العدد 19 تشرين الثاني 2025
المجلة العراقية للبحوث الانسانية والاجتماعية والعلمية
No.19 – Nov 2025 Iraqi Journal of Humanitarian, Social and Scientific Research
Print ISSN 2710-0952 Electronic ISSN2790-1254

التعاون الدولي لمواجهة الجرائم السيبرانية
دراسة مقارنة بين التشريعات الوطنية والمعاهدات الدولية

Cooperation to Combat Cybercrime
A Comparative Study of National Legislation and International Trea

م.د مبين ماجد جابر

جامعة كربلاء(مركز الدراسات الاستراتيجية)

الخلاصة

يتناول البحث التعاون الدولي لمواجهة الجرائم السيبرانية من خلال دراسة مقارنة بين التشريعات الوطنية، مثل تلك الموجودة في العراق، والمعاهدات الدولية كاتفاقية بودابست والاتفاقية العربية لمكافحة جرائم تقنية المعلومات. يبرز البحث أهمية التعاون الدولي في التصدي للجرائم السيبرانية التي تتجاوز الحدود الوطنية، ويشير إلى الفجوات القانونية في الأنظمة الوطنية التي تعيق فعالية التصدي لهذه الجرائم. كما يناقش التحديات التي تواجه الدول في تنفيذ القوانين الحالية، مثل نقص الموارد والتكنولوجيا. يقدم البحث توصيات لتوحيد التشريعات الوطنية وتعزيز التعاون بين الدول، بالإضافة إلى تحديث القوانين بشكل دوري لمواكبة التطورات السريعة في تكنولوجيا المعلومات.

الكلمات المفتاحية:(التعاون الدولي ،الجرائم السيبرانية، التشريعات الوطنية، المعاهدات الدولية)

Abstract

The research addresses international cooperation to combat cybercrime through a comparative study of national legislations, such as those in Iraq, and international treaties like the Budapest Convention and the Arab Convention on Combating Cybercrime. The study highlights the importance of international collaboration in tackling cybercrimes that transcend national borders and points out the legal gaps in national systems that hinder effective responses to these crimes. It also discusses the challenges faced by countries in implementing existing laws, such as a lack of resources and technology. The research provides recommendations for harmonizing national legislations, enhancing cooperation among countries, and periodically updating laws to keep pace with rapid developments in information technology.

Keywords: (international cooperation, cybercrimes, national legislation, international treaties)

المقدمة

أصبحت الجرائم السيبرانية تهديدًا حقيقيًا للأمن الوطني والدولي، إذ تتجاوز آثارها الحدود الجغرافية وتؤثر على الأفراد والمجتمعات والدول. تبرز أهمية التعاون الدولي لمواجهة هذه الجرائم، حيث

تتطلب طبيعتها المعقدة استجابة قانونية موحدة تشمل التشريعات الوطنية والمعاهدات الدولية. يتناول هذا البحث دراسة مقارنة بين التشريعات الوطنية، مثل تلك الموجودة في العراق، والمعاهدات الدولية مثل اتفاقية بودابست لعام 2001 والاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010.

أولاً-أهمية البحث:

تتمثل أهمية هذا البحث في تسليط الضوء على الجهود المبذولة لمكافحة الجرائم السيبرانية، وفهم كيفية تأثير التشريعات الوطنية على الأمن السيبراني. كما يساهم البحث في تعزيز الوعي حول الفجوات القانونية الموجودة في الأنظمة الوطنية، ويقدم توصيات لتحسين استجابة الدول لمواجهة التهديدات السيبرانية. من خلال تحليل الأطر القانونية، يمكن للباحثين وصناع القرار فهم التحديات والفرص المرتبطة بالأمن السيبراني.

ثانيا- إشكالية البحث:

تتجلى إشكالية البحث في كيفية تحقيق توازن فعّال بين حماية الحقوق الفردية وضمان الأمن السيبراني، خاصة في ظل الفروقات الثقافية والقانونية بين الدول. بالإضافة إلى ذلك، يثير البحث تساؤلات حول فعالية التشريعات الحالية في مواجهة الجرائم السيبرانية، ومدى توافقها مع المعاهدات الدولية، وكذلك التحديات التي تواجهها الدول في تنفيذ هذه القوانين.

ثالثاً- منهجية البحث:

يعتمد البحث على منهجية تحليلية مقارنة، حيث يتم دراسة التشريعات الوطنية في العراق والدول العربية، ومقارنتها بالمعاهدات الدولية ذات الصلة. سيتم تحليل النصوص القانونية، وتقييم فعاليتها في التصدي للجرائم السيبرانية، مع التركيز على المبادرات الدولية والإقليمية. من خلال هذه المنهجية، يسعى البحث إلى تقديم رؤى واضحة حول مدى فعالية الجهود القانونية في مواجهة التهديدات السيبرانية، وتحديد الفجوات والتحديات التي تعيق التصدي لهذه الجرائم.

رابعاً-خطة البحث:

في سياق دارستنا لموضوع الجريمة في الفضاء السيبراني والإطار المفاهيمي لها وجهود مكافحتها، سنعمل على تقسيم هذه الدراسة من خلال مبحثين، حيث سنتناول في المبحث الأول، مفهوم السيبرانية ومواجهتها في القوانين العراقية، فيما سنستعرض في المبحث الثاني، جهود مواجهة الجرائم السيبرانية في أوروبا والعالم العربي.

المبحث الأول
مفهوم السيبرانية ومواجهتها في القوانين العراقية

تعتبر السيبرانية من المفاهيم الحديثة التي اكتسبت أهمية متزايدة في عصر التكنولوجيا الرقمية، حيث تشير إلى علم التحكم الآلي وتطبيقاته في الفضاء الإلكتروني. يعود أصل المصطلح إلى اليونانية، ويعكس قدرة الأنظمة على التحكم عن بُعد. في ظل التقدم التكنولوجي السريع، أصبحت الجرائم السيبرانية تهديدًا حقيقيًا للمجتمعات، مما يستدعي دراسة دقيقة لمفهومها وأبعادها. يتناول هذا المبحث التعريفات المختلفة للجريمة السيبرانية، والمعايير المتبعة في تصنيفها، بالإضافة إلى موقف المشرع العراقي من هذه الظاهرة التي تتطلب استجابة قانونية فعالة لحماية الأفراد والمصالح العامة.

ولغرض بيان هذا المبحث بشكل دقيق، سوف نقسمه على مطلبين، الأول بعنوان: الإطار المفاهيمي للفضاء السيبراني، اما الثاني بعنوان: موقع الجريمة السيبرانية في التنظيم التشريعي العراقي، **والتفاصيل على النحو الآتي:**

المطلب الأول: الإطار المفاهيمي للفضاء السيبراني

تشير المراجع العلمية إلى أن أول من استخدم مصطلح علم التحكم الآلي كان عالم الرياضيات (نوربرت وينر)، وكان ذلك في عام 1948 أثناء دراسة موضوع القيادة والسيطرة والاتصال في عالم الحيوان، وكذلك مجال الهندسة الميكانيكية.

أما فيما يخص البحث عن مصدر كلمة "سيبر" في المعاجم اللغوية، فيتبين انها يونانية الأصل وتعود إلى مصطلح (kybernetes) ، والتي ورد ذكرها في البداية في أدب الخيال العلمي وتعني القيادة أوالتحكم عن بعد، وبالرجوع إلى القواميس اللغوية، غالبًا ما لم تشر إلى مصدر كلمة السيبرانية باستثناء ما وجدناه في القاموس (المورد) حيث عرفها بالقول: السيبراني هو علم التحكم، ومصدره (علم التحكم الآلي) وهو مصدر يتوافق مع مفهوم الهجمات الإلكترونية، أي الاستيلاء على الأشياء والتحكم فيها عن بعد[1].

وتأكيدًا لما تم تقديمه سابقًا، لم تشر معظم القواميس المتخصصة في المصطلحات العسكرية بكلمة "سيبر" إلى مصدرها، أو التحكم في البرامج الإلكترونية الأخرى أو تعطيلها، بينما يعرّف قاموس مصطلحات أمن المعلومات المصطلح السيبراني بالقول: "هجوم عبر الفضاء الإلكتروني يهدف إلى التحكم في مواقع الويب أو البنية التحتية المحمية إلكترونيًا لتعطيلها أو تدميرها أو إتلافها أو تخريبها.

اما في اللغة العربية وبالرجوع إلى من يتقنها، نجد أن التحدي الذي وأجهوه في اختيار مصطلح قريب من مصطلح السيبرانية في اللغة الإنجليزية، ويدل على ذلك حقيقة أن الترجمة العربية للعنوان في اتفاقية مجلس أوروبا بشأن الجرائم الإلكترونية كانت ترجمة غير صحيحة، حيث تمت ترجمة العنوان إلى اللغة العربية باسم "اتفاقية الجرائم الإلكترونية" والسبب في ذلك يرجع إلى عدم وجود مصطلح مقابل في اللغة العربية.

وسنتكلم أيضا عن مدلول الهجمات السيبرانية فقهياً، فقد اختلفت الآراء في تقديم تعريف أو دلالة ثابتة للجريمة السيبرانية، لذلك قام بعض الكتاب والباحثين المتخصصين في هذا الصدد بتقسيمها إلى مجموعتين، الأولى مجموعة من التعريفات تقوم على معيار واحد، أو معيار شخصي يعتمد على المعرفة التقنية المتاحة لدى الشخص الذي ارتكب الجريمة (الحاسوب) أو موضوع الجريمة (المعلومات)، أو معيار شخصي يستند إلى المعرفة التقنية المتوفرة في شخص مرتكب الجريمة، وتستند المجموعة الثانية من التعريفات إلى مجموعة من المعايير وتتضمن تعريفات تسلط الضوء على أنماط الجريمة وموضوعها وبعض العناصر المتعلقة بآليات ارتكابها أو البيئة الرقمية أو الخصائص التي يتمتع بها الجاني نظرًا لوجود العديد من التعريفات التي قدمها المختصون، سيتم إبراز التعريفات المقدمة من أجل إلقاء نظرة على اتجاهات هذه التعريفات والنقد الموجه لها بشيء من التفصيل، على النحو التالي:

أولاً: التعريفات التي تستند إلى وسيلة ارتكاب الجريمة:

ويستند هذا الاتجاه إلى عرض تعريفه للجريمة الإلكترونية من خلال الحاسوب الذي يلعب أدوارًا مختلفة في ارتكاب الجريمة، وقد عرّفها الفقيه الألماني "تيدمان"على أنها "جميع أشكال السلوك غير

---

[1] أ.د. أمير فرج يوسف، مكافحة جريمة الإرهاب الإلكتروني، الإرهاب الرقمي في ظل اتفاقية مجلس التعاون لمكافحة الإرهاب، الطبعة الأولى، دار الكتب والدراسات العربية، الإسكندرية، 2015، ص 123.

القانوني (الضار بالمجتمع) التي يتم ارتكابها باستخدام الحاسوب، كما عرّفها "ليلس بال" على أنها فعل إجرامي يستخدم الكمبيوتر لارتكابه أداة رئيسية، وكذلك تعريف (ميري) على أنه" الفعل غير القانوني الذي يشارك فيه الحاسوب في عمله، وقد انتقد هذا الاتجاه على أساس أن الوسيلة لم يأخذها المشرع الجنائي في الاعتبار عند التجريم، حيث أن معظمها متساوي.

كما أن توافر أركان الجريمة بشكل جماعي هو موضوع النظر عند تطبيق النص، لذا فإن العودة إلى العمل الأساسي هي أساس التجريم وليس الوسيلة [2].

ثانياً: التعريفات التي تستند إلى موضوع الجريمة:

إن الجريمة وفقاً لهذا الاتجاه تعرف ليس من خلال وسيلة الجريمة بل من خلال موضوع الجريمة أي التي تقع على الحاسوب أو داخل نظامه، ومن هذه التعريفات تعريف (روسينت بال) بأنها كل «نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو التي تحول عن طريقه، وفي الفقه العربي عرفتها الدكتورة هدى قشقوش «بأنها مجموع الجرائم التي تتصل بالمعلوماتية، وعرفها الدكتور هلالي عبدالاله احمد «بأنها عمل أو امتناع عن عمل يأتيه الإنسان إضراراً بمكونات الحاسوب أو شبكات الاتصال به المحمية قانوناً والمعاقب على هذا الفعل بموجب القانون»، كما عرفها الدكتور نائل عبد الرحمن صالح بأنها: «سلوك غير مشروع معاقب عليه قانوناً صادر عن إرادة جرمية محله معطيات الحاسوب»، تم انتقاد هذا الاتجاه لأنه يتبنى معيارًا موضوعيًا يؤدي إلى تعريفات عامة ومطلقة لا تحدد الأفعال بدقة، ولا تأخذ في الاعتبار الجدل القائم حول مدى تطبيق قواعد التجريم التقليدية على أعمال الحذف والنسخ.

ثالثاً: التعريفات التي تستند إلى المعيار الشخصي:

يعرّف هذا الاتجاه الجريمة من خلال توفر المعرفة بتكنولوجيا المعلومات لمرتكب الجريمة، وقدم (ديفيد طومسون) هذه التعريفات على أنها "أي جريمة مطلوب ارتكابها إذا كان الجاني على علم بتكنولوجيا الحاسوب"، وفي نفس الاتجاه الذي حدده "شتاين شولبيرج" على أنه "أي عمل لا يمثل المعرفة القانونية لتكنولوجيا المعلومات ضروري لمرتكب الجريمة وللتحقيق والمقاضاة في الفقه العربي، عرفت نبيلة هبة هروال الجريمة بأنها" جرائم عابرة للحدود تحدث في أو من خلال الإنترنت من قبل شخص لديه معرفة أعلى به "[3].

كما تم انتقاد هذه التعريفات، لأن ارتكاب الأفعال التي تشكل جريمة لا يتطلب معرفة فائقة، حيث يمكن للشخص العادي إرسال بريد إلكتروني احتيالي، ويمكن أيضًا ارتكاب الجرائم الإلكترونية دون الحاجة إلى معرفة متعمقة، من أجل تطوير أدوات تسهل ارتكاب الجريمة مثل استخدام أدوات برامج الحاسوب المصممة للعثور على المنافذ المفتوحة أو كسر الحماية بكلمة مرور.

رابعاً: التعريفات ذات المعايير المتعددة:

قدم جزء من الفقه أكثر من معيار لتعريف الجرائم المذكورة، من خلال وصف السلوك، أي ارتكاب الجريمة بالحاسوب، بالإضافة إلى ربط السلوك بالمعالجة الآلية أو نقل البيانات، يستند القانون الذي يمكن أن ترتكبه المعلوماتية إلى افتراض تحقيق الربح، وكذلك تعريف الخبير الأمريكي دون باركر، الذي عرّفها

---

[2] أ.د.هشام محمد فريد رستم، الجرائم المعلوماتية أصول التحقيق الجنائي الفني، الطبعة الثالثة، المجلد الأول، كلية الشريعة والقانون، جامعة الأمارات العربية المتحدة، 2004، ص 406.

[3] أ.م. نبيلة هبة هروال، الجوانب الاجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، دراسة مقارنة، دار الفكر الجامعي، الاسكندرية، 2013، ص30.

على أنها "عمل إجرامي، مهما كانت علاقته بتكنولوجيا المعلومات، يكبد فيه الضحية خسارة نتيجة لذلك، ويحقق الجاني ربحًا متعمدًا ".

وهنا يجب أن نتحدث أيضًا عن تعريف الهجمات الإلكترونية بشكل اصطلاحي في دراستنا، حيث استخدم مصطلح الهجمات الإلكترونية، على عكس ما كان يفعله بعض المتخصصين، اعتمد بعضها مصطلح الفضاء الإلكتروني، بناءً على البيئة التي تحدث فيها العمليات السيبرانية الناشئة عن أداء الأنظمة الإلكترونية، وتتمثل مهمتها في متابعة وجمع المعلومات التي تعمل إلكترونيًا وتحليلها، ثم اتخاذ إجراءات محددة لمهاجمتها من خلال أنظمة إلكترونية أخرى مخصصة لهذا الغرض.

كما تبنى آخرون مصطلح الحرب الإلكترونية على أساس أيديولوجية أمنية أو عسكرية، والتي تحدد طريقة لتحقيق أهداف على المستوى الأمني أو العسكري ضد العدو المفترض.

اختار آخرون مصطلح الهجمات الإلكترونية، كوصف واقعي يجمع كل ما سبق ذكره، لأنه فعل يحدث في عالم افتراضي قائم على استخدام البيانات الرقمية ووسائل الاتصال الإلكترونية، ثم تم تطويره ليشمل مفهومًا أوسع، استنادًا إلى تحقيق أهداف عسكرية أو أمنية ملموسة ومباشرة، نتيجة لاختراق مواقع الويب الحساسة، والتي عادةً ما تؤدي وظائف مصنفة كأولوية، مثل أنظمة الحماية لمحطات الطاقة النووية أو الكهربائية والمطارات ووسائل النقل الأخرى.

ولأن مصطلح الحرب مصطلح لا يحظى بشعبية في الوقت الحاضر على مستوى التنظيم القانوني الدولي فإن مصطلح الهجمات الإلكترونية عبر الإنترنت هو أقرب إلى الموضوع الذي تناولته هذه الدراسة خاصة وأن العديد من الإجراءات الدولية أشارت إلى مصطلح الهجمات، واعتبرت هو السلوك الذي يؤخذ في الاعتبار أثناء النزاعات المسلحة، وفقًا للقانون الدولي الإنساني [4].

وفي نفس الموضوع، فإن اهتمام المتخصصين في القانون الدولي الإنساني يتركز عادة على وصف الوسائل والأثر بمعنى آخر، التركيز على وسائل الهجوم، وطريقة تنفيذها، والآثار التي ستنجم عنها، بدلاً من التركيز على ما هو وارد في وسائل وأساليب محاربة أنفسهم، وهذا النهج مدعوم من قبل توماس ريد وبيتر ماكبيرني، المتخصصين في القانون الدولي الإنساني، اللذين فضلا مصطلح الهجوم الإلكتروني، بدلاً من الحرب الإلكترونية، على أساس أن الأخيرة هي أوسع نطاقا من السابق.

في ملاحظة دقيقة لاختيار المصطلح المناسب، يتابع ميشيل جيرفيس ليقول: "مصطلح الحرب الإلكترونية ليس مصطلحًا مناسبًا، لأنه مصطلح عام لا يميز بين آثار استخدام الإنترنت كوسيلة أو طريقة للقتال " تعرض مصطلح الهجوم السيبراني لعدة تعريفات من زوايا مختلفة على الرغم من أنها تشترك في محتوى مشابه في المعنى، وهو استهداف المواقع عبر وسائل الاتصال الإلكترونية الأخرى [5].

ومن بين هذه التعريفات آراء الخبراء والمتخصصين في القانون الدولي الإنساني، أولهم شاين الذي يقول: استخدام الطيف الإلكتروني أو الكهرومغناطيسي لتخزين وتعديل وتبادل البيانات وجهاً لوجه مع أنظمة التحكم في البنية التحتية المرتبطة، في حين عرّفها "وورتز" بالقول:" الهجوم عبر الإنترنت يقوم

---

[4] انظر: الفقرة 2 من المادة 54 من البروتوكول الإضافي الأول لعام 1977، والتي نصت انه: "يحظر مهاجمة أو تدمير أو نقل أو تعطيل الأعيان والمواد التي لا غنى عنها لبقاء السكان المدنيين".

[5] أ.م.جيل برهام، تأثير تطور تكنولوجيا الحرب السيبرانية على بناء القوة في اسرائيل، ترجمة للعربية يولا البطل، مؤسسة الدراسات الفلسطينية، فلسطين، 2013، ص 1.

على التسلل إلى مواقع رسوم متحركة غير مصرح بها، بهدف تعطيل أو تدمير أو حيازة البيانات المتوفرة فيها، وهي سلسلة من الهجمات الكارتونية التي نفذتها دولة ضد أخرى.

عرّفها شميدث بأنها: "مجموعة من الإجراءات التي اتخذتها الدولة لمهاجمة أنظمة المعلومات المعادية بهدف التأثير عليها وإلحاق الأذى بها، وفي الوقت نفسه الدفاع عن أنظمة المعلومات في الدولة المهاجمة"، عرفها زيمت وباري بأنها: "مجموعة عمليات تعتمد على الحرب الإلكترونية والخداع النفسي وكذلك استهداف شبكة الاتصالات العسكرية للعدو وعملياته الأمنية الإلكترونية."

وأخيراً يذهب ماركو روسيني إلى تعريفها بالقول: "تطويع الإمكانيات الالكترونية العسكرية لأجل التأثير في مواقع الكترونية أخرى وتعطيلها أو تدميرها سواء أكانت تقدم خدمات مدنية أو عسكرية، وفي رأينا أن التعريف الذي ذهب إليه ميشيل هو الأقرب لمفهوم الهجمات السيبرانية التي عرفها روسيني، إذ يعرفها بالقول: "الهجوم السيبراني، هو أي تصرف دفاعياً كان أم هجومياً، يتوقع منه وعلى نحو معقول في التسبب بجرح أو قتل شخص أو إلحاق أضرار مادية أو دمار بالهدف المهاجم."[6].

المطلب الثاني: موقع الجريمة السيبرانية في التنظيم التشريعي العراقي

لا يزال موقف المشرّع العراقي من الجريمة السيبرانية يعاني من قصور واضح، نتيجة الاعتماد المستمر على القوانين التقليدية وعدم وجود تشريع خاص ومتكامل ينظم الجرائم المعلوماتية حتى الآن.

وعلى الرغم من تقديم عدة مشاريع قوانين في هذا المجال، إلا أنها لم تُعتمد، بسبب ما أُثير حولها من جدل يتعلق بتقييد حرية التعبير. ونتيجة لهذا الفراغ التشريعي، تلجأ السلطات العراقية إلى معالجة بعض الجرائم السيبرانية من خلال نصوص قانون العقوبات العام، مثل القذف والابتزاز.

في المقابل، يشارك العراق في الجهود الدولية الرامية إلى إعداد اتفاقية دولية لمكافحة الجريمة السيبرانية، مع التأكيد على أهمية احترام السيادة الوطنية ومراعاة خصوصية القوانين الداخلية.

تضمن قانون العقوبات العراقي العديد من العقوبات التي لا تزال سارية المفعول حتى اليوم، وتشمل هذه العقوبات النشر والتهديد والأخلاق العامة وغيرها من المواد والنصوص القانونية، جميعها، التي تضمن اتباع ذلك وعدم تجاهله، ومع ذلك، فإن هذا القانون لم يعد يواكب التطورات المتسارعة والتعقيدات المتزايدة التي تشهدها المحاكم يوميًا، في ظل غياب تدخل تشريعي فعّال يضع الضوابط الكفيلة بمنع الأفراد من الإضرار بالغير أو المساس بالمصلحة العامة والخاصة، الأمر الذي يستدعي مراجعة قانونية شاملة تواكب متطلبات الواقع العملي.

يهدف الأمن السيبراني إلى حماية قنوات الاتصال الرقمية بكل ما تحمله من تعقيدات، إضافة إلى تأمين الشبكات المحلية والعالمية ضد محاولات الاختراق التي قد تؤدي إلى تدمير البنية التحتية لأنظمة المعلومات، بما يشمل الأجهزة والمعدات والبرمجيات، لا سيما تلك المرتبطة بالقطاعات الحيوية مثل المال، والطاقة، والإحصاء. وتُرتكب هذه الهجمات الإلكترونية غالبًا عبر أساليب معقدة مثل اختراق الأنظمة المالية وتحويل الأموال بصورة غير مشروعة.

وبصورة أشمل، فإن هذه الأنظمة تهدف إلى مواجهة جميع أشكال الجرائم المعلوماتية التي تتم أحيانًا بوسائل عنيفة وذات آثار مدمّرة. وتزداد خطورة هذه التهديدات في ظل وجود جيوش إلكترونية

[6] انظر المادة الخامسة من اتفاقية مجلس أوروبا المتعلقة بالجريمة الالكترونية لعام 2001.

مدعومة بمعدات متقدمة وأدوات رقمية متخصصة في اختراق الأنظمة السيبرانية، سواء في الدول المتقدمة أو تلك التي تعاني من هشاشة في بنيتها التحتية، مثل العراق.

ويمتلك العراق موقعًا استراتيجيًا واقتصاديًا يجعله عرضة لهذه الهجمات؛ إذ يملك نحو 11% من احتياطي النفط العالمي، فضلًا عن كميات كبيرة من الكبريت والغاز الطبيعي. ونتيجة لذلك، أصبح العراق ساحة صراع غير مباشر بين القوى العالمية التي تسعى إلى إبقائه سوقًا استهلاكيًا مفتوحًا لمنتجاتها، في ظل غياب صناعة وطنية متطورة، الأمر الذي يتطلب تعزيز البنية التشريعية والتقنية لحماية الأمن الوطني في الفضاء الرقمي.[7]

تُعد حرية الرأي والتعبير من الحقوق الأساسية التي يتمتع بها كل فرد، وهي تجسّد صوت المجتمع وتطلعاته، كما تُعد أحد المؤشرات الجوهرية التي يُقاس بها مدى تقدم الدول وتحضرها. وقد كفل الدستور هذا الحق في المادة (38)، التي نصّت على ما يلي:

أولاً: حرية التعبير عن الرأي بجميع الوسائل،

ثانيًا: حرية الصحافة والطباعة والإعلام والإعلان،

ثالثًا: حرية الاجتماع والتظاهر، شريطة أن تُمارس وفقًا للقانون.

ومع التقدّم التكنولوجي الهائل، ولا سيما في مجال الاتصالات، أصبحت شبكة الإنترنت أداة فعالة لنقل وتبادل الآراء والأفكار بسرعة غير مسبوقة. وقد أسهمت هذه التقنية الحديثة في توسيع نطاق حرية التعبير، حيث باتت المنصات الرقمية فضاءً مفتوحًا للتفاعل الاجتماعي والثقافي والسياسي.

غير أن هذه الحرية، ورغم أهميتها، لم تكن بمنأى عن التجاوزات، إذ سُجلت حالات استغلال لهذه الوسائل في انتهاك خصوصية الأفراد والتعدي على حقوقهم. ومن هنا تبرز القاعدة القانونية الأساسية: "تنتهي حرية الفرد عندما تبدأ حقوق الآخرين"، مما يفرض ضرورة وجود قوانين منظمة تمنع الانفلات وتوازن بين حرية التعبير وحماية النظام العام وحقوق الأفراد.

أشارت التقارير إلى أن العراق شهد بعد عام 2003 عددًا متزايدًا من الهجمات السيبرانية الخطيرة، والتي استهدفت بشكل مباشر مواقع حكومية حساسة، مما جعله من بين الدول الأكثر تعرضًا للاختراقات الرقمية في المنطقة. وتُعد هذه التهديدات السيبرانية من أبرز التحديات التي تواجه البنية التحتية الرقمية للبلاد.

ومن أبرز المواقف المثيرة للجدل في هذا السياق، ما صرّح به رئيس الجمهورية الأسبق، السيد إياد علاوي، خلال مقابلة تلفزيونية أُجريت في نيسان/أبريل عام 2018، حيث أعرب عن شكوكه بشأن استخدام الأقمار الصناعية في عملية التصويت خلال الانتخابات العراقية. وأشار إلى أن هذه الأقمار الصناعية مملوكة لدول أجنبية، وبالتالي فإن العراق لا يمتلك السيطرة الكاملة عليها، مما يثير مخاوف جدية بشأن احتمال تعرّض عملية نقل البيانات الانتخابية للاختراق أو التلاعب.

---

[7] د. زاهر الزبيدي، «تهديدات افتراضية للأمن السيبراني العراقي»، 2018، موقع شبكة النبأ المعلوماتية. https://annabaa.org/arabic/informatics/17379

وأضاف أن احتمالية حدوث عمليات قرصنة أو تغيير في نتائج الانتخابات تبقى واردة في ظل غياب آلية رقابية محكمة. وفي هذا الإطار، شدّد على ضرورة وضع إجراءات فنية وتشريعية صارمة تمنع تدخل القوى الخارجية أو الجهات ذات المصالح في سير العملية الانتخابية.

كما نوه إلى أهمية السماح بتقنيات تدقيق البيانات، ومنها تدقيق الصوت، وهو ما قد يفتح الباب لنقاش أوسع حول ما يُعرف بـ"مجموعة كامبريدج"، في إشارة محتملة إلى فضيحة شركة Cambridge Analytica، والتي اتُّهمت سابقًا باستخدام البيانات الرقمية للتأثير في نتائج الانتخابات في عدة دول. ويُعتقد أن مثل هذه الجهات قد تمتلك القدرة على التسلل إلى أنظمة الحواسيب المسؤولة عن نقل البيانات والتصويت الإلكتروني، الأمر الذي قد يُلحق ضررًا بالغًا بالأمن السيبراني للدولة ويؤثر سلبًا على مصداقية العملية السياسية وهيكلية الحكومة، بما يخدم مصالح خارجية على حساب الإرادة الوطنية.[8]

وشهد العراق زيادة ملحوظة في الطلب على الشبكات المخصصة للتواصل الاجتماعي، وذلك على ما يبدو لأنه يحتوي على مشروع حضاري يتم التعبير عنه من خلال الحاجة إلى استكمال الخطوات إلكترونياً، وأولها السياسة الإلكترونية الدولية التي يُراد لها أن تكون يُمارس الأمن السيبراني بشكل سلمي وخالي من العنف.

وقد صرّح النائب علي الغانمي، عضو لجنة الأمن والدفاع النيابية، في حديثه لصحيفة المدى، بأن مجلس النواب سيقوم بقراءة تقرير لجنة الأمن والدفاع بشأن التعديلات المطروحة على مشروع قانون الجرائم الإلكترونية. وأوضح أن التعديلات الجديدة جاءت نتيجة لمجموعة من الاتفاقات والمشاورات، وأسفرت عن تغيير مسمى القانون من "قانون مكافحة الجرائم الإلكترونية" إلى "قانون الجرائم ضد الحاسوب والإنترنت"، إضافة إلى تضمين مشروع القانون إنشاء المركز الوطني للرقمنة، الذي سيكون مسؤولًا عن إصدار تقارير فنية يمكن اعتمادها كأدلة قضائية أمام المحاكم في القضايا المرتبطة بالجرائم المعلوماتية.

وكان مجلس النواب قد أنهى القراءة الأولى لمشروع القانون خلال العام الماضي، والذي تضمّن عقوبات مشددة وصلت في بعض الحالات إلى السجن المؤبد وغرامات مالية كبيرة، مما أثار انتقادات قانونية وحقوقية واسعة. ووفقًا لما صرّح به ممثل الدائرة القانونية في مجلس النواب، فإن التعديلات الحالية جاءت لمعالجة تناقضات مشروع القانون السابق لعام 2011، والذي اعتُبر مخالفًا لأحكام قانون العقوبات رقم (111) لسنة 1969، كما تعارض مع الاتفاقيات الدولية التي تُوصي بضرورة احترام حرية الرأي والتعبير.

وأكد الغانمي أن النسخة المعدّلة من القانون أصبحت أكثر نضجًا وتوازنًا، حيث جاءت متماشية مع النهج الديمقراطي ولا تتعارض مع حقوق المواطنين الأساسية، لا سيما الحق في التعبير عن الرأي. كما أشار إلى أن القانون بصيغته الجديدة يُتوقع أن يُسهم في تحسين مستوى الأمن المعلوماتي، ويكون له أثر إيجابي على الحياة الاجتماعية عبر الحد من الجرائم الإلكترونية وتنظيم التعامل مع الوسائط الرقمية.

أعلنت لجنة الأمن والدفاع في مجلس النواب العراقي عن نيتها إعادة طرح مشروع قانون جرائم المعلوماتية، والذي يمنح السلطات صلاحيات واسعة في مراقبة ومحاسبة المواطنين بناءً على منشوراتهم على منصات التواصل الاجتماعي. كما أكدت اللجنة أنها ستعمل على عرض مشروع القانون للتصويت

[8] د. زاهر الزبيدي، «تهديدات افتراضية للأمن السيبراني العراقي»، مرجع سابق.

خلال المرحلة المقبلة، مشيرةً إلى أهمية إقراره في ظل تزايد التهديدات الإلكترونية، واعتباره أداة للحد من معدلات الجرائم الإلكترونية في البلاد.

ورغم التأكيدات الرسمية على ضرورة هذا القانون لتعزيز الأمن السيبراني وضبط الفضاء الرقمي، فقد أثار المشروع موجة واسعة من القلق والانتقادات، لا سيما في الأوساط المدنية والحقوقية. ويعود الجدل إلى المخاوف المتزايدة من إمكانية استغلال القانون لقمع حرية الرأي والتعبير، تحت غطاء مكافحة الجرائم المعلوماتية.[9]

في الخامس من حزيران/يونيو 2022، أعلنت لجنة الأمن والدفاع في مجلس النواب العراقي عن نيتها إعادة تقديم مشروع قانون جرائم المعلوماتية، وهو مشروع قانون يهدف إلى تنظيم السلوك الرقمي عبر الإنترنت ويمنح السلطات صلاحيات موسعة في مراقبة وتتبع الأفعال الإلكترونية للمواطنين. كما أشارت اللجنة إلى إمكانية طرح القانون للتصويت خلال الدورة التشريعية الحالية، مؤكدة أن إقراره ضروري للحد من ارتفاع معدلات الجرائم المعلوماتية.

وفي الوقت ذاته، حذّرت اللجنة من مخاطر إساءة استخدام القانون، مشددة على ضرورة عدم توظيفه كأداة لـ قمع حرية التعبير، وإنما كوسيلة لتقنين وضبط استخدام الفضاء الإلكتروني بما يضمن الأمن الرقمي للدولة والمجتمع.

وقد شهدت محاولات تمرير هذا القانون زخمًا متزايدًا خلال نهاية عام 2021، ما أثار قلقًا واسعًا لدى منظمات المجتمع المدني والناشطين والمدونين، الذين عبّروا عن تخوفهم من أن يؤدي اعتماد القانون بصيغته المقترحة إلى فرض قيود على الحريات الرقمية والإعلامية.

وفي تطور مهم، أعلن رئيس مجلس النواب العراقي محمد الحلبوسي، خلال جلسة حوارية حضرها ممثلون عن عدد من الدول الغربية، أن القانون لن يُمرر بصيغته الحالية، ما اعتُبر استجابة واضحة للمخاوف الدولية والمحلية بشأن حقوق الإنسان وحرية التعبير في العراق.

هذا وقد أكد النائب ياسر وتوت، عضو لجنة الأمن والدفاع في مجلس النواب العراقي، أن اللجنة عازمة على المضي قدمًا في تشريع قانون جرائم المعلوماتية خلال المرحلة التشريعية المقبلة. وبيّن أن اللجنة ستشرع بعرض فقرات القانون بندًا بندًا لمناقشتها داخليًا، قبل إحالتها إلى اللجان البرلمانية الأخرى المختصة من أجل إبداء الرأي الفني والتشريعي بشأنها. وأوضح أن وجود مثل هذا القانون بات ضروريًا، أسوةً بما هو معمول به في الدول المتقدمة، التي اعتمدت قوانين رصينة تهدف إلى الحد من الجرائم الإلكترونية، مع ضمان حماية الحقوق والحريات لكل من الدولة والمواطنين على حد سواء.

وفي سياق متصل، يُلاحظ أن المشرّع العراقي لا يزال يفتقر إلى التمييز الدقيق بين مفهومي قانون جرائم المعلوماتية وقانون أمن المعلومات، وهو ما يؤدي إلى تداخل تشريعي قد ينعكس سلبًا على فاعلية النصوص القانونية وتطبيقاتها.

فالبيانات، وفق المفاهيم التقنية، تُعد مدخلات أولية، تخضع للمعالجة الحاسوبية لتتحول إلى مخرجات تُصنّف كمعلومات، سواء كانت نصوصًا قابلة للقراءة أو صورًا يمكن رؤيتها. وعليه، فإن معالجة

---

[9] صفاء الكبيسي، «محاولات جديدة لتشريع قانون جرائم المعلوماتية تثير جدلاً في العراق»، 2022، موقع صحيفة العربي الجديد. https://www.alaraby.co.uk/entertainment_media

البيانات للوصول إلى معلومات ذات قيمة عملية أو قانونية، يندرج ضمن قانون أمن المعلومات الذي يعنى بحماية هذه البيانات والأنظمة التي تعالجها. في حين أن قانون جرائم المعلوماتية يجب أن يركّز على الأفعال الجرمية التي تُرتكب باستخدام تلك المعلومات أو من خلال الوسائل الإلكترونية.

ومن هنا، تبرز الحاجة الملحة إلى إعادة تعريف المفاهيم التقنية داخل الأطر القانونية العراقية، بما يتماشى مع المعايير الدولية، لضمان صياغة تشريعية دقيقة تحمي الحقوق الرقمية، وتمنع إساءة استخدام النصوص القانونية تحت ذرائع الأمن أو النظام العام.

وقد خرق المشرع العراقي قانون العقوبات العراقي رقم (111) في عام 1969، بارتكاب جرائم ضد الاتصالات السلكية واللاسلكية، وتعريض سلامة الجمهور للخطر، وبالتالي حُكم عليه بالسجن لمدة لا تزيد عن سبع سنوات أو بالسجن لكل من عطل وسيلة اتصال متخصصة بسبب لصالح الجمهور.

وتضمن الدستور العراقي فقرات تشير الى اعتبار بعض السلوكيات من هذا القبيل جريمة سياسية، حيث اكد على ذلك في بعض مواده[10] .

على الرغم من تنامي خطر الإرهاب الإلكتروني عالميًا، إلا أن المشرّع العراقي لم يتطرق صراحةً في نصوصه القانونية إلى هذا النوع من التهديدات، ولم يُدرجه ضمن الأشكال المعترف بها للإرهاب، بالرغم من آثاره الجسيمة على الأمن الوطني والسلم المجتمعي. فالإرهاب الإلكتروني، الذي يعتمد على استخدام التكنولوجيا والمجال الرقمي في تنفيذ هجمات تستهدف البنى التحتية الحيوية أو نشر الذعر والفوضى، بات يشكل تحديًا خطيرًا للدول، ويتطلب معالجة قانونية دقيقة.

وبالرجوع إلى قانون جهاز مكافحة الإرهاب، يتضح أن المهام الموكلة إلى هذا الجهاز تتمحور في مجملها حول مجابهة واستئصال الإرهاب بجميع أشكاله، وتطوير استراتيجيات شاملة لمكافحته.

ورغم هذا الإطار العام، فإن القانون لم يُدرج الإرهاب الإلكتروني ضمن الأشكال التي يُفترض مواجهتها، كما لم يفرد تعريفًا مستقلًا أو تنظيمًا خاصًا لهذا النوع من الجرائم. وهذا يُظهر فجوة تشريعية واضحة في التعامل مع التهديدات الإلكترونية الحديثة، ويُبرز الحاجة إلى توسيع مفهوم الإرهاب قانونيًا ليشمل الجرائم السيبرانية المنظمة، التي تستهدف البنى التحتية الرقمية، والمعلومات الحكومية، والمصالح الاقتصادية الحيوية.

إن المشرع العراقي لم يُدرج الإرهاب الإلكتروني بشكل صريح في قوانينه، رغم خطورته المتزايدة على الأمن الوطني والمجتمع. قانون جهاز مكافحة الإرهاب يركز على مواجهة الإرهاب التقليدي، لكنه يفتقر لتعريف وتنظيم واضح للإرهاب الإلكتروني. هذا يُشكّل ثغرة قانونية تحد من قدرة الأجهزة الأمنية على التصدي للتهديدات الرقمية الحديثة. لذا، هناك حاجة ملحة لتحديث التشريعات لتشمل الإرهاب الإلكتروني، مع توسيع صلاحيات الأجهزة المختصة وتعزيز التنسيق بين الجهات الأمنية للحفاظ على الأمن السيبراني الوطني.

[10] المادة (٧) من الدستور العراقي الدائم لسنة ٢٠٠٥

المبحث الثاني
جهود مواجهة الجرائم السيبرانية في أوروبا والعالم العربي

تعتبر الجرائم السيبرانية من التحديات الكبرى التي تواجه المجتمعات الحديثة، مما يستدعي تكاتف الجهود الدولية والإقليمية لمواجهتها. في هذا السياق، تلعب المنظمات الأوروبية دورًا محوريًا من خلال اتفاقيات مثل اتفاقية بودابست لعام 2001، التي وضعت إطارًا قانونيًا لمكافحة الجرائم السيبرانية.

من جهة أخرى، تسعى الدول العربية أيضًا لتعزيز التعاون في هذا المجال، عبر الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010، التي تهدف إلى حماية المجتمعات العربية من مخاطر الفضاء السيبراني. يتناول هذا المبحث الجهود الأوروبية والعربية في مواجهة الجرائم السيبرانية، مع التركيز على الأطر التشريعية والمبادرات المشتركة التي تهدف إلى تعزيز الأمن السيبراني.

ومن اجل بيان هذا المبحث بشكل اوفى، سوف نقسمه على مطلبين، الأول بعنوان: الجهود الأوروبية في مواجهة الجرائم السيبرانية ، اما الثاني بعنوان: الجهود العربية في مواجهة الجرائم السيبرانية **، والتفاصيل على النحو الآتي:**

المطلب الأول: الجهود الأوروبية في مواجهة الجرائم السيبرانية

تلعب المنظمات الدولية دوراً مهماً على المستوى العالمي، فضلاً عن عدد من المنظمات الإقليمية التي تركز عملها على مناطق محددة، باستثناء أن عدداً منها لديها أنشطة تتعامل مع القضايا المتعلقة بالجريمة السيبرانية، ويعد المجلس الأوربي، من أقدم المنظمات السياسية الأوربية، وفي عملها يغطي جميع المجالات السياسية عدا الدفاع، أما الاتحاد، فلديه قدرة محدودة على التشريع في مجال القانون الجنائي، والذي بعد رمزاً لسيادة الدولة، ولأن الاتحاد منظمة تجارية، وبالنظر إلى أن الجريمة السيبرانية تقف كعقبة أمام التجارة بين الدول الأعضاء، يتخذ الاتحاد الأطر القانونية لمواجهتها، ووعليه سنبحث الجهود الأوربية في مواجهة الجرائم السيبرانية في امرين أثنين على النحو التالي:

أولاً: اتفاقية المجلس الأوروبي بودابست 2001:

اتفاقية بودابست لعام 2001 أهم صك دولي في مكافحة الجرائم السيبرانية، على مستوى العالم، وفي أوربا على وجه الخصوص، والسبب في إبرام الاتفاقية، يتمثل في الحاجة إلى اتخاذ تدابير قانونية تشريعية لمكافحة الجرائم السيبرانية في ظل الاعتماد على تكنولوجيا المعلومات والنمو الحاصل في أنظمة الحاسوب وتدفق المعلومات، فضلاً عن أهمية مكافحة الأنشطة التي تستهدف العناصر الثلاثة لأمن المعلومات ونظم الحاسوب وهي سرية وسلامة المحتوى وتوفر المعلومات والنظم، وسنتحدث عن واقع الاتفاقية على النحو الاتي:

1_ نبذة تاريخية عن أنشطة مجلس أوربا:

إن من المهم اخذ لمحة عامة عن أنشطة المجلس في أوربا، في مواجهة الجرائم السيبرانية، ففي عام 1976، عقد مجلس أوربا مؤتمراً تناول فيه الطبيعة الدولية لجرائم الحاسوب، وقد ناقشها بشكل مستمر في جدول الإعمال، وفي عام 1996 قررت اللجنة الأوربية لمشكلات الجريمة إنشاء لجنة لمعالجة الجرائم

السيبرانية، وخلال ثلاثة أعوام عقدت هذه اللجان عشرات الاجتماعات، تكللت باعتماد الجمعية مشروع اتفاقية بودابست في نيسان عام 2001، والذي فتح باب التوقيع عليها في تشرين الثاني من نفس العام[11].

2_ أحكام اتفاقية بودابست:

تعد معاهدة بودابست هي أبرز مثال على التعاون في الفضاء السيبراني لمواجهة التهديدات والجرائم السيبرانية، إنها الاتفاقية الدولية الملزمة المتعددة الأطراف في مجال مكافحة الجريمة السيبرانية، تم فتحه للتوقيع عليها في عام 2001 ودخلت حيز التنفيذ عام 2004، إذ بدأت حتى الآن 50 دولة، من داخل وخارج الاتحاد الأوربي بالاتفاق عليها، وصدقت من قبل 40 دولة، من بينها الولايات المتحدة الأمريكية وكندا واليابان، وقد أسهمت هذه الاتفاقية في وضع أطر تشريعية لمكافحة الجرائم السيبرانية، وفي نفس الوقت أظهرت مدى إدراك الدول لتهديدات الجريمة على الأمن السيبراني، وضرورة التصدي لأبرز التهديدات وإشكالها[12].

حيث أن أهداف الاتفاقية، واضحة من ديباجاتها، حيث ركزت على حماية المجتمع من الجرائم السيبرانية، وضرورة وقاية المصالح العامة المشروعة عند استعمال وتبلور تكنولوجيا المعلومات، كذلك ضمان التوازن بين مصالح إنفاذ القانون واحترام حقوق الأساسيات، ومنها الحق في الخصوصية والحق في حرية التعبير، من خلال اعتماد التشريعات المناسبة لمنع الأعمال الموجهة ضد سرية وسلامة وتوفر نظم الحاسوب، والشبكات والبيانات ودعم وتعزيز التعاون الدولي في المسائل الجنائية.

3_ البروتوكول الإضافي الأول بشأن تجريم الأفعال المرتبطة بالتمييز العنصري وكراهية الأجانب التي ترتكب عن طريق نظام الحاسوب:

وتبين خلال المفاوضات إن تجريم العنصرية وتوزيع المواد المعادية للأجانب، من القضايا المثيرة للجدل، فيما يتعلق بحرية التعبير، حيث تتمتع في بعض الدول يحظى بحماية قوية، الأمر الذي أثار مخاوف من عدم انضمام بعض الدول، لذلك بعد الاتفاقية، تم وضع البروتوكول الإضافي الأول في عام 2003، واتفاقية بشأن حماية الأطفال من الاستغلال الجنسي في عام 2007.

نستنتج من خلاصة ما تقدم، أنه رغم أهمية الاتفاقية على المستوى الإقليمي والدولي، باعتبارها عملاً دولياً يقوم على إيجاد لغة فهم مشتركه للجرائم السيبرانية، عبر إنشاء شكل كحد أدنى مشابه لهذه الجرائم، إلا ان المعاهدة غير ملزمة لكل دول الاتحاد الأوربي بشأن الموافقة على المعاهدة وتنفيذها، ويرى المجلس الأوربي ذاته أن المعاهدة صارت قديمة، اذ لم يكن هناك استعمال الارهابين للأنترنت، والهجمات الروبوتية، والتصيد الاحتيالي عند إنشاء المعاهدة، إلا أن المعاهدة تعتبر الكيان الأساسي لأي عمل دولي تلاها، ومثال تشريعي يؤخذ به عند إنشاء أي تشريع وطني غايته مكافحة الجرائم السيبرانية، للمضمون الذي يعكس عملاً دولياً و حوارات خبراء مختصين في مواضيع الأمن والجريمة في الفضاء السيبراني.

ثانياً: قرارات الاتحاد الأوربي ذات الصلة بمكافحة الجرائم السيبرانية:

إن الاحكام المتضمنة عمل تشريعي ينبثق من الاتحاد الأوربي في نطاق التشارك الجنائي والقضائي في القضايا الجنائية، وهي ايضاً تجبر الأعضاء بتحقيق الخلاصة، دون أن تعطيهم وسائل

---

[11] أ.د. عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والانترنت، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2007، ص 24.

[12] أ.د. حسين محمد الغول، جرائم شبكة الأنترنت والمسؤولية الجزائية الناشئة عنها، الطبعة الأولى، مكتبة بدران الحقوقية للنشر والتوزيع، بيروت، لبنان، 2017، ص 49.

إنجازها وطنياً، وليس لها أثر مباشر على الدول الأعضاء، أما بالنسبة للقرارات التي صدرت في نطاق أوربا فيما يهم الجريمة السيبرانية فهي التالية:

1_ القرار الإطاري للمجلس بشأن مكافحة استغلال الأطفال على الأنترنت في المواد الإباحية 2004:

في عام 2004، تبنى المجلس القرار (2004/68)، للتصدي لاستغلال الأطفال على شبكة الانترنت وقد تضمن أحكاماً تمنع تبادل الصور الخاصة عبر الأنترنت، وقد سبق للمجلس الأوربي في عام 2000، أن تبنى القرار (2000/375)، للتصدي لاستغلال الأطفال على شبكة الأنترنت، وفي وقت سابق في عام 1996 صدر بيان بخصوص المضمون الغير قانوني والضار على شبكة الحاسوب، علماً انه تم تغير القرار بتوجيه (2011/92)، بخصوص استغلال الأطفال في المواد الإباحية 2011.

2_ القرار الخاص بمكافحة الاحتيال:

في عام 2001، تبنى المجلس الأوربي قراراً يواجه الجريمة السيبرانية بصورة مباشرة، عبر القرار الإطاري (2001/413)، بشأن مكافحة الاحتيال وتزوير وسائل الدفع غير النقدية، فقد فرض المجلس مهام بشأن تنسيق القانون الجنائي فيما يهم أطراف معينة من الاحتيال المتصل بالحاسوب والبرامج الخاصة بالحاسوب، التي تستخدم لارتكاب الجرائم المشار عليها في القرار الإطاري.

3_ القرار بشأن الهجمات ضد أنظمة المعلومات 2005:

تبنى المجلس في عام 2005، قراراً بخصوص الهجمات ضد أنظمة المعلومات، وهو ليس إعادة لما أتى في معاهدة بودابست لعام 2011، بل جاء ليكون مشتركاً مع المعاهدة، ويركز القرار على تنسيق الأحكام الجوهرية للقانون الجنائي وكذلك المرتبطة بالتعاون الدولي[13].

4_ القرار الخاص بمكافحة الإرهاب:

غير المجلس الأوربي في عام 2008، القرار الإطاري بالإرهاب الذي وحد تعريف الجرائم الإرهابية في كافة دول الاتحاد الأوربي، وبنى أسساً لملاحقة قضائية فعالة لهذه الجرائم، وقد أتى هذا القرار فارغاً من تجريم استعمال الإرهابين للأنترنت في نشر الدعاية وخبراتهم في صنع القنابل، لذلك صدر القرار الإطاري (2008/919)، لاتخاذ إجراءات لإغلاق هذه المشاكل وتقرب التشريعات الأوربية لإيقاف الإرهاب وجعل الأنظمة متناسبة مع معاهدة بودابست لعام 2001، ويضم على وجه الخصوص الأحكام على الاستفزاز العام لارتكاب جريمة إرهابية.

5_ القرارات التوجيهية للاتحاد الأوربي ذات الصلة بالجرائم السيبرانية:

عرفت التوصيات بأنها فئة من التدابير غير المرغمة الصادرة من منظمة دولية والموجهة إلى الدول الأعضاء بصدد قضية معينة، وبمعنى آخر إنها خطوط عامة توجه الدول الأطراف بشأن تنفيذ مهامها، ولكن في مجال الاتحاد الأوربي تضع التوجيهات تأثيراً مباشراً على الدول الأطراف، فهي ترغم الأعضاء بإنجاز المهام، وتترك لهم الطرق والوسائل طبقاً للأنظمة الداخلية للدول الأطراف.

أما بخصوص التوجيهات الصادرة من الاتحاد الأوربي، بخصوص السيبرانية وهي كالتالي:

أ_ التوجيه بشأن التجارة الإلكترونية عام 2000:

إن التوجيه (2000/31)، يعالج مسؤولية مورد خدمة الانترنت عن أعمال تقترفها أطراف ثالثة، ليتم إنشاء معايير قانونية لتأمين إطار، لأجل التنمية العامة لمجتمع المعلومات ودعم التنمية الاقتصادية بوجه عام، وكذلك أجهزة إنفاذ القانون[14].

---

(13) أ.د. أمير فرج يوسف، مكافحة جريمة الإرهاب الإلكتروني، الإرهاب الرقمي في ظل اتفاقية مجلس التعاون لمكافحة الإرهاب، مرجع سابق،، ص 87.

ب_ التوجيه بشأن الخصوصية:

هذا التوجيه تم تغيره لملاحقة التطورات في قضايا الخصوصية، الذي كانت الغاية منه وقاية خصوصية الاتصالات الإلكترونية، كما تضمن أمن الخدمات وسرية معلومات العميل، وقد تم مراجعته في عام 2017، وتم طرح فكرة استبداله بقانون أفضل احتراماً للحياة الخاصة، وحماية البيانات الشخصية في البيانات الإلكترونية.

6_ التوجيه بشأن الاحتفاظ بالبيانات عام 2006:

هذا التوجيه (2006/24)، يشمل واجباً على موردي خدمات الانترنت، بحفظ بعض البيانات المتنقلة على شبكة الأنترنت، بغاية البحث عن مواقع الجناة في الفضاء السيبراني، وقد أثار هذا التوجيه مشكلة بخصوص وقاية الحق في الخصوصية، وقدم طعن بصدده إلى محكمة العدل الأوربية، والتي الغته منذ دخوله حيز التنفيذ.

7_ التوجيه بشأن الهجمات ضد نظم المعلومات:

يهدف هذا التوجيه (2013/40)، لحل الهجمات السيبرانية واسعة المجال عبر مطالبة الدول الأطراف بتعزيز القوانين الوطنية المتعلقة بجرائم الأنترنت، وتطبيق عقوبات جنائية أكثر صرامة.

8_ التوجيه بشأن حماية البيانات الشخصية في 2016:

ويهدف هذا التوجيه (2016/679)، إلى وقاية الأشخاص الطبيعيين، بما يتعلق بحل البيانات الشخصية، إذ بموجبه تم إلغاء التوجيه (46/95)، بالإضافة إلى تعزيز حرية نقل هذه البيانات ويهدف هذا التوجيه بالمساهمة في تحقيق نطاق من الحرية والأمن[15].

مما تقدم يتبين تعدد الأدوات التشريعية في القارة الاوربية، فالاتفاقيات التي تصدر من مجلس الاتحاد في القضايا الجنائية والقرارات الإطارية والتوجيهات، التي تأتي من الاتحاد الأوربي، تعمل بأكملها على رسم سياسة جنائية وأطر قانونية في مواجهة الجرائم السيبرانية المنطوية، في مجلس أوربا والاتحاد الأوربي على حد سواء، الأمر الذي يدل على نضج المستوى التشريعي وتطوره ويوفر الأطر القانونية لمواجهة الجريمة السيبرانية إقليميا على مستوى القارة الأوربية، فضلاً عن أي استخدام غير مشروع للفضاء السيبراني، وقد استحدث القرار الإطاري جرائماً جديدة فيما يتعلق بالسلوكيات التي قد تؤدي إلى إعمال إرهابية، ووفر سنداً قانونياً لملاحقة نشر الدعاية الإرهابية، وتطوير المهارات الفنية للإرهابيين لصنع القنابل على شبكة الانترنت.

المطلب الثاني: الجهود العربية في مواجهة الجرائم السيبرانية

إن تبلور الجريمة بشكل عام والجريمة السيبرانية بشكل خاص، آخذ في الازدياد على مستوى العالم، ومن الواضح أن مواجهة هذه الظاهرة بكفاءة وفعالية من أصعب الأمور في البلدان النامية، والبلدان التي في طور الانتقال، والتي غالباً ما كانت عرضة للتغيرات السياسية والاجتماعية والاقتصادية سريعة مثل الدول العربية، وسنركز على الجهود الإقليمية في المجال التشريعي لمواجهة الجرائم السيبرانية في الوطن العربي على أهم الأطر التشريعية على النحو التالي:

---

(14) أ.د.عادل عبد صادق، أسلحة الفضاء الإلكتروني في ضوء القون الدولي الإنساني، مكتبة الإسكندرية، الإسكندرية، 2016، ص 103.

(15) أ.د. رامي متولي القاضي، مكافحة الجرائم المعلوماتية في التشريعات المقارنة وفي ضوء الاتفاقيات والمواثيق الدولية، الطبعة الأولى، دار النهضة العربية، القاهرة، 2011، ص 143.

أولاً: الاتفاقية العربية لمكافحة جرائم تقنية المعلومات 2010:

إن الاتفاقية العربية للحد من جرائم تقنية المعلومات 2010، وجدت لهدف تطوير التعاون بين الدول العربية، بغاية مكافحة الجرائم السيبرانية، وسوف نتكلم عن هذه الاتفاقية العربية على الشكل التالي:

1_ نبذة تاريخية عن أنشطة الجامعة العربية:

إن التعاون الأمني في نطاق جامعة الدول العربية يعود إلى وقت مبكر منذ توقيع ميثاق جامعة الدول العربية في 1945، وفي مجال مكافحة الجريمة بشكل عام في 1950، بإنشاء مكتب مكافحة المخدرات في جامعة الدول العربية، وقد تم دعم هذا التعاون بإنشاء المنظمة العربية للدفاع الاجتماعي عام 1960 التي كان الغرض من إنشائها مكافحة الجريمة وتأمين التعاون المتبادل بين أجهزة إنفاذ القانون.

أما في مجال مكافحة الجرائم السيبرانية، فقد أصدر مجلس وزراء الداخلية العرب، مجموعة من التوصيات عن هذه الجرائم في المؤتمر المنعقد في تونس 1998، وقد دعا فيها الدول الأعضاء إلى تشكيل لجنة وطنية تتولى دراسة جوانب استخدام الحاسوب والانترنت لغرض وضع التدابير لسلامة استخدامها، ووضع النصوص الكفيلة بتجريم إساءة استخدام الحاسوب والانترنت، وفرض عقوبات بحق مرتكبيها.

2_ أحكام الاتفاقية العربية لمكافحة جرائم تقنية المعلومات:

أعلنت الجامعة العربية في نهاية 2010، عن اتفاقية عربية لمكافحة جرائم تقنية المعلومات في اجتماع وزراء الداخلية في القاهرة، وتزامن مع ذلك توقيع أربع اتفاقيات أخرى، تتكون الاتفاقية من خمسة فصول تضمنت (43)، مادة.

3_ الأهداف العامة من الاتفاقية:

تشير الديباجة إلى إن الهدف من الاتفاقية في المادة الأولى، هو رغبة الدول في تعزيز التعاون لمواجهة جرائم تقنية المعلومات، لحماية المجتمع العربي وأمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها، من خلال تبني سياسة جنائية موحدة تجاه هذا النوع من الجرائم، فضلاً عن الالتزام بحماية واحترام وضمان حقوق الإنسان الأساسية، استرشاداً بالمبادئ الدينية والأخلاقية السامية، وبالأخص الشريعة الإسلامية التي تنبذ كل أشكال الجريمة[16].

4_ أحكام مشروع بناء الثقة في الفضاء السيبراني:

في هذه المبادرة تهدف إلى ضمان أمن وسلامة الفضاء السيبراني في المنطقة العربية، وقد رعاها مركز البحوث والدراسات القانونية والقضائية الجامعة العربية، وانصب في مشروع (بناء الثقة في الفضاء السيبراني)، وهو جهد جدير بالاهتمام لكونه يؤسس لحماية الفضاء السيبراني عبر قواعد قانونية، في غياب أطر قانونية واضحة وشاملة في المنطقة العربية.

نستنتج من خلاصة ما تقدم حيث ان الاتفاقية العربية لمكافحة جرائم تقنية المعلومات راعت خصوصية المنطقة العربية، وذلك كان واضحاً من خلال الديباجة من خلال الإشارة إلى مراعاة النظام العام في كل دولة، والأخذ بالمبادئ الدينية والأخلاقية لاسيما الشريعة الإسلامية، اما الانتقادات الموجهة إلى الاتفاقية، استخدامها لألفاظ فضفاضة وواسعة كمصطلح (تقنية المعلومات)، على سبيل المثال، كذلك لم تنص الاتفاقية على معايير محددة للحفاظ على خصوصية المستخدم وحماية بياناته، فضلاً عن شمولها طائفة واسعة من الجرائم على عكس اتفاقية بودابست، ولعل السبب في ذلك يرجع إلى وجود أدوات

---

[16] أ.م.سليمان أحمد فضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، دار النهضة العربية، القاهرة، 2013، ص 177.

تشريعية للمنظمات الفاعلة في المنطقة الأوربية غير الاتفاقيات تسمح لها بالتأثير على قوانين الدول الأعضاء، أن اقتصار التجريم على مسائل بعينها تتعلق بالولوج إلى الحاسوب وإساءة استخدام البرامج وغير ذلك التي احتوتها اتفاقية بودابست.

ثانياً: التشريعات العربية الداخلية لمكافحة الجرائم السيبرانية:

شهد الوطن العربي حركة تشريعية بداية القرن الحالي لضبط المعاملات الإلكترونية ومواجهة الجرائم السيبرانية، إذ صدر قانون التجارة والمبادلات الالكترونية التونسي عام 2000، وبعد عامين أصدرت إمارة دبي بشأن التجارة الالكترونية، وعقب ذلك صدر القانون العربي النموذجي لمكافحة جرائم تقنية المعلومات، والذي وضع القواعد الأساسية التي ينبغي على المشرع العربي اللجوء إليها عند سن قانون وطني لمكافحة هذه الجرائم[17].

1_ قانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية المعلومات 2003:

في عام 2003، تم مناقشة مشروعين أحدهما لمكافحة الجرائم السيبرانية والآخر يخص التجارة الالكترونية، وما يهمنا بهذا الخصوص القانون العربي الاسترشادي (النموذجي) لمكافحة جرائم تقنية المعلومات، اذ تم إقراره من قبل مجلس وزراء العدل العرب في دورته التاسعة عشر، ومجلس وزراء الداخلية العرب في الدورة الحادية والعشرين، فضلاً عن تحقيق التقارب الإداري والتنظيمي بين أجهزة الأمن، لتوفير وحدة الأسلوب والممارسة الأمنية المبنية على وحدة القواعد، كذلك تبادل المعلومات عن حالة الجريمة المنظمة عبر الدول، فضلاً عن توسيع نطاق المعرفة بالتنظيمات الإجرامية ومصادر تمويلها، والتنسيق بين القدرات البشرية والخبرات التكنولوجية وتحديد سبل التدريب والتعاون التقني ولقانون الإمارات الاسترشادي أحكام واستنتاجات:

- **أحكام قانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية المعلومات:**

حيث جاء القانون في (27) مادة، لم تتضمن النصوص القانونية عقوبات محددة، وهذا مسلك محمود، باعتبار إن تقدير مدة العقوبة إلى الدول الأعضاء، يتيح لهم الحرية في تقدير العقوبات طبقاً للبنية الثقافية والاجتماعية والسياسية للدولة العضو، وتضمن نصوصاً وأحكام موضوعية تجرم الدخول غير المشروع.

على ذلك نجد، أن الشمول الذي احتوته النصوص القانونية يمكن الدولة من إصدار التشريع الكامل لمواجهة الجرائم السيبرانية، ويمكن الإضافة على النصوص التي لدى الدولة العضو، إذ لا يوجد ما يمنع ان تقوم الدولة العضو بتحديث النصوص التشريعية كل على حده لتتماشي مع القانون النموذجي، ويعتبر صدور هذا القانون في عام 2003، قد مهد للانضمام إلى الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010، ومقارنة باتفاقية بودابست 2001، يحتوي القانون النموذجي العربي على عدد واسع من الجرائم التي تضمنت بالمقابل عدد محدود وقليل نسبياً، من الجرائم ذات الصلة بالحاسوب بشكل خاص والجرائم السيبرانية بشكل عام.

ب- وثيقة الرياض للنظام الموحد لمكافحة جرائم تقنية المعلومات في دول مجلس التعاون لدول الخليج العربي 2013:

أقر المجلس الأعلى لمجلس التعاون لدول الخليج العربي المنعقد في البحرين عام 2012، النظام الموحد لمكافحة جرائم تقنية المعلومات لدول مجلس التعاون الخليجي، وهذا القانون يأتي في إطار سلسلة من القوانين والأنظمة الاسترشادية في مسائل التعاون العدلي والقضائي بين دول مجلس التعاون الخليجي، إذ يتجدد هذا النظام كل أربعة سنوات تلقائياً في حال عدم ورود ملاحظة عليه.

---

[17] أ. م. فاروق سعد، قانون الفضاء الكوني، الطبعة الثالثة، مطبعة صادر الحقوقية، بيروت، 2004، ص 203.

وقد سميت هذه الوثيقة ب (وثيقة الرياض للنظام القانوني الموحد لمكافحة جرائم تقنية المعلومات لدول مجلس التعاون الخليجي)، وتتكون من (39) مادة قانونية صيغت من قبل خبراء ذوي اختصاص من الدول الأعضاء، بهدف محاربة الجرائم السيبرانية وفرض العقوبة على مرتكبيها، وتم تحديد الأفعال في هذه الوثيقة أما العقوبات فقد تركت للدول الأعضاء، وهناك احكام واستنتاجات لوثيقة الرياض لمكافحة جرائم تقنية المعلومات[18].

-أحكام الوثيقة:

جاءت الوثيقة في المادة الأولى بالتعريفات، وفي المادة الثانية نصت على الاختصاص، ومن المادة (3) إلى المادة (30) نصت الوثيقة على الجوانب الموضوعية للجرائم، فقد جرمت الدخول غير المشروع وإتلاف المستندات المعلوماتية، والتزوير المعلوماتي، وكذلك الدخول إلى المواقع بشكل غير مشروع للقيام بفعل غير مشروع، كذلك تجريم استخدام البطاقات الائتمانية بشكل غير مشروع، وتجريم الاستفادة من القنوات المسموعة والمرئية بشكل غير مشروع.

ولم تنشط دول مجلس التعاون للخليج العربي في مجال التشريع فقط، بل أيضاً عقدت العديد من المؤتمرات في مجال الأمن السيبراني برعاية ومشاركة دول مجلس التعاون الخليجي، ففي عام 2008 انعقد المؤتمر الثاني لجرائم تقنية المعلومات في أبو ظبي بدولة الإمارات العربية المتحدة، وفي عام 2009، انعقد المؤتمر الدولي الثالث أيضاً في أبو ظبي لبحث الجوانب الإجرائية، وفي عام 2014 احتضنت أبو ظبي المؤتمر العالمي للأمن السيبراني، وكذلك مسقط بعمان إذ عقد مؤتمر الأمن السيبراني، وبالتعاون مع الاتحاد الدولي للاتصالات استضافت سلطنة عمان المؤتمر الإقليمي الثالث للأمن السيبراني، وترأس المؤتمر السنوي السادس للمراكز الوطنية للأمن السيبراني العماني بدول منطقة التعاون الإسلامي في بروناي، ومؤتمر الأمن السيبراني في الدوحة بدولة قطر بمشاركة شركة تانجينت لينك البريطانية.

ونستنتج من ذلك على ان عكس التشريعات على المستوى العربي المتمثلة بالاتفاقية العربية لمكافحة جرائم تقنية المعلومات، أو القوانين النموذجية الاسترشادية على مستوى الجامعة العربية، أو منظمة دول مجلس التعاون لدول الخليج العربي ثلاث حقائق مهمة: مدى النضج والوعي العربي لظاهرة الجرائم السيبرانية وآثارها على المستوى الاقتصادي والاجتماعي والثقافي، كما أنها تصيغ تشريعات تشمل طائفة واسعة من الجرائم السيبرانية راعت النصوص، الخلفية الثقافية والدينية والعادات والتقاليد الخاصة بالمجتمعات العربية، كما أنها تكاتف الجهود العربية المحلية والإقليمية لمواجهة الجرائم السيبرانية عبر سن تشريعات موحدة، وعقد العديد من المؤتمرات الإقليمية لمواجهة التطورات في مجال مكافحة الجرائم السيبرانية، والسعي لتوحيد فهم عام لهذه الظاهرة وسبل مكافحتها.

خاتمة

في ختام هذا البحث، يتضح أن الجرائم السيبرانية تمثل تحديًا متزايدًا يتطلب استجابة قانونية فعالة على المستويين الوطني والدولي. من خلال دراسة التشريعات الوطنية في العراق والمعاهدات الدولية كاتفاقية بودابست والاتفاقية العربية لمكافحة جرائم تقنية المعلومات، تم تسليط الضوء على الفجوات والتحديات التي تواجه الدول في مواجهة هذه الجرائم.

وبناء على ماتناولناه في إطار هذه الدراسة فقد توصلنا الى مجموعة من النتائج والمقترحات كانت **على النحو الآتي:**

---

[18] نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادي، منشورات الحلبي الحقوقية، بيروت، 2005، ص 251.

أولاً- النتائج:

1- هناك تباين كبير بين التشريعات الوطنية في الدول العربية، مما يعكس عدم وجود إطار قانوني موحد لمواجهة الجرائم السيبرانية.
2- لا تزال هناك فجوات قانونية في القوانين الوطنية، مما يجعلها غير قادرة على التعامل مع التعقيدات السريعة التي تطرأ على الفضاء السيبراني.
3- يتضح أن التعاون الدولي والإقليمي ضروري لتعزيز الأمن السيبراني، حيث أن الجرائم السيبرانية غالبًا ما تتجاوز الحدود الوطنية.
4- تواجه الدول تحديات كبيرة في تنفيذ القوانين الحالية، بما في ذلك نقص الموارد والتكنولوجيا اللازمة لمكافحة الجرائم السيبرانية.

ثانياً- التوصيات:

1- يجب العمل على توحيد التشريعات الوطنية في الدول العربية بما يتماشى مع المعاهدات الدولية، مما يسهل التعاون بين الدول في مكافحة الجرائم السيبرانية.
2- ينبغي توفير برامج تدريبية للكوادر القانونية والأمنية لتعزيز قدراتهم في التعامل مع الجرائم السيبرانية.
3- يجب تعزيز التعاون بين الدول من خلال تبادل المعلومات والخبرات، وإنشاء شبكات تعاون لمواجهة التهديدات السيبرانية.
4- تحديث التشريعات الوطنية بشكل دوري لتواكب التطورات السريعة في تكنولوجيا المعلومات والجرائم السيبرانية.

(المصادر)

أولاً- الكتب القانونية:

1- أ.د. أمير فرج يوسف، مكافحة جريمة الإرهاب الإلكتروني، الإرهاب الرقمي في ظل اتفاقية مجلس التعاون لمكافحة الإرهاب، الطبعة الأولى، دار الكتب والدراسات العربية، الإسكندرية، 2015.
2- أ.م. جيل برهام، تأثير تطور تكنولوجيا الحرب السيبرانية على بناء القوة في اسرائيل، ترجمة للعربية يولا البطل، مؤسسة الدراسات الفلسطينية، فلسطين، 2013.
3- أ.د. حسين محمد الغول، جرائم شبكة الأنترنت والمسؤولية الجزائية الناشئة عنها، الطبعة الأولى، مكتبة بدران الحقوقية للنشر والتوزيع، بيروت، لبنان، 2017.
4- أ.د. رامي متولي القاضي، مكافحة الجرائم المعلوماتية في التشريعات المقارنة وفي ضوء الاتفاقيات والمواثيق الدولية، الطبعة الأولى، دار النهضة العربية، القاهرة، 2011.
5- أ.م. سليمان أحمد فضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، دار النهضة العربية، القاهرة، 2013.
6- أ.د. عادل عبد صادق، أسلحة الفضاء الإلكتروني في ضوء القون الدولي الإنساني، مكتبة الإسكندرية، الإسكندرية، 2016.
7- أ.د. عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والانترنت، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2007.
8- أ.م. فاروق سعد، قانون الفضاء الكوني، الطبعة الثالثة، مطبعة صادر الحقوقية، بيروت، 2004.

9- نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادي، منشورات الحلبي الحقوقية، بيروت، 2005.
10- أ.م. نبيلة هبة هروال، الجوانب الاجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، دراسة مقارنة، دار الفكر الجامعي، الاسكندرية، 2013.
11- أ.د. هشام محمد فريد رستم، الجرائم المعلوماتية أصول التحقيق الجنائي الفني، الطبعة الثالثة، المجلد الأول، كلية الشريعة والقانون، جامعة الأمارات العربية المتحدة، 2004.

ثانياً- القوانين والمواثيق الدولية

1- البروتوكول الإضافي الأول لعام 1977.
2- اتفاقية مجلس أوروبا المتعلقة بالجريمة الالكترونية لعام 2001.
3- مشروع قانون جرائم المعلومات لسنة ٢٠١٨
4- الدستور العراقي الدائم لسنة ٢٠٠٥
5- قانون جهاز مكافحة الارهاب لسنة ٢٠٠٨
6- قانون العقوبات العراقي رقم 111 لعام 1969.

ثالثاً- المواقع الالكترونية:

1- د. زاهر الزبيدي، «تهديدات افتراضية للأمن السيبراني العراقي»، 2018، موقع شبكة النبأ المعلوماتية. https://annabaa.org/arabic/informatics/17379V
2- صفاء الكبيسي، «محاولات جديدة لتشريع قانون جرائم المعلوماتية تثير جدلاً في العراق»، 2022، موقع صحيفة العربي الجديد. https://www.alaraby.co.uk/entertainment_media