص والمجتمع المدني والمؤسسات الأكاديمية، بما يُسهم في تطوير بيئة رقمية آمنة ومحفزة على الابتكار.(٦٥)

إلى جانب الجانب التشريعي، تبرز فرص أخرى على المستوى القانوني، حيث يمكن للعراق أن يُفعّل دور المركز الوطني للأمن السيبراني ليكون الجهة المحورية في التنسيق بين مختلف الجهات الأمنية والمدنية وتطوير قدرات الرصد والاستجابة وإعداد الخطط الوطنية وتنفيذ التدريبات الدورية وبناء قواعد بيانات مشتركة ومنصات للإنذار المبكر، كما أن وجود إرادة سياسية واضحة لتبني استراتيجية وطنية للأمن السيبراني، كما أُعلن في السنوات الأخيرة، يُعدُّ مؤشراً إيجابياً على وجود استعداد لتطوير هذه المنظومة، شريطة أن تُترجم هذه الاستراتيجية إلى خطوات تنفيذية ملموسة مدعومة بالتشريعات والموارد البشرية والتقنية.(٦٦)

الفرص لا تقتصر على الداخل، بل تمتد إلى إمكانية الانخراط في شبكات التعاون الإقليمي والدولي، والاستفادة من المبادرات العالمية في مجال تبادل المعلومات وبناء القدرات وتطوير السياسات، وهو ما يُعزز من موقع العراق في خارطة الأمن السيبراني العالمية ويُسهم في نقل الخبرات والتقنيات ورفع مستوى الجاهزية الوطنية، كما أن الاستثمار في التعليم والتدريب ودعم البحث العلمي في مجالات الأمن السيبراني، يُعدُّ من أهم الفرص التي يمكن أن تُسهم في بناء جيل جديد من الكفاءات القادرة على قيادة هذا القطاع الحيوي.(٦٧)

إن بناء منظومة وطنية متكاملة للأمن السيبراني في العراق ليس مجرد مشروع تقني أو قانوني، بل هو مشروع وطني بامتياز، يتطلب رؤية استراتيجية وتخطيطًا طويل الأمد وتعاوناً وثيقاً بين السلطات ومشاركة فاعلة من

رقم الإيداع في دار الكتب والوثائق :2895 لسنة 2025م

المجتمع، وإذا ما استُثمرت هذه الفرص بشكل مدروس، فإن العراق سيكون قادراً على بناء درع رقمي يحمي مصالحه ويُعزز مناعته السيبرانية ويُمهّد الطريق نحو تحول رقمي آمن ومستدام.[٦٨]

الخاتمة

أثبتت الدراسة إن إدارة المخاطر السيبرانية في العراق تتطلب مقاربة شاملة تتجاوز الجهود الفردية للسلطات نحو بناء منظومة مؤسساتية متكاملة تقوم على توزيع واضح للاختصاصات وتنسيق فعّال بين الجهات المعنية، وقد أظهرت التحليلات أن غياب الإطار القانوني الشامل يشكل عائقاً رئيسياً أمام تفعيل هذه الاختصاصات، في حين أن هناك فرصاً حقيقية لتطوير البنية السيبرانية الوطنية من خلال الاستفادة من التجارب المقارنة، وتعزيز التعاون بين السلطات وتحديث التشريعات بما يتلائم مع طبيعة التهديدات الرقمية، إن تحقيق الأمن السيبراني لا يمكن أن يتم بمعزل عن التكامل بين السلطات التنفيذية والتشريعية والقضائية، وهو ما يتطلب إرادة سياسية واضحة وتخطيطاً استراتيجياً طويل الأمد، وإشراكاً فعّالاً لجميع الفاعلين في هذا المجال، وفي الختام توصلنا لمجموعة من النتائج والمقترحات:

النتائج:

١-يتسم الإطار القانوني العراقي بالقصور في تنظيم توزيع الاختصاصات السيبرانية، نتيجة غياب قانون شامل ومحدد للأمن السيبراني .

٢-تتعدد الجهات التنفيذية المعنية بالأمن السيبراني دون وجود تنسيق مؤسسي فعّال، مما يؤدي إلى تداخل الصلاحيات وضعف الاستجابة .

٣-يواجه القضاء العراقي تحديات في تكييف الجرائم السيبرانية ضمن النصوص القانونية التقليدية، ما يَحدُّ من فعالية الرقابة القضائية .

٤-هناك إدراك متزايد بأهمية الأمن السيبراني على المستوى الوطني، ما يفتح المجال أمام فرص واعدة لبناء منظومة متكاملة إذا ما تم استثمارها بشكل مدروس.

المقترحات:

١-الإسراع في إقرار قانون وطني شامل للأمن السيبراني يُنظم توزيع الاختصاصات بين السلطات ويُحدد آليات التنسيق فيما بينهم .

٢-إنشاء هيئة وطنية عليا تُعنى بتنسيق جهود الأمن السيبراني بين الجهات الأمنية والمدنية، وتكون ذات صلاحيات واضحة ومحددة .

٣-تطوير القدرات التقنية والبشرية للجهات القضائية والتشريعية لتمكينها من مواكبة تطورات الجرائم السيبرانية والتشريعات الرقمية .

رقم الإيداع في دار الكتب والوثائق :2895 لسنة 2025م

٤-تعزيز التعاون مع الدول ذات التجارب الرائدة في الأمن السيبراني والاستفادة من خبراتها في بناء السياسات والتشريعات الوطنية.

الهوامش

(١) نورة شلوش: القرصنة الإلكترونية في الفضاء السيبراني، التهديد المتصاعد لأمن الدول، بحث منشور في مجلة مركز بابل للدراسات الإنسانية، العدد ٦، المجلد ٨، جامعة بابل، العراق، ٢٠١٨، ص ١٨٨.

(٢) حسين محمد الغول: جرائم شبكة الانترنت والمسؤولية الجزائية الناشئة عنها، الطبعة الاولى، مكتبة بدران الحقوقية للنشر والتوزيع، بيروت، لبنان، ٢٠١٧، ص٢٢.

(٣) محمد علي سالم: الجريمة المعلوماتية، مجلة جامعة بابل، العدد ٢، المجلد ١٤، العراق، ٢٠٠٧، ص ١٨.

(٤) محمد علي سالم، الجريمة المعلوماتية، مرجع سابق، ص٣١.

(٥) جلال محمد الزغبي وأسامة أحمد المناعسة: جرائم تقنية المعلومات الالكترونية، الطبعة الأولى، منشورات دار الثقافة للنشر والتوزيع، عمان، الأردن، ٢٠١٠، ص٣٤.

(٦) سعد الحاج بكري: شبكات الاتصال وتوظيف المعلومات في مكافحة الجريمة " التشريع المقارن" المكتبة العربية للدراسات والتدريب، مصر، ٢٠١٥، ص ١١.

(٧) محمد علي سالم: الجريمة المعلوماتية، مرجع سابق، ص٥٦.

(٨) نورة شلوش: القرصنة الإلكترونية في الفضاء السيبراني، التهديد المتصاعد لأمن الدول، مرجع سابق، ص١٩١.

(٩) أحمد فخري رشيد: المواجهة الأمنية للجريمة المعلوماتية، الطبعة الأولى، دار السنهوري، بغداد، ٢٠١٨، ص ١٧.

(١٠) محروس نصار غريب، الجريمة المعلوماتية، مجلة التقني، العدد٩، المجلد ٢٤، هيئة التعليم التقني، بغداد، ٢٠١١، ص ١٢٠.

(١١) جلال محمد الزغبي وأسامة أحمد المناعسة: جرائم تقنية المعلومات الالكترونية، مرجع سابق، ص٥١.

(١٢) أحمد فخري رشيد: المواجهة الأمنية للجريمة المعلوماتية، مرجع سابق، ص٢٤.

(١٣) محمد علي سالم: الجريمة المعلوماتية، مرجع سابق، ص٧٢.

(١٤) سعد الحاج بكري: شبكات الاتصال وتوظيف المعلومات في مكافحة الجريمة " التشريع المقارن" المكتبة العربية للدراسات والتدريب، مصر، ٢٠١٥، ص ١١.

(١٥) محروس نصار غريب: الجريمة المعلوماتية، مرجع سابق، ص١٢٦

(١٦) جلال محمد الزغبي وأسامة أحمد المناعسة: جرائم تقنية المعلومات الالكترونية، مرجع سابق، ص٧٨.

(١٧) أحمد فخري رشيد: المواجهة الأمنية للجريمة المعلوماتية، مرجع سابق، ص٣٦.

(١٨) محمد علي سالم: الجريمة المعلوماتية، مرجع سابق، ص٨٤.

(١٩) محمود مدين عبد الرحمن: الجريمة الإلكترونية وتحديات الأمن القومي، المصرية للنشر والتوزيع، القاهرة، ٢٠١٧، ص ٢٢.

(٢٠) أحمد عبيس نعمة الفتلاوي: الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، العدد الرابع، السنة الثامنة، كلية جامعة بابل، العراق، ٢٠١٦، ص١٤.

رقم الإيداع في دار الكتب والوثائق :2895 لسنة 2025م

(٢١) محمود مدين عبد الرحمن: الجريمة الإلكترونية وتحديات الأمن القومي، مرجع سابق، ص٨٤.

(٢٢) قانون الامن السيبراني الاردني رقم ١٦ لسنة ٢٠١٩، متاح على الموقع الالكتروني: https://althunibat.com/ar/jordan-cybersecurity-law-2019/ تاريخ الزيارة: ٢٠٢٥/١٢/١٧.

(٢٣) قانون الجرائم الإلكترونية الأردني رقم ١٧ لسنة ٢٠٢٣ والمنشور في الجريدة الرسمية رقم (٥٨٧٤) الصادر بتاريخ ٢٠٢٣/٨/١٣.

((٢٤)) ينظر في تفصيل ذلك: قانون التوقيع الالكتروني والمعاملات الالكترونية العراقي رقم (٧٨) لسنة ٢٠١٢، والقانون الاتحادي رقم (٢) لسنة ٢٠٠٦ بشأن مكافحة جرائم تقنية المعلومات في الامارات العربية المتحدة، والمرسوم السلطاني رقم (٢٠٠١/٢٧) حول تعديل بعض احكام قانون الجزاء العماني بإضافة المادة (٢٧٦) حول جرائم الحاسوب.

(٢٥) حسين محمد الغول: جرائم شبكة الانترنت والمسؤولية الجزائية الناشئة عنها، مرجع سابق، ص٥٤.

(٢٦) سليم عبدالله الجبوري: الحماية القانونية لمعلومات شبكة الإنترنت، منشورات الحلبي الحقوقية، بيروت، ٢٠١١، ص ٢٥.

(٢٧) منير محمد الجنبيهي وممدوح محمد الجنبيهي: امن المعلومات الالكترونية، دار الفكر الجامعي، الاسكندرية، ٢٠٠٥، ص ٧.

(٢٨) محروس نصار غريب: الجريمة المعلوماتية، مرجع سابق، ص١٣١.

(٢٩) أحمد فخري رشيد: المواجهة الأمنية للجريمة المعلوماتية، مرجع سابق، ص٦٢.

(٣٠) أحمد عبيس نعمة الفتلاوي: الهجمات السيبرانية، مرجع سابق، ص١٨

(٣١) علي محمد كاظم الموسوي: المشاركة المباشرة في الهجمات السيبرانية، مرجع سابق، ص٩١.

(٣٢) نورة شلوش: القرصنة الإلكترونية في الفضاء السيبراني، التهديد المتصاعد لأمن الدول، مرجع سابق، ص١٩٤.

(٣٣) علي محمد كاظم الموسوي: المشاركة المباشرة في الهجمات السيبرانية، الطبعة الأولى، منشورات شركة المؤسسة الحديثة للكتاب، بيروت، ٢٠١٩، ص ٥٣-٥٤.

(٣٤) محمد علي سالم: الجريمة المعلوماتية، مرجع سابق، ص١٢١.

(٣٥)أحمد عبيس الفتلاوي: "الهجمات السيبرانية" " مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي، مجلة المحقق للعلوم القانونية والسياسية، العدد الرابع، مصر، ٢٠١٦، ص ٢٢.

(٣٦) سراب ثامر أحمد: الهجمات على شبكات الحاسوب في القانون الدولي الإنساني، أطروحة اعدت لنيل درجة الدكتوراه، كلية الحقوق، جامعة النهرين، العراق، ٢٠١٥، ص ١١٧.

(٣٧) خالد حسن أحمد لطفي: الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، مصر، ٢٠٢٠، ص ١٣.

(٣٨) علي محمد كاظم الموسوي: المشاركة المباشرة في الهجمات السيبرانية، مرجع سابق، ص١٢٨.

(٣٩) سراب ثامر أحمد: الهجمات على شبكات الحاسوب في القانون الدولي الإنساني، مرجع سابق، ص١٦١.

(٤٠) بهاء شاهين: شبكة الأنترنت، الطبعة الثانية، العربية لعلوم الحاسبات، القاهرة، ٢٠٠١، ص ٥٣.

(٤١) حسين محمد الغول: جرائم شبكة الانترنت والمسؤولية الجزائية الناشئة عنها، مرجع سابق، ص١١٦.

(٤٢) سراب ثامر أحمد: الهجمات على شبكات الحاسوب في القانون الدولي الإنساني، مرجع سابق، ص١٨٤.

(٤٣) جمال إبراهيم الحيدري: الجرائم الالكترونية وسبل معالجتها، منشورات مكتبة السنهوري، بغداد، ٢٠١٢، ص ٣٣.

رقم الإيداع في دار الكتب والوثائق :2895 لسنة 2025م

(٤٤) خالد حسن أحمد لطفي: الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية، مرجع سابق، ص١١٤.

(٤٥) سعد الحاج بكري: شبكات الاتصال وتوظيف المعلومات في مكافحة الجريمة " التشريع المقارن"، مرجع سابق، ص٤٤.

(٤٦) سراب ثامر أحمد: الهجمات على شبكات الحاسوب في القانون الدولي الإنساني، مرجع سابق، ص١٩٧.

(٤٧) جلال محمد الزغبي وأسامة أحمد المناعسة: جرائم تقنية المعلومات الالكترونية، مرجع سابق، ص١١٢.

(٤٨) علي نعمة جواد الزرفي: الجريمة المعلوماتية الماسة بالحياة الخاصة دراسة مقارنة، المكتب الجامعي الحديث، القاهرة، ٢٠١٩، ص٣٨.

(٤٩) محمد محمود المكاوي: الجوانب الأخلاقية والاجتماعية للجرائم المعلوماتية، الطبعة الأولى، المكتبة العصرية، بيروت، ٢٠١٠، ص٩٣.

(٥٠) خالد حسن أحمد لطفي: الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية، مرجع سابق، ص١٤٢.

(٥١) منير محمد الجنبيهي وممدوح محمد الجنبيهي: امن المعلومات الالكترونية، مرجع سابق، ص٥٤.

(٥٢) سعد الحاج بكري: شبكات الاتصال وتوظيف المعلومات في مكافحة الجريمة " التشريع المقارن"، مرجع سابق، ص٦٨.

(٥٣) علي نعمة جواد الزرفي: الجريمة المعلوماتية الماسة بالحياة الخاصة دراسة مقارنة، مرجع سابق، ص٨٧.

(٥٤) إيهاب السنباطي: الترجمة الجديدة والكاملة للاتفاقيات المتعلقة بالجريمة الالكترونية، دار النهضة العربية، القاهرة، ٢٠٠٨، ص ١٢-٢١.

(٥٥) سعد الحاج بكري: شبكات الاتصال وتوظيف المعلومات في مكافحة الجريمة " التشريع المقارن"، مرجع سابق، ص٩٣.

(٥٦) علي نعمة جواد الزرفي، الجريمة المعلوماتية الماسة بالحياة الخاصة دراسة مقارنة، مرجع سابق، ص٨٧.

(٥٧) إيهاب السنباطي: الترجمة الجديدة والكاملة للاتفاقيات المتعلقة بالجريمة الالكترونية، مرجع سابق، ص٤٨.

(٥٨) علي محمد كاظم الموسوي: المشاركة المباشرة في الهجمات السيبرانية، مرجع سابق، ص١٦٩.

(٥٩) يوسف حسن يوسف: الجرائم الدولية للإنترنت، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، ٢٠١١، ص٣٦.

(٦٠) طارق ابراهيم الدسوقي عطية: عولمة الجريمة، (القسم الأول)، دار الجامعة الجديدة، الاسكندرية، مصر، ٢٠١٠، ص٢٤٢.

(٦١) محمد عبدالله ابو بكر سلامة: جرائم الكومبيوتر والإنترنت، منشأة المعارف، الاسكندرية، مصر، ٢٠٠٦، ص١٢٠.

(٦٢) يوسف حسن يوسف: الجرائم الدولية للإنترنت، مرجع سابق، ص٧١.

(٦٣) نائلة عادل محمد فريد قورة: جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، بيروت، ٢٠٠٥، ص٢٤٨.

(٦٤) نائلة عادل محمد فريد قورة: جرائم الحاسب الآلي الاقتصادية، مرجع سابق، ص٢٥١

(٦٥) زهراء عماد محمد كلنتر: المسؤولية الدولية الناشئة عن الهجمات السيبرانية، مكتبة القانون المقارن، بغداد، ٢٠٢١، ص٨٦.

(٦٦) زهراء عماد محمد كلنتر: المسؤولية الدولية الناشئة عن الهجمات السيبرانية، مرجع سابق، ص٩٣.

(٦٧) محمد عبدالله ابو بكر سلامة: جرائم الكومبيوتر والإنترنت، مرجع سابق، ص١٣٧.

(٦٨) منى الأشقر جبور: الامن السيبراني، التحديات ومستلزمات المواجهة، اللقاء السنوي الأول للمختصين في أمن وسلامة الفضاء السيبراني، جامعة الدول العربية، المركز القانوني للبحوث القانونية والقضائية، بيروت، ٢٠١٢، ص ٣.

رقم الإيداع في دار الكتب والوثائق :2895 لسنة 2025م

المصادر

أولاً-الكتب:

١. أحمد فخري رشيد: المواجهة الأمنية للجريمة المعلوماتية، الطبعة الأولى، دار السنهوري، بغداد، ٢٠١٨.
٢. إيهاب السنباطي: الترجمة الجديدة والكاملة للاتفاقيات المتعلقة بالجريمة الالكترونية، دار النهضة العربية، القاهرة، ٢٠٠٨.
٣. بهاء شاهين: شبكة الأنترنت، الطبعة الثانية، العربية لعلوم الحاسبات، القاهرة، ٢٠٠١.
٤. جلال محمد الزغبي وأسامة أحمد المناعسة: جرائم تقنية المعلومات الالكترونية، الطبعة الأولى، منشورات دار الثقافة للنشر والتوزيع، عمان، الأردن، ٢٠١٠.
٥. جمال إبراهيم الحيدري: الجرائم الالكترونية وسبل معالجتها، منشورات مكتبة السنهوري، بغداد، ٢٠١٢.
٦. حسين محمد الغول: جرائم شبكة الانترنت والمسؤولية الجزائية الناشئة عنها، الطبعة الاولى، مكتبة بدران الحقوقية للنشر والتوزيع، بيروت، لبنان، ٢٠١٧.
٧. خالد حسن أحمد لطفي: الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، مصر، ٢٠٢٠.
٨. زهراء عماد محمد كلنتر: المسؤولية الدولية الناشئة عن الهجمات السيبرانية، مكتبة القانون المقارن، بغداد، ٢٠٢١.
٩. سعد الحاج بكري: شبكات الاتصال وتوظيف المعلومات في مكافحة الجريمة " التشريع المقارن" المكتبة العربية للدراسات والتدريب، مصر، ٢٠١٥.
١٠. سعد الحاج بكري: شبكات الاتصال وتوظيف المعلومات في مكافحة الجريمة " التشريع المقارن" المكتبة العربية للدراسات والتدريب، مصر، ٢٠١٥.
١١. سليم عبدالله الجبوري: الحماية القانونية لمعلومات شبكة الإنترنت، الطبعة الاولى، منشورات الحلبي الحقوقية، بيروت، ٢٠١١.
١٢. طارق ابراهيم الدسوقي عطية: عولمة الجريمة، (القسم الأول) ، دار الجامعة الجديدة، الاسكندرية، مصر، ٢٠١٠.
١٣. علي محمد كاظم الموسوي، المشاركة المباشرة في الهجمات السيبرانية، الطبعة الأولى، منشورات شركة المؤسسة الحديثة للكتاب، بيروت، ٢٠١٩.
١٤. علي نعمة جواد الزرفي، الجريمة المعلوماتية الماسة بالحياة الخاصة دراسة مقارنة، المكتب الجامعي الحديث، القاهرة، ٢٠١٩.
١٥. محروس نصار غريب، الجريمة المعلوماتية، مجلة التقني، العدد ٩، المجلد ٢٤، هيئة التعليم التقني، بغداد، ٢٠١١.
١٦. محمد عبدالله ابو بكر سلامة، جرائم الكومبيوتر والإنترنت، منشأة المعارف، الاسكندرية، مصر، ٢٠٠٦.
١٧. محمد محمود المكاوي، الجوانب الأخلاقية والاجتماعية للجرائم المعلوماتية، الطبعة الأولى، المكتبة العصرية، بيروت، ٢٠١٠،
١٨. محمود مدين عبد الرحمن، الجريمة الإلكترونية وتحديات الأمن القومي، المصرية للنشر والتوزيع، القاهرة، ٢٠١٧.
١٩. منير محمد الجنبيهي وممدوح محمد الجنبيهي، امن المعلومات الالكترونية، دار الفكر الجامعي، الاسكندرية، ٢٠٠٥.
٢٠. نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، بيروت، ٢٠٠٥.
٢١. يوسف حسن يوسف، الجرائم الدولية للإنترنت، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، ٢٠١١.

ثانياً-الأبحاث المجلات والدوريات

رقم الإيداع في دار الكتب والوثائق :2895 لسنة 2025م

١. أحمد عبيس نعمة الفتلاوي: الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، العدد الرابع، السنة الثامنة، كلية جامعة بابل، العراق، ٢٠١٦.
٢. محمد علي سالم: الجريمة المعلوماتية، مجلة جامعة بابل، العدد ٢، المجلد ١٤، العراق، ٢٠٠٧.
٣. منى الأشقر جبور: الامن السيبراني، التحديات ومستلزمات المواجهة، اللقاء السنوي الأول للمختصين في أمن وسلامة الفضاء السيبراني، جامعة الدول العربية، المركز القانوني للبحوث القانونية والقضائية، بيروت، ٢٠١٢.
٤. نورة شلوش: القرصنة الإلكترونية في الفضاء السيبراني، التهديد المتصاعد لأمن الدول، بحث منشور في مجلة مركز بابل للدراسات الإنسانية، العدد ٦، المجلد ٨، جامعة بابل، العراق، ٢٠١٨.

ثالثاً-الرسائل الجامعية:

سراب ثامر أحمد، الهجمات على شبكات الحاسوب في القانون الدولي الإنساني، أطروحة اعدت لنيل درجة الدكتوراه، كلية الحقوق، جامعة النهرين، العراق، ٢٠١٥.

رابعاً-القوانين:

١. القانون الاتحادي رقم (٢) لسنة ٢٠٠٦ بشأن مكافحة جرائم تقنية المعلومات في الامارات العربية المتحدة.
٢. قانون الامن السيبراني الاردني رقم ١٦ لسنة ٢٠١٩، متاح على الموقع الالكتروني : https://althunibat.com/ar/jordan-cybersecurity-law-2019/
٣. قانون التوقيع الالكتروني والمعاملات الالكترونية العراقي رقم (٧٨) لسنة ٢٠١٢.
٤. قانون الجرائم الإلكترونية الأردني رقم ١٧ لسنة ٢٠٢٣ والمنشور في الجريدة الرسمية رقم (٥٨٧٤) الصادر بتاريخ ٢٠٢٣/٨/١٣.
٥. المرسوم السلطاني رقم (٢٠٠١/٢٧) حول تعديل بعض احكام قانون الجزاء العماني.

رقم الإيداع في دار الكتب والوثائق :2895 لسنة 2025م