حقوق الانسان والأمن السيبراني
(للحق في الخصوصية وحرية التعبير عن الرأي)

الباحث

م.م زيدون طارق علي حمود

جامعة النهرين/ كلية هندسة المعلومات

البريد الإلكتروني Email : zaidoon.tariq@nahrainuniv.edu.iq

الكلمات المفتاحية: الأمن السيبراني، حقوق الإنسان، الحق في الخصوصية، حرية التعبير، الجرائم الإلكترونية، التشريعات الرقمية.

كيفية اقتباس البحث

حمود، زيدون طارق علي ، حقوق الانسان والأمن السيبراني (للحق في الخصوصية وحرية التعبير عن الرأي)،مجلة مركز بابل للدراسات الانسانية، حزيران ٢٠٢٦، المجلد:١٦ ،العدد:٦ .

مفهرسة في Indexed
IASJ

مسجلة في Registered
ROAD

Human Rights and Cyber security
(The Right to Privacy and Freedom of Expression)

Researcher
Asst. Lecturer. Zaidoon Tariq Ali Hamoud
Al-Nahrain University / College of Information Engineering

Keywords : Cyber security, Human Rights, Right to Privacy, Freedom of Expression, Cybercrime, Digital Legislation.

How To Cite This Article
Hamoud, Zaidoon Tariq Ali, Human Rights and Cyber security(The Right to Privacy and Freedom of Expression),Journal Of Babylon Center For Humanities Studies, june 2026,Volume:16,Issue 6.

Abstract

Iraq is experiencing a rapid digital transformation that has made cyberspace an essential domain for the exercise of human rights, particularly the right to privacy and freedom of expression. The widespread use of the Internet and digital platforms has enhanced access to information, community participation, and free communication. However, this development has also generated increasing challenges, including cybercrime, digital breaches, surveillance, and personal data theft, highlighting the importance of cyber security in protecting individuals and institutions. This research aims to clarify the concept of cyber security and its relationship with human rights, as well as to analyse the relevant legislative and regulatory frameworks at both the international and national levels. It further examines the current situation in Iraq and conducts a comparative study with the Kingdom of Saudi Arabia regarding cyber security policies and legislation. The study also discusses the extent to which existing laws and measures can achieve a balance between cyber security requirements and the protection of

fundamental rights and freedoms. The research concludes that building a secure digital environment requires the development of national legislation, the strengthening of legal and institutional oversight, and the promotion of digital awareness. Such efforts are essential to ensuring the protection of privacy and freedom of expression while effectively combating cyber threats and cybercrime in accordance with international human rights standards. This research aims to provide a comprehensive overview of the concept of cybersecurity and its importance, highlighting the nature of fundamental human rights, particularly the right to privacy and freedom of expression in cyberspace. It also seeks to review and analyze the regulatory and legislative frameworks at the international, regional, and national levels related to cybersecurity and its connection to the protection of human rights.

الملخص:

يشهد العراق تحولاً رقمياً متسارعاً جعل من الفضاء السيبراني جزءاً أساسياً من ممارسات حقوق الإنسان، ولا سيما الحق في الخصوصية وحرية التعبير عن الرأي، حيث ساهم انتشار الإنترنت والمنصات الرقمية في تعزيز الوصول إلى المعلومات والمشاركة المجتمعية والتواصل الحر، وفي المقابل، أفرز هذا التطور تحديات متزايدة تمثلت في الجرائم الإلكترونية والاختراقات الرقمية والتجسس وسرقة البيانات الشخصية، مما أبرز أهمية الأمن السيبراني في حماية الأفراد والمؤسسات، ويهدف هذا البحث إلى بيان مفهوم الأمن السيبراني وعلاقته بحقوق الإنسان، وتحليل الأطر التشريعية والتنظيمية ذات الصلة على المستويات الدولية والوطنية، مع دراسة واقع العراق وإجراء مقارنة مع المملكة العربية السعودية في مجال السياسات والتشريعات السيبرانية، كما يناقش البحث مدى قدرة التشريعات والإجراءات المعتمدة على تحقيق التوازن بين متطلبات الأمن السيبراني وحماية الحقوق والحريات الأساسية، ويخلص إلى أن بناء بيئة رقمية آمنة يتطلب تطوير التشريعات الوطنية، وتعزيز الرقابة القانونية والمؤسسية، ونشر الوعي الرقمي، بما يضمن حماية الخصوصية وحرية التعبير ومواجهة التهديدات والجرائم الإلكترونية وفق المعايير الدولية لحقوق الإنسان. يهدف البحث إلى تقديم رؤية متكاملة حول مفهوم الأمن السيبراني وأهميته، مع تسليط الضوء على طبيعة حقوق الإنسان الاساسية، ولا سيما الحق في الخصوصية وحرية التعبير في الفضاء السيبراني، كما يسعى إلى استعراض وتحليل الأطر التنظيمية والتشريعية على المستويات الدولية والإقليمية والوطنية ذات الصلة بالأمن السيبراني وعلاقته بحماية حقوق الإنسان

الأهمية:

تكمن أهمية هذا البحث في بيان أثر الأمن السيبراني على حماية حقوق الإنسان، ولاسيما الحق في الخصوصية وحرية التعبير عن الرأي في البيئة الرقمية، كما يسلط الضوء على التحديات التي تفرضها التقنيات الحديثة وضرورة تحقيق التوازن بين متطلبات الأمن وحماية الحقوق والحريات الأساسية للأفراد، فضلاً عن تقييم مدى توافر التشريعات القانونية والإجراءات التنظيمية التي تعتمدها الدولة لحماية هذه الحقوق ومواكبة التطورات التكنولوجية المتسارعة.

الأهداف:

يهدف البحث إلى تقديم رؤية متكاملة حول مفهوم الأمن السيبراني وأهميته، مع تسليط الضوء على طبيعة حقوق الإنسان الاساسية، ولا سيما الحق في الخصوصية وحرية التعبير في الفضاء السيبراني، كما يسعى إلى استعراض وتحليل الأطر التنظيمية والتشريعية على المستويات الدولية والإقليمية والوطنية ذات الصلة بالأمن السيبراني وعلاقته بحماية حقوق الإنسان، فضلاً عن إجراء مقارنة بين جهود كل من المملكة العربية السعودية والعراق في مجال تعزيز الأمن السيبراني، من حيث السياسات والتشريعات والممارسات التطبيقية، كذلك يهدف إلى رفع مستوى الوعي والتثقيف الرقمي لدى الأفراد، بما يعزز فهمهم لحقوقهم وواجباتهم في البيئة الرقمية، ويسهم في بناء مجتمع رقمي أكثر أمانًا ومسؤولية.

المشكلة:

يعد تأمين الفضاء السيبراني من التحديات المعقدة التي تفرضها طبيعة البيئة الرقمية، حيث تتيح للجهات الإجرامية التحرك والعمل عبر الحدود دون قيود جغرافية، فضلًا عن الترابط العميق بين الأنظمة الإلكترونية والبنى التحتية المادية، وما يرافق ذلك من صعوبة في السيطرة على الثغرات داخل الشبكات المتداخلة وما قد تخلّفه من آثار جسيمة، وفي هذا السياق، تبرز الحاجة الملحّة إلى اعتماد أفضل ممارسات الأمن السيبراني كخيار أساسي للدول لا غنى عنه. وفي ضوء ذلك، تتمحور إشكالية الدراسة حول جملة من التساؤلات، أبرزها: ما المقصود بالأمن السيبراني وما طبيعة علاقته بحقوق الإنسان من حيث المفهوم والأهمية؟ وهل يوجد إطار تنظيمي يندرج ضمن الرؤية الاستراتيجية السياسية في العراق؟ وإلى أي مدى تتوفر تشريعات تنظم مجال الأمن السيبراني وحقوق الإنسان؟ فضلًا عن التساؤل حول طبيعة حقوق الإنسان في الفضاء السيبراني وحدودها؟ وما هي أوجه التشابه والاختلاف بين العراق والمملكة العربية السعودية بالمجال التنظيمي والتشريعي الأمن السيبراني.

هيكلية البحث:

المبحث الأول: ماهية الأمن السيبراني وعلاقته بحقوق الإنسان

المطلب الأول: مفهوم الأمن السيبراني وأهميته

الفرع الأول: تعريف الأمن السيبراني

الفرع الثاني: أهمية الأمن السيبراني

المطلب الثاني: طبيعة حقوق الإنسان في الفضاء السيبراني

الفرع الأول: حقوق الإنسان في مجال الأمن السيبراني

الفرع الثاني: الانتهاكات السيبرانية لحقوق الإنسان

المبحث الثاني: الأبعاد القانونية والتنظيمية للأمن السيبراني

المطلب الأول: الإطار القانوني والتنظيمي للأمن السيبراني

الفرع الأول: الإطار التشريعي للأمن السيبراني على المستوى الدولي.

الفرع الثاني: الإطار التشريعي للأمن السيبراني على المستوى الإقليمي

المطلب الثاني: التجارب الوطنية في مجال الأمن السيبراني

الفرع الأول: جهود المملكة العربية السعودية في مجال الأمن السيبراني.

الفرع الثاني: جهود العراق في مجال الأمن السيبراني

المقدمة:

أدى التوسع المتسارع في استخدام تكنولوجيا المعلومات والاتصالات والتحول الرقمي إلى جعل الأمن السيبراني أحد أهم القضايا المعاصرة المرتبطة بحماية حقوق الإنسان في البيئة الرقمية. فمع تزايد الاعتماد على الفضاء الإلكتروني في مختلف مجالات الحياة، برزت تحديات جديدة تمس حقوق الأفراد الأساسية، وفي مقدمتها الحق في الخصوصية وحرية التعبير عن الرأي، اللذان يشكلان ركيزتين أساسيتين في المنظومة الدولية لحقوق الإنسان.

وفي ظل الارتفاع المستمر للهجمات الإلكترونية وتطور أساليبها، أصبحت البيانات الشخصية والمعلومات الرقمية عرضة لمخاطر الاختراق والاستغلال غير المشروع، مما يهدد خصوصية الأفراد وأمنهم الشخصي. كما أن بعض التدابير والإجراءات المتخذة في مجال الأمن السيبراني قد تثير إشكاليات تتعلق بحرية التعبير والوصول إلى المعلومات إذا لم تُمارس ضمن أطر قانونية تضمن التوازن بين متطلبات الأمن وحماية الحقوق والحريات الأساسية.

وتزداد أهمية هذا الموضوع مع التطور المستمر للتقنيات الرقمية والذكاء الاصطناعي والحوسبة السحابية وغيرها من التقنيات الناشئة التي توفر فرصًا واسعة للتنمية والتواصل، لكنها في الوقت

Journal Of Babylon Center For Humanities Studies 2026 Volume :16 Issue : 6
(ISSN): 2227-2895 (Print) (E-ISSN):2313-0059 (Online)

ذاته تخلق تحديات قانونية وأمنية جديدة. لذلك أصبح من الضروري وضع تشريعات وسياسات فعالة تستند إلى المعايير الدولية لحقوق الإنسان، وتنسجم مع القوانين الوطنية، بما يحقق حماية الفضاء السيبراني ويضمن احترام الحق في الخصوصية وحرية التعبير، ويعزز الثقة في البيئة الرقمية على المستويين الفردي والمؤسسي.

المبحث الأول

ماهية الأمن السيبراني وعلاقته بحقوق الانسان

المطلب الأول: مفهوم الأمن السيبراني واهميته

تتزايد أهمية الأمن السيبراني بشكل متزايد بسبب الاعتماد المتزايد على أنظمة الكمبيوتر والإنترنت ومعايير الشبكات اللاسلكية، وبسبب نمو الأجهزة الذكية والأجهزة المختلفة التي تشكل ونظراً لتعقيده، سياسياً وتكنولوجياً، يُعدّ الأمن السيبراني أحد التحديات الرئيسية في عالمنا المعاصر.

الفرع الأول: تعريف الأمن السيبراني.

الأمن في اللغة ضد الخوف وأصل الأمن الطمأنينة، و(الأمن، والأمانة والاستئمان) كلها معان تدل على توافر الطمأنينة لنفس الأنسان، أي زوال كل ما من شأنه أن يهدد حياته، أي اطمئن ولم يخف فهو آمن، والأمن ضد الخوف (الرازي، ١٩٩٨، الصفحات ٢٢-٢٣)، وأمن البلد أي أطمأن به أهله فهو آمن (الفيومي، صفحة ١٠)ويعني الحماية والسلامة والاستقرار. والأمن اصطلاحاً يعرف بأنه (الإجراءات التي تتخذ لحفظ أسرار الدولة وتأمين أفرادها ومنشآتها ومصالحها الحيوية في الداخل والخارج، والقدرة على مواجهة الأحداث والطوارئ دون اضطراب) (مصطفى، ٢٠٢٣). ومعنى مصطلح لفظ (السيبراني) فهو ترجمة لمصطلح الانكليزية (cyber) ومعناها هو الافتراضي أو المتخيل، ولها دلالات مختلفة لأي شيء مرتبط بثقافة الحواسيب أو تقنية المعلومات أو الواقع الافتراضي، ويشير إلى ذلك الحيز الذي تتم فيه ومن خلاله اغلب الأنشطة السيبرانية "فضاء الإنترنت" (برى، ٢٠١٩، صفحة ١٠)، **الأمن السيبراني:** وهو مجموعة من الوسائل التقنية والإدارية التي يتم استخدامها لمنع الاستخدام الغير مصرح به على شبكات الحاسوب وسوء الاستغلال واستعادة المعلومات الإلكترونية التي تحتويها بغية ضمان واستمرارية عمل نظم المعلومات، وتأمين الحماية والسرية والخصوصية للبيانات الخاصة بفواعل الفضاء السيبراني (بوغرارة، ٢٠١٨، صفحة ١٠٦).

ويعرفه الاتحاد الدولي للاتصالات (ITU) بأنه: مجموعة من المهمات مثل تجميع وسائل وسياسات وإجراءات أمنية، ومبادئ توجيهية ومقاربات لإدارة المخاطر، وتدريبات، وممارسات

فضلى، وتقنيات، يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين (ITU, 2008). ويعرف بأنه: أمن الشبكات والأنظمة المعلوماتية والبيانات والمعلومات والأجهزة المتصلة بالإنترنت، وهو المجال الذي يتعلق بإجراءات ومقاييس ومعايير الحماية المفروض اتخاذها، أو الالتزام بها لمواجهة التهديدات، ومن التعديات، أو الحد من أثرها في أقسى واسوأ الاحوال (الزهراني، ٢٠٢٠، صفحة ١١). وتعرفه مديرية الأمن السيبراني في وزارة الداخلية العراقية: هو مجموعة الإجراءات والتقنيات والسياسات المستخدمة لحماية الفضاء السيبراني من التهديدات والاختراقات والحد من الهجمات الإلكترونية (مديرية الامن السيبراني، ٢٠٢٢).

كما عرفته الوكالة الأمريكية للأمن السيبراني وأمن البنية التحتية بأنه : فن حماية الشبكات والأجهزة والبيانات من الوصول غير المصرح به أو الاستخدام الإجرامي وممارسة ضمان السرية والنزاهة وتوافر المعلومات (CISA, 2009). ويمكن تعريفه بأنه : مجموعة الممارسات التي ترمي إلى حماية الأنظمة والشبكات والبرامج من الهجمات الرقمية أياً كان نوعها، وهذه الممارسات متنوعة إلى تدابير احتياطية استباقية قبل وقوع الخلل، وعلاجية بعد وقوع الخلل (الطيار، ٢٠٢٠، صفحة ٢٦٤).

يمكن تعريف الأمن السيبراني بأنه: مجموعة من التدابير والممارسات التي تُتخذ لحماية الشبكات والأنظمة الإلكترونية والبيانات والمعلومات الحساسة، بما في ذلك البنية التحتية الحيوية، من التهديدات والهجمات الإلكترونية التي تستهدف الدول والأفراد، ويهدف إلى ضمان سرية المعلومات ونزاهتها وتوافرها، مع تأكيد حماية حقوق الإنسان وصون مصالحه الحيوية في البيئة الرقمية.

الفرع الثاني: اهمية الامن السيبراني لحقوق الانسان

أهمية الأمن السيبراني وعناصر:

أدى التطور والانفتاح التكنولوجي الذي نعيشه اليوم مع الأنظمة الإلكترونية إلى تزايد الاعتماد على هذه التكنولوجيات في التنمية الاقتصادية والاجتماعية، إلا أن الانفتاح جعلها عرضة للتهديدات والخاطر الإجرامية من قبل المخترق أو المهاجم أو الدخيل، بالتالي من الضروري فهم وإدراك هذه المخاطر ومن ثم وضع الأطر القانونية والتنظيمية والإجرائية لمواجهة المخاطر السيبرانية وتوعية المؤسسات والأفراد حول المخاطر وآثارها على أعمالهم وحياتهم الشخصية.

يرتبط الأمن السيبراني بالجريمة الإلكترونية التي هي أساس الأمن المعلوماتي الذي يعمل على مكافحتها، وهي عبارة عن جرائم ذكية تنشأ في البيئة الإلكترونية أو الافتراضية، حيث قوم بها أفراد أو منظمات لديهم درجة عالية من الذكاء ويمتلكون المعرفة والتقنية، مما يتسبب في خسائر

فادحة للمجتمع، وتظهر أهميته في عالمنا المترابط بواسطة الشبكة العنكبوتية، إذ أصبح يمثل عنصراً مهماً في الحياة الإنسانية على كافة المستويات السياسية والاقتصادية والاجتماعية، فهو الآن عصب الحياة الحالية التي تعتمد عليها الدول والأفراد في كل معاملاتها، بل اصبح ينظر إليه بأنه رافد جديد للأمن القومي، وجزء من الأمن الجماعي، بما أن العلاقة بين الأمن والتكنولوجيا علاقة مترابطة ومتزايدة، مع إمكانية تعرض المصالح الاستراتيجية إلى مخاطر إلكترونية، الأمر الذى يهدد بتحول دور الأنظمة الإلكترونية لوسيط ومصدر لأدوات الصراع الدولي (علاء الدين فرحان، ٢٠٢١).

ثانياً: أنواع الأمن السيبراني (Gregg Lindemulder, 2024):

١.أمان الشبكة (حماية الشبكات من الوصول غير المصرح به).

٢.أمان التطبيقات (ضمان أمان البرامج والتطبيقات).

٣.أمن المعلومات أو البيانات (حماية البيانات الحساسة).

٤.أمن السحابة (حماية التخزين السحابي والتطبيقات).

٥.أمان نقاط النهاية (حماية الأجهزة مثل أجهزة الكمبيوتر المحمولة والهواتف).

٦.الأمن التشغيلي (إدارة بروتوكولات الأمن الداخلي).

٧.أمن إنترنت الأشياء (IoT).

وبما أنّ الجرائم السيبرانية، بطبيعتها، عابرة للحدود، فإنّها تتطلّب تعاوناً بين الدول والمؤسسات المعنية لإجراء التحقيقات فيها وملاحقة المرتكبين، وقبل اعتماد اتفاق عالمي لمكافحة الجرائم السيبرانية، لم يتوفّر تعريف متّفق عليه لهذه الجرائم، فنشأت اختلافات بشأن الممارسات التي تعتبرها الدول المختلفة جرائم سيبرانية، ما أدّى إلى تناقضات في التنفيذ والملاحقة القضائية، وحماية البنية التحتية الحيوية للدول و حقوق الأنسان.

يعد الأمن السيبراني القوي ركيزة أساسية لحماية الأفراد من تهديدات مثل المراقبة الرقمية والرقابة وتسريب البيانات، مما يساهم في تعزيز حقوقهم في الخصوصية وحرية التعبير. ومع ذلك، يبرز جانب إشكالي عندما تؤطّر هذه القضايا ضمن مفهوم (الأمن القومي)، إذ قد تستغل بعض الدول هذا الإطار لتبرير فرض المراقبة، أو تقييد الحريات، أو استهداف المعارضين والصحفيين والناشطين، وتتجلى المفارقة في الدور المزدوج للدول، فهي مطالبة بحماية الفضاء الرقمي، لكنها قد تنخرط في الوقت ذاته في ممارسات اختراق أو في سباق تسلح سيبراني، ما يؤدي إلى زيادة التهديدات بدلاً من الحدّ منها. وفي ظل هذا الواقع، تتأثر مجموعة من الحقوق الأساسية، مثل

الحق في الخصوصية وحرية التعبير وحرية التجمع والوصول إلى المعلومات، حيث تصبح عرضة للتقييد أو الانتهاك (SOHAIR AHMED SHAIKH، ٢٠٢٥).

كما أن التوسع في استخدام التكنولوجيا الرقمية أدى إلى جمع كميات ضخمة من البيانات الشخصية من قبل الحكومات والشركات، مما يفاقم التحديات المرتبطة بحماية الخصوصية. ويمكن أن تسهم المراقبة والهجمات الإلكترونية، خاصة تلك التي تستهدف وسائل الإعلام أو الأفراد، في تقليص مساحة حرية التعبير والحد من تدفق المعلومات. فضلاً عن ذلك، فإن إساءة استخدام تقنيات المراقبة قد تؤدي إلى تقويض الحريات السياسية والمدنية بشكل أوسع (Robb Shawe، ٢٠٢٥).

عليه يتطلب التداخل بين الأمن السيبراني وحقوق الإنسان اعتماد إطارٍ شامل يضع معايير حقوق الإنسان في صميم السياسات والممارسات الأمنية. ومن الضروري تحقيق توازن دقيق بين متطلبات الأمن وحماية الحريات، بحيث لا تؤدي الجهود الرامية إلى تأمين الفضاء الرقمي إلى المساس بالحقوق الأساسية التي يُفترض أن تصونها.

المطلب الثاني: طبيعة حقوق الإنسان في الفضاء السيبراني

يتمتع الأنسان بحقوق ثابتة بغض النظر عن الزمان والمكان بما في ذلك الفضاء السيبراني، ويجب على الدول والأفراد احترامها وحمايتها في جميع الظروف، وهي مجموعة من الحقوق الأساسية التي يجب أن يتمتع بها الأفراد في البيئة الرقمية، مثل الحق في الخصوصية، وحرية التعبير، والحق في الوصول إلى المعلومات، والحماية من التمييز، والأمن الرقمي، هذه الحقوق تتشابك مع القضايا الأمنية في الفضاء السيبراني، مما يتطلب توازنًا دقيقًا بين حماية هذه الحقوق وتعزيز الأمن الرقمي.

الفرع الأول: حقوق الإنسان في مجال الأمن السيبراني

أدى التطور المتسارع في التكنولوجيا الرقمية إلى تسهيل الوصول إلى الإنترنت ووسائل التواصل الاجتماعي بشكل غير مسبوق، ورغم ما توفره من فوائد كبيرة في مجالات التواصل والمعرفة، إلا أنها تطرح تحديات جدية على مستوى الحقوق والحريات. فقد تُستخدم هذه التقنيات في المراقبة الرقمية، والمضايقات عبر الإنترنت، والتحيزات الخوارزمية، وأتمتة اتخاذ القرار دون شفافية، مما قد يؤدي إلى انتهاك الحقوق وتفاقم عدم المساواة، خاصة لدى الفئات المهمشة، وفي هذا الإطار، يبرز الأمن السيبراني كعامل مزدوج؛ إذ يسهم في حماية البيانات والأنظمة، لكنه قد يستغل أيضًا لتبرير انتهاك الحق في الخصوصية من خلال التوسع في جمع البيانات أو مراقبة

الأفراد دون ضوابط قانونية واضحة. (الامم المتحدة، مكتب المفوض السامي لحقوق الانسان، ٢٠٢٥).

أولا: الحق في الخصوصية وحماية البيانات الشخصية.

الحق في الخصوصية يعتبر حقًا أساسيًا من حقوق الإنسان، وتم الاعتراف به على المستوى الدولي والوطني، وذلك من خلال تأكيد الاعلان العالمي لحقوق الانسان ، وما تناولته (المادة ١٧) من العهد الدولي الخاص بالحقوق المدنية والسياسية بأنه: (لا يجوز تعريض أي شخص، على نحو تعسفي أو غير قانوني، لتدخل في خصوصياته أو شؤون أسرته أو مسكنه أو مراسلاته، ولا لأي حملات غير قانونية تمس شرفه وسمعته. ولكل شخص الحق في حماية القانون من مثل هذا التدخل أو تلك الحملات) (الإعلان العالمي لحقوق الإنسان، ١٩٤٨).

على الصعيد الوطني، كفل دستور العراق لعام ٢٠٠٥ الحق في الخصوصية بشكل صريح في المادة (١٧)، التي تنص على أن لكل فرد حقًا في الخصوصية الشخصية بما لا يتعارض مع حقوق الآخرين والآداب العامة. كما تضمّن قانون العقوبات العراقي نصوصًا تُجرّم انتهاك الخصوصية، مثل إفشاء الأسرار أو التنصت على المحادثات. وأكد قانون المحاماة بدوره التزام المحامي بالحفاظ على سرية ما يُؤتمن عليه بحكم مهنته، حتى بعد انتهاء وكالته، باستثناء ما يهدف إلى منع وقوع جريمة. كذلك نص قانون نقابة الصحفيين العراقيين رقم (١٧٨) لسنة ١٩٦٩، في المادة (٢٥)، على حظر تضليل الجمهور بالمعلومات غير الصحيحة، ووجوب تصحيح الأخطاء فورًا، تأكيدًا لحق الرد بوصفه حقًا أساسيًا. (قانون نقابة الصحفيين رقم ١٧٨المعدل، ١٩٦٩).

وتشمل سمات البيانات الشخصية في إطار الخصوصية المعلوماتية عدة أنواع تختلف بحسب طبيعتها وحساسيتها، ويمكن تلخيصها كما يأتي:

١-البيانات الفردية: وهي المعلومات التي تُعرّف بالشخص بشكل مباشر، مثل الاسم، الصورة، الجنسية، محل السكن، والمهنة.

٢-البيانات المدنية: تشمل البيانات الرسمية التي تنظمها الجهات الحكومية، مثل تاريخ الميلاد، الجنس، الحالة الاجتماعية، العنوان، وغيرها من المعلومات التي تحظى بحماية قانونية نظراً لحساسيتها (قانون تسجيل الولادات والوفيات العراقي، ١٩٧١)..

٣-البيانات الاجتماعية: تتعلق بحياة الفرد الاجتماعية ومكانته وعلاقاته، بما في ذلك تفاصيل حياته الأسرية وتفاعلاته مع المجتمع (باسم محمد فاضل، ٢٠١٨).

٤-البيانات الصحية: هي المعلومات المرتبطة بالحالة الصحية للفرد، وتُعد من أكثر البيانات خصوصية، لذلك يُحظر كشفها أو معالجتها دون مبرر قانوني (Paula Lobato de Faria, 2014).

٥-البيانات المالية: تتعلق بالوضع المالي للفرد، كالدخل، النفقات، الديون، والسمعة الائتمانية، وتتميز بسرية عالية ولا يجوز تداولها دون ضوابط (اديب ميالة و مي محرزي، ٢٠١١).

تعد الهجمات السيبرانية من أبرز التهديدات لأمن الدول واقتصادها وسلامة المجتمع، إذ تشمل أنشطة مثل القرصنة، والفيروسات، وسرقة الهوية والبيانات، والتلاعب بها، وبرامج الفدية، وهجمات حجب الخدمة، والاحتيال الإلكتروني. كما توسّع المجرمون في ارتكاب جرائم مالية عبر الإنترنت، إلى جانب ظواهر مثل التنمر الإلكتروني، والمضايقات، ونشر الأخبار الكاذبة. وتتزايد هذه التهديدات بوتيرة متسارعة مع تطور التكنولوجيا. (البداينة، ٢٠١٤).

تتزايد الهجمات السيبرانية وتعد تهديداً خطيراً في عالمنا اليوم، إذ كبدت هذه الهجمات الاقتصاد العالمي في العام ٢٠٢٣ خسائر تفوق قيمتها تسعة تريليونات دولار، مقارنةً بـ ٨٦٠ مليار دولار في عام ٢٠١٧، وفقًا لتقديرات ، من المتوقع أن ترتفع التكلفة العالمية للهجمات الإلكترونية في السنوات الأربع المقبلة، من ٩.٢٢ تريليون دولار في عام ٢٠٢٤ إلى ١٣.٨٢ تريليون دولار بحلول عام ٢٠٢٨ (Steve Morgan، ٢٠٢٤). ولهذه الهجمات الإلكترونية أشكال متعددة من بينها، هجمات برامج الفدية* ، واختراق البريد الإلكتروني للشركات، وانتهاكات البيانات، وهجمات حجب الخدمة الموزعة (DDoS)، وسرقة الملكية الفكرية، والاحتيال المالي وسرقة الهوية، واستخدام برامج التجسس. ومن الأمثلة على المخاطر الشديدة المرتبطة بالتجسس الإلكتروني برمجية " بيغاسوس" (Pegasus)، التي طورتها شركة NSO Group الإسرائيلية (Kali Robinson، ٢٠٢٢).

تستطيع هذه البرمجية اختراق الأجهزة الجوالة خلسة، ما يتيح للجهة المهاجمة الوصول إلى الرسائل النصية والرسائل الإلكترونية والصور، وحتّى تشغيل الكاميرا والميكروفون، وقد استُخدم برنامج التجسس هذا لمراقبة الصحافيين والناشطين في مجال حقوق الإنسان والمعارضين السياسيين في جميع أنحاء العالم. يهدد هذا الاستخدام واسع النطاق الخصوصية الفردية ويقوّض المؤسسات الديمقراطية وسيادة القانون، كما ينشئ بيئة من الخوف وعدم الثقة، يمارس فيها

* برامج الفدية هي نوع من البرمجيات الخبيثة التي تصيب جهاز كمبيوتر الضحية أو شبكته، وتُشفّر ملفاته أو تقيّد الوصول إلى نظامه. ثم يطلب المهاجم فدية من الضحية مقابل استعادة الوصول إلى البيانات أو النظام.

الأفراد الرقابة الذاتية أو يتجنبون الانخراط في أنشطة شرعية خوفاً من مراقبة تحركاتهم، ويُعتبر هذا التراجع في الحريات المدنية من تداعيات الهجمات السيبرانية التي تتجاوز الخسائر المادية لتؤثر أيضاً على النسيج المجتمعي (ميتيهان دورماز، ٢٠٢٤).

كما إن الحق في الخصوصية يمهد التمتع بحقوق الإنسان الأخرى، وبالتالي، قد يؤثر التمييز وعدم المساواة في التمتع بالحق في الخصوصية في مجال المراقبة وجمع البيانات ومعالجتها على حقوق أخرى، بما في ذلك الحق في الحياة والحرية والأمن، وحرية التعبير، وحرية التجمع السلمي، وحرية التنقل، والصحة، والتعليم والسكن. لذا يؤدي الحق في الخصوصية دوراً محورياً في توازن القوى بين الدولة والفرد، وهو حق أساسي لممارسة الحقوق في مجتمع ديمقراطي، وتتزايد أهميته في التمتع بحقوق بالحقوق الاخرى وممارستها الفضاء الرقمي وخارجه (الجمعية العامة، ٢٠٢٥).

عليه اصبح وصول المستخدمين للتكنولوجيا وخدمات الإنترنت والاتصالات على نطاق واسع حول العالم، وبالتالي أصبحت التهديدات السيبرانية أسهل وأكثر انتشاراً، وذات طبيعة عابرة للحدد وبشكل متزايد، لذلك يمثل الفضاء السيبراني تهديدًا متزايدًا على حقوق الدول والمؤسسات والأفراد ، حيث يشكل مجالًا خصبًا للتهديدات، والانتهاكات الأمنية، والتلاعب بالمعلومات، مما يؤثر سلبًا على الحق في الخصوصية والأمان والرفاهية العامة.

ثانياً: حرية التعبير والرأي عبر الإنترنت والحق في الوصول للمعلومات.

يعد الحق في حرية الرأي والتعبير من الحقوق التي أكدها القانون الدولي عام ١٩٤٨ عبر الإعلان العالمي لحقوق الإنسان حيث تنص (المادة ١٩) على أن: (لكل شخص الحق في حرية الرأي والتعبير، ويشمل هذا الحق حرية اعتناق الآراء دون أي تدخل، واستقاء الأنباء والأفكار وتلقيها ونقلها إلى الآخرين، بأية وسيلة ودونما اعتبار للحدود). وقد تم ترسيخ هذا الحق من خلال (المادة ١٩) من "العهد الدولي الخاص بالحقوق المدنية والسياسية"، وتتألف الحقوق الواردة في المادة المذكورة من ثلاثة فقرات أساسية وهي (العهد الدولي الخاص بالحقوق المدنية والسياسية، ١٩٦٦): (الحق في اعتناق الآراء دون تدخل (حرية الرأي). لكل إنسان حق في حرية التعبير. ويشمل هذا الحق حريته في التماس مختلف ضروب المعلومات والأفكار وتلقيها ونقلها إلى آخرين دونما اعتبار للحدود، سواء على شكل مكتوب أو مطبوع أو في قالب فني أو بأية وسيلة أخرى يختارها. (الوصول إلى المعلومات). الحق في نقل المعلومات (حرية التعبير). إن ممارسة الحقوق المنصوص عليها في الفقرة ٢ من هذه المادة تستلزم واجبات ومسؤوليات خاصة. ولذلك، يجوز إخضاعها لبعض القيود، شريطة أن تكون محددة بنص القانون وأن تكون

ضرورية: (أ) لاحترام حقوق الآخرين أو سمعتهم؛ (ب) لحماية الأمن الوطني أو النظام العام أو الصحة العامة أو الآداب العامة.

كما أن حرية التعبير عن الرأي عبر الإنترنت هي حق أساسي من حقوق الإنسان، إذ نصت (المادة ١٩) الفقرة الثانية من العهد الدولي الخاص بالحقوق المدنية والسياسية على أن الحق في حرية التعبير ينطبق بغض النظر عن الحدود وبأي وسيلة يختارها الفرد، ليتضح لنا أن المادة المذكورة تشمل وسائل الاتصال عبر الإنترنت. وقد أكد مجلس حقوق الإنسان التابع للأمم المتحدة في قراره صدر عام ٢٠١٦ (الأمم المتحدة، ٢٠١٦): (إن الحقوق نفسها التي يتمتع بها الناس خارج الإنترنت يجب حمايتها أيضًا عبر الإنترنت، وخاصة حرية التعبير، التي تنطبق بغض النظر عن الحدود ومن خلال أي وسيلة من اختيار الفرد)، وفقًا للمادة ١٩ من الإعلان العالمي لحقوق الإنسان والعهد الدولي الخاص بالحقوق المدنية والسياسية.

جاء الحق في حرية التعبير عن الرأي مكرساً في الدستور العراقي من خلال (المادة ٣٨)، إذ تكفل الدولة وبما لا يخل بالنظام العام والآداب: (اولاً: حرية التعبير عن الرأي بكل الوسائل. ثانياً : حرية الصحافة والطباعة والاعلان والاعلام والنشر. ثالثاً : حرية الاجتماع والتظاهر السلمي وتنظم بقانون.).

وفي العصر الرقمي واجه الحق في حرية التعبير عن الرأي العديد من التحديات ؛ في ظل انتشار وسائل التواصل الاجتماعي والمنصات الرقمية، أصبح من السهل على الحكومات والشركات التي تسعى إلى تنظيم الجرائم الإلكترونية المتزايدة، من مراقبة وتقييد الرأي العام، من خلال استخدام تقنيات المراقبة المتطورة على الهواتف المحمولة وغيرها، مما يفرض قيود على حرية التعبير عن الرأي.

الفرع الثاني: الانتهاكات السيبرانية لحقوق الإنسان

أولاً: التجسس الرقمي وانتهاك الحق في الخصوصية

الفئات الرئيسية الفاعلة في الهجمات السيبرانية:

١-الدول:

حكومات أو أجهزة استخبارات، تهدف إلى التجسس، التخريب، أو التأثير السياسي، غالبًا ما تستهدف بنى تحتية حساسة (كهرباء، اتصالات، دفاع) مثال: هجمات مرتبطة بصراعات جيوسياسية. (ستيف مور، ٢٠٢٦).

٢-الناشطون الرقميون:

Journal Of Babylon Center For Humanities Studies 2026 Volume :16 Issue : 6
(ISSN): 2227-2895 (Print) (E-ISSN):2313-0059 (Online)

أفراد أو مجموعات يستخدمون أدوات الاختراق للتعبير عن مواقف أيديولوجية أو سياسية، وغالبًا لا يهدفون إلى تحقيق مكاسب مالية، بل يسعون للتأثير أو الاحتجاج الرقمي (باسم علي خريسان، ٢٠٢٢).

٣-الجماعات الإجرامية السيبرانية:

شبكات منظمة تهدف إلى تحقيق أرباح مادية من خلال أنشطة غير قانونية مثل سرقة البيانات، وطلب الفدية، والاحتيال المالي. وغالبًا ما يكون من الصعب تحديد مواقعهم بسبب انتشارهم الدولي.

٤-الجهات المدعومة من الدول:

مجموعات تعمل بدعم أو توجيه من حكومات، وتهدف إلى تحقيق مصالح سياسية أو استراتيجية. وغالبًا ما تنفذ عمليات تجسس أو هجمات معقدة، مما يجعل تتبعها ومحاسبتها أمرًا صعبًا (صلاح حيدر عبد الواحد، ٢٠٢١).

٥-المرتزقة السيبرانيون :

أفراد أو شركات خاصة يقدمون خدمات هجومية أو دفاعية في المجال السيبراني مقابل المال، سواء لصالح دول أو شركات أو حتى جهات غير رسمية، مما يثير إشكاليات قانونية وأخلاقية كبيرة بسبب تسليع القدرات الرقمية (محمد يوسف، ٢٠٢٤).

تعد القوانين والمواثيق الدولية لحقوق الإنسان ضمان للفرد وحماية حياته الشخصية وأسراره ومراسلاته وبياناته من أي تدخل أو انتهاك غير مشروع. فالخصوصية تمثل جزءًا مهمًا من كرامة الإنسان وحريته، وتوفر له الشعور بالأمان والثقة في المجتمع. ومع التطور التكنولوجي المتسارع وانتشار وسائل الاتصال الحديثة والإنترنت، أصبح موضوع حماية الخصوصية أكثر تعقيدًا، حيث تزايدت أشكال الانتهاكات التي قد يتعرض لها الأفراد، مثل التنصت على الاتصالات، أو اختراق الحسابات الإلكترونية، أو نشر المعلومات الشخصية دون إذن صاحبها. كما قد تصدر هذه الانتهاكات من أفراد أو مؤسسات أو حتى جهات رسمية إذا لم تكن هناك ضوابط قانونية واضحة تحمي هذا الحق. وتتمثل هذه الانتهاكات في التالي: (الامم المتحدة، الجمعية العامة، ٢٠٢٢).

١-مراقبة الاجهزة الشخصية والاتصالات:

في ظل التطور التكنولوجي المتسارع، أصبحت البيانات من أهم الموارد التي تعتمد عليها المجتمعات الحديثة. فهي لم تعد مجرد معلومات عابرة، بل تحولت إلى عنصر أساسي في اتخاذ القرارات ورسم السياسات، سواء على المستوى الحكومي أو المؤسسي.

ومع هذا التوسع الكبير في استخدام البيانات، برزت تساؤلات مهمة حول كيفية إدارتها وتنظيمها، ومن المسؤول عن حمايتها وضمان خصوصيتها. فالتعامل مع البيانات يتطلب وجود أنظمة واضحة تضمن دقتها وسلامتها، إضافة إلى تشريعات تحمي الأفراد من سوء الاستخدام. لذلك، فإن تنظيم البيانات وإدارتها بشكل فعّال أصبح ضرورة ملحّة، ليس فقط للاستفادة منها، بل أيضًا للحفاظ على الأمن المعلوماتي وتعزيز الثقة في الأنظمة الرقمية.

أصبحت الأجهزة الشخصية مثل الهواتف الذكية والحاسبات ووسائل التواصل الإلكتروني جزءًا أساسيًا من حياة الإنسان اليومية. وقد رافق هذا التطور ظهور تحديات قانونية تتعلق بحماية خصوصية الأفراد وضمان عدم انتهاك بياناتهم أو مراقبة اتصالاتهم بطرق غير مشروعة (حسنين علاء محمد، ٢٠٢٥). حيث تتعرض فئة كبيرة من الأفراد لهجمات سيبرانية تهدف إلى الاستيلاء على هوياتهم أو معلوماتهم الشخصية أو أموالهم، ومن بين هذه الهجمات هي برمجيات الفدية و التصيد الاحتيالي؛ إذ يعتمد المهاجمون في برمجيات الفدية على تشفير ملفات الضحية ثم ابتزازها مقابل فك التشفير، بينما يستخدمون في التصيد الاحتيالي رسائل وهمية لخداع المستخدمين وحملهم على مشاركة كلمات المرور أو البيانات المالية، مما يشكل خطرًا بالغًا على خصوصيتهم (ايمن إسماعيل، ٢٠٢٥).

٢-مراقبة العامة :

شهد العالم انتشاراً متسارعاً لكاميرات المراقبة في الفضاءات العامة كالشوارع ومواقف السيارات ومراكز النقل، مع توقعات بتجاوز عددها مليار كاميرا على مستوى العالم، وبلوغ كثافتها في بعض المدن أكثر من ١٠٠ كاميرا لكل ألف نسمة. ولا تقتصر هذه الأنظمة على الجهات الحكومية، بل تمتلك شركات خاصة تقنيات مراقبة متطورة، قد تتيح مشاركة البيانات مع السلطات، الأمر الذي يوسّع نطاق الرصد ويثير إشكاليات تتعلق بالشفافية والمساءلة. كما شهدت الكاميرات تطوراً كبيراً بفضل اعتمادها على تقنيات الذكاء الاصطناعي، مثل التعرف على الوجوه وتحليل السلوكيات، وهي قدرات تثير مخاوف متزايدة بشأن انتهاك الخصوصية. إضافة إلى ذلك، أصبح استخدام الطائرات المسيّرة شائعاً في عمليات المراقبة، خاصة أثناء التجمعات العامة والاحتجاجات (الامم المتحدة، الجمعية العامة، ٢٠٢٢).

وتشهد هذه التطورات عادةً ارتباطاً وثيقاً بظهور أنظمة هوية حديثة وتوسّع استخدام قواعد البيانات البيومترية. ففي عدد من الدول، تعتمد أنظمة الهوية على تخزين مركزي مكثّف للبيانات الشخصية، بما يشمل المعلومات البيومترية مثل بصمات الأصابع، وملامح الوجه، ومسح قزحية العين، وحتى الحمض النووي. إضافةً إلى ذلك، غالباً ما تكون هذه القواعد مترابطة وقابلة

للوصول والبحث من قبل جهات حكومية متعددة. ونتيجة لذلك، بات التعرف على هوية الأفراد في مختلف الأماكن أكثر سهولة من أي وقت مضى (اللجنة الدولية للصليب الاحمر، ٢٠٢٤).

ثانياً الرقابة الالكترونية وتقييد حرية التعبير على الانترنت

لقد تزايدت وتيرة الجرائم الإلكترونية وتعقيدها وتكلفتها في السنوات الأخيرة ، وأصبحت مواجهتها صعبة للغاية. إذ يبلغ متوسط تكلفة اختراق البيانات عالميًا نحو ٤.٤٤ مليون دولار، مع تفاوت كبير بين الدول، حيث تصل في الولايات المتحدة إلى ١٠.٢٢ مليون دولار مقابل ٢.٥١ مليون دولار في الهند. وتكون الخسائر أكبر في القطاعات الخاضعة لرقابة مشددة مثل الرعاية الصحية، التي سجلت أعلى تكلفة اختراق بنحو ٧.٤٢ مليون دولار في عام ٢٠٢٥ (Palatty James Nivedita، ٢٠٢٦). ويزداد الإجماع والتعاون الدوليان أهميةً لمواجهة المخاطر المتسارعة التي تشكلها هذه الجرائم على الدول والشركات والأفراد. من بين هذه الهجمات، أعلنت (حكومة كوستاريكا) حالة طوارئ وطنية عقب تعرّضها لهجوم ببرنامج فدية أدّى إلى قطع الاتصال عن ٢٧ جهة حكومية، ما تسبب في تعطّل الخدمات اليومية لعدة أشهر. في حين قام موظف في (شركة متعددة الجنسيات) في هونغ كونغ بتحويل مبلغ ٢٥.٦ مليون دولار أمريكي بعد تلقيه تعليمات خلال مكالمة عبر تطبيق «زووم» مع أشخاص ظنّ أنهم زملاؤه، ليتبيّن لاحقًا أن جميع المشاركين كانوا مزيفين، وأن الأموال أُرسلت إلى حسابات وهمية (Charlie Plumb، ٢٠٢٤). كما تعرّضت شركة إعداد التقارير الائتمانية Equifax لاختراق كبير، إذ تمكن القراصنة من الوصول إلى البيانات (الشخصية لأكثر من ١٤٣ مليون أمريكي)، استغل المهاجمون ثغرة أمنية غير مُعالجة في موقع الشركة للدخول إلى شبكتها، ثم تحركوا بشكل جانبي داخل الأنظمة للوصول إلى خوادم أخرى، حيث حصلوا على معلومات حساسة مثل أرقام الضمان الاجتماعي، وأرقام رخص القيادة، وأرقام بطاقات الائتمان (Matthew Kosinski، ٢٠٢٦).

استخدمت عدة حكومات برنامج التجسس لمراقبة المواطنين، حيث يعمل هذا البرنامج بشكل خفي على أجهزة الضحايا، فيقوم بتسجيل ضغطات لوحة المفاتيح، واعتراض المكالمات، وجمع مختلف أنواع البيانات الشخصية. وهذا الانتشار الواسع لمثل هذا الاستخدام يشكّل تهديدًا مباشرًا لخصوصية الأفراد، ويُضعف ركائز المؤسسات الديمقراطية وسيادة القانون، كما يخلق مناخًا يسوده الخوف وانعدام الثقة، يدفع الأفراد إلى فرض رقابة ذاتية على سلوكهم أو العزوف عن ممارسة أنشطة مشروعة خشية تعقّب تحرّكاتهم، ولا يقتصر أثر الجرائم الإلكترونية على الخسائر

المادية فحسب، بل يمتد ليطال الحريات المدنية ويُحدث خللًا في البنية المجتمعية (ميتيهان دورماز، ٢٠٢٤).

شهدت قوانين الجرائم الإلكترونية حول العالم توسعًا ملحوظًا، إذ اتسمت بعض هذه القوانين بقدر كبير من الغموض والاتساع، مما أدى إلى تقويض حقوق الإنسان. وغالبًا ما تُستخدم هذه التشريعات من قبل الحكومات لملاحقة فئات متعددة، مثل الصحفيين، والمدافعين عن حقوق الإنسان، وخبراء التكنولوجيا، والمعارضين السياسيين، والمحامين، والمصلحين الدينيين، والفنانين. كما تتعامل بعض الحكومات، بما في ذلك تلك التي تدعم إقرار معاهدة دولية، مع أشكال من حرية التعبير—كالنقد والمعارضة—بوصفها جرائم. وبذلك، فإن أي معاهدة للجرائم الإلكترونية تتبنى هذا النهج ستكون متعارضة مع التزامات حقوق الإنسان (Brown Deborah، ٢٠٢١).

يتبين مما سبق تصاعد أزمة حقوق الإنسان المرتبطة بالانتشار العالمي لأدوات الاختراق السيبراني، مثل برنامج Pegasus* وغيرها من برامج التجسس، التي تستخدم في المراقبة السرية للأجهزة الرقمية. ورغم أن هذه الأدوات تُبرَّر أحيانًا بمكافحة الإرهاب والجريمة، إلا أنها تُستغل في كثير من الحالات لأغراض غير مشروعة، مثل التجسس على الصحفيين والنشطاء والمعارضين السياسيين والمدافعين عن حقوق الإنسان، مما يشكل تهديدًا خطيرًا لحرية التعبير والخصوصية.

عليه يجب احترام هذه حقوق الإنسان، بما في ذلك حرية التعبير والخصوصية والوصول إلى المعلومات، وحمايتها وإعمالها في الفضاء السيبراني، إلا أن طبيعة هذه الحقوق في الفضاء السيبراني متشابكة، وتتطلب تكييف مبادئ وقوانين حقوق الإنسان التقليدية مع التحديات الجديدة التي تقدمها التقنيات الرقمية في الفضاء السيبراني، لضمان حماية حقوق الإنسان في العصر الرقمي المتسارع.

* هو نوع من برمجيات التجسس المتقدمة التي طورتها شركة NSO Group. يستخدم لاختراق الهواتف الذكية (مثل أجهزة أندرويد وآيفون) بشكل سري، وغالبًا دون علم المستخدم يمكنه قراءة الرسائل واتساب، SMS، وغيرها وتسجيل المكالمات وتشغيل الكاميرا والميكروفون دون علمك تتبع موقعك والوصول إلى الصور والملفات.

المبحث الثاني

الأبعاد القانونية والتنظيمية للأمن السيبراني

المطلب الأول: الإطار القانوني والتنظيمي للأمن السيبراني

الفرع الأول: الإطار التشريعي للأمن السيبراني على المستوى الدولي

تعد اتفاقية بودابست لعام ٢٠٠١ من أبرز الاتفاقيات الدولية في مجال الجرائم الإلكترونية، حيث تهدف إلى تعزيز التعاون القضائي بين الدول، وقد انضمت إليها أكثر من ٦٥ دولة، رغم عدم شمولها لجميع أنواع الهجمات السيبرانية. اتفاقية بودابست بشأن الجرائم الإلكترونية هي معاهدة دولية تهدف إلى توحيد التشريعات وتعزيز التعاون الدولي لمكافحة الجرائم الإلكترونية. تركّز على تجريم الأفعال المرتبطة بالحاسوب والإنترنت، وتوفير إطار قانوني لملاحقة مرتكبيها، كما تسعى إلى دعم التحقيقات من خلال أدوات إجرائية فعالة لجمع الأدلة الرقمية وفق سيادة القانون، وتعزز التعاون بين الجهات الأمنية والقضائية على المستوى الدولي، تؤكد النصوص الدولية على ضرورة تحقيق التوازن بين متطلبات إنفاذ القانون واحترام حقوق الإنسان الأساسية، كحرية الرأي والتعبير وتبادل المعلومات دون قيود، إضافة إلى حماية الخصوصية، كما تشدد على أهمية حماية البيانات الشخصية وفق الاتفاقيات الدولية ذات الصلة، وتأخذ بعين الاعتبار حماية حقوق الطفل ضمن الأطر الدولية المعتمدة (Convention on Cybercrime Budapest، ٢٠٠١).

تم اعتماد البرنامج العالمي لمكافحة الإرهاب في مجال الأمن السيبراني والتقنيات الجديدة "برنامج الأمم المتحدة الأمن السيبراني والتكنولوجيا الجديدة" (UNOCT) في عام ٢٠٢٠، الذي يعمل على بناء قدرات الدول الأعضاء والمنظمات الدولية والإقليمية من أجل تطوير وتنفيذ استجابات فعالة للتحديات والفرص التي توفرها شبكة الإنترنت وتقنيات المعلومات والاتصالات الأخرى في مكافحة الإرهاب (مكتب مكافحة الارهاب UNCCT، ٢٠٢٣). ويعمل برنامج الأمن السيبراني والتكنولوجيا الجديدة على تنفيذ أنشطته بالتعاون مع شركاء مثل معهد الأمم المتحدة الإقليمي لبحوث الجريمة والعدالة (UNICRI) [*]، والمنظمة الدولية للشرطة الجنائية (الإنتربول)، والمديرية التنفيذية لمكافحة الإرهاب(CTED) ، وإدارة منظمة السلام(DPO) ، وإدارة الشؤون

[*] UNICRI : يقدم معهد الأمم المتحدة الإقليمي لبحوث الجريمة والعدالة حلولاً مبتكرة قائمة على الأدلة لمواجهة التهديدات الناشئة، وتعزيز العدالة والأمن، وتعزيز حقوق الإنسان في جميع أنحاء العالم.

السياسية وحفظ السلام (DPPA) ، ومكتب تكنولوجيا المعلومات والاتصالات (OICT) [*]، ومكتب الأمم المتحدة المعني بالمخدرات والجريمة (UNODC) ، والاتحاد الدولي للاتصالات (ITU). وع هذه الشراكات فإن هذا البرنامج يدعم حقوق الإنسان من خلال العمل على حماية البنية التحتية الرقمية وضمان الوصول العادل إلى التكنولوجيا، مع التركيز على منع إساءة استخدام التكنولوجيا لأغراض غير مشروعة مثل الإرهاب والجرائم الإلكترونية وحماية البنية التحتية الحيوية للدول (الامم المتحدة، مكتب مكافحة الارهاب، ٢٠٢٤).

اعتمدت الجمعية العامة للأمم المتحدة اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية ، في ٢٤ ديسمبر ٢٠٢٤، وهي اتفاقية دولية تاريخية تهدف إلى تعزيز التعاون في مكافحة الجريمة الإلكترونية وحماية المجتمع من التهديدات الرقمية، من خلال ثلاثة أهداف رئيسية، وهي: تحسين طرق منع الجرائم الإلكترونية ومواجهتها، وتعزيز التعاون الدولي لمكافحة الجرائم الإلكترونية، وتوفير المساعدة الفنية وبناء القدرات لا سيّما للبلدان النامية، والتي سيتم فتح باب التوقيع على هذه الاتفاقية امام الدول في فيتنام عام ٢٠٢٥ وستدخل حيز التنفيذ بعد ٩٠ يوم من التصديق عليها للدول الأعضاء في الامم المتحدة بواقع أربعين دولة، وفق المادة ٦٤ للاتفاقية، وقرار الجمعية العامة للأمم المتحدة. (Nations United، 2024).

الفرع الثاني : الإطار التشريعي للأمن السيبراني على المستوى الاقليمي

تم إنشاء الوكالة الأوربية للأمن السيبراني عام ٢٠٠٤ بهدف تعزيز قدرات دول الاتحاد الأوروبي والقطاع الخاص على منع وكشف والاستجابة للتهديدات السيبرانية. وتعمل على إعداد استراتيجيات وخطط تنفيذية لتحسين حماية الشبكات والمعلومات الحيوية، من خلال تعزيز التعاون بين الدول الأعضاء، ونشر الوعي والتدريب، وتطوير المعايير الأوروبية، وتقديم المشورة الفنية، وتتمثل أبرز أهدافها في: رفع الوعي والثقافة الأمنية، تطوير القدرات السيبرانية، تعزيز التعاون والتنسيق، دعم مواجهة الحوادث والتهديدات، تطوير المعايير والأدوات الأمنية، الاستجابة للتهديدات الناشئة، تحسين أمن القطاعات الحيوية، دعم المستخدمين، وتشجيع البحث والتطوير في مجال الأمن السيبراني.

كذلك أنشأت الأمم المتحدة مجموعة خبراء حكوميين (GGE) لدراسة تهديدات الأمن السيبراني والتوصل إلى توصيات لتعزيز الأمن والاستقرار في هذا المجال.

[*] OICT : مكتب تكنولوجيا المعلومات والاتصالات يسعى لضمان حصول زملائه في جميع أنحاء العالم على أدوات تكنولوجيا المعلومات والاتصالات اللازمة للنجاح في مهامهم، من خلال الأهداف الاستراتيجية الرئيسية الثلاثة: تسريع الابتكار، بناء مرونة الأمن السيبراني، تمكين التحول الرقمي.

اتفاقية الاتحاد الأفريقي لعام ٢٠١٤ تهدف إلى معالجة قضايا الأمن السيبراني والتجارة الإلكترونية وحماية البيانات في القارة، مع تمكين الدول من سنّ تشريعات وطنية لمكافحة الجرائم الإلكترونية والإرهابية، وأكدت على حماية البيانات بإلزام إبلاغ الأفراد قبل مشاركة معلوماتهم مع أطراف ثالثة، كما شددت على ربط الأمن السيبراني بحقوق الإنسان، مثل حرية التعبير والخصوصية وضمان المحاكمة العادلة (AFRICAN UNION CONVENTION ON CYBER SECURITY، ٢٠١٤).

الاتفاقية العربية لمكافحة جرائم تقنية المعلومات هي اتفاقية إقليمية تهدف إلى تعزيز التعاون بين الدول العربية في مجال مكافحة الجرائم المعلوماتية وحماية مصالحها ومجتمعاتها. وقد تم إبرامها في القاهرة بتاريخ ٢١ ديسمبر ٢٠١٠، وتتضمن مواد تتعلق بتجريم الأفعال المجرمة المتعلقة بتقنية المعلومات، والتدابير اللازمة لحماية البيانات والتصدي للجرائم، إذ تتكون من (٤٣) مادة مقسمة إلى أربعة فصول فضلاً عن الفصل الخامس الذي حدّد الأحكام الختامية للاتفاقية. حددت نطاق تطبيقها في منع هذه الجرائم والتحقيق فيها وملاحقة مرتكبيها، مع التأكيد على احترام سيادة الدول وعدم التدخل في شؤونها الداخلية، كما تناولت تجريم عدة أفعال مثل الدخول غير المشروع، الاعتراض على البيانات، الاعتداء على سلامتها، وإساءة استخدام تقنية المعلومات، وشملت أيضًا جرائم التزوير والاحتيال والمواد الإباحية، خاصة المتعلقة بالأطفال، إضافة إلى حماية الخصوصية، وأكدت على الالتزام بحقوق الإنسان ومراعاة الأنظمة الوطنية والمعاهدات الدولية ذات الصلة (الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، ٢٠١٠).

تركّز السياسات في الفضاء الإلكتروني بشكل رئيسي على قضايا الأمن السيبراني ومكافحة الجرائم الإلكترونية ضمن إطار الدول القومية وأمنها. وفي المقابل، ينبغي أن تحظى حقوق الإنسان باهتمام واسع من قبل صُنّاع القرار، نظراً لأن التهديدات السيبرانية التي تستهدف الدول أو بنيتها التحتية الحيوية قد تترك آثاراً مباشرة أو غير مباشرة على هذه الحقوق.

المطلب الثاني : التجارب الوطنية في مجال الأمن السيبراني

الفرع الأول: جهود المملكة العربية السعودية في مجال الامن السيبراني

أولاً: الإطار التنظيمي للأمن السيبراني للمملكة العربية السعودية

تعد المملكة العربية السعودية من أوائل الدول العربية التي سنت تشريعًا للأمن السيبراني، إذ أصدرت عام ٢٠٠٧ نظام مكافحة جرائم المعلوماتية، والذي ركز على مواجهة الاختراقات والاحتيال الإلكتروني وحماية الخصوصية، مما وفر أساسا قانونيًا مبكرا لتنظيم الفضاء الرقمي (رنا مصباح عبد المحسن، ٢٠٢٣). تلتها الأردن في عام ٢٠١٠ بإقرار قانون الجرائم

الإلكترونية، الذي تناول إساءة استخدام الإنترنت وفرض عقوبات على الجرائم الرقمية، مع إدخال تعديلات لاحقة لمواكبة التطورات (قانون الجرائم الالكترونية المعدل، ٢٠١٠). ثم جاءت الإمارات العربية المتحدة في عام ٢٠١٢ بإصدار قانون مكافحة جرائم تقنية المعلومات، والذي عُدّ من أكثر التشريعات تطورًا آنذاك، إذ شمل طيفًا واسعًا من الجرائم مثل الاختراق والابتزاز الإلكتروني ونشر الشائعات، مع تحديثات مستمرة لمواكبة التقدم التقني السريع (قانون مكافحة جرائم تقنية المعلومات المعدل، ٢٠١٢).

تجسد جهود المملكة العربية السعودية في الامن السيبراني نموذجا متقدما في بناء بيئة سيبرانية آمنة ومتكاملة، حيث حرصت على تطوير منظومة تشريعية قوية تواكب التوسع الكبير في استخدام التقنيات الحديثة عبر مختلف القطاعات. ولأهمية حماية البيانات والأصول الرقمية، جعلت المملكة من الأمن السيبراني أولوية استراتيجية لضمان استمرارية الأعمال، وصون حقوق الأفراد والمؤسسات، وتعزيز استقرار الاقتصاد الوطني. تم تأسيس الهيئة الوطنية للأمن السيبراني لتكون الجهة المرجعية المختصة بالأمن السيبراني، حيث تضطلع بمهام تنظيمية وتشغيلية ورقابية تهدف إلى تعزيز مستوى الجاهزية السيبرانية لدى مختلف الجهات الوطنية (الهيئة الوطنية للأمن السيبراني، ٢٠١٩). وقد أصدرت الهيئة ما يُعرف بـ "الضوابط الأساسية للأمن السيبراني ٢٠١٨ (ECC) ، و تهدف هذه الضوابط إلى تحديد الحد الأدنى من متطلبات الأمن السيبراني، وفق أفضل الممارسات والمعايير، للحد من المخاطر التي قد تهدد الأصول المعلوماتية والتقنية من مصادر داخلية وخارجية. وتركّز الحماية على ثلاثة أهداف رئيسية: (سرية المعلومات، سلامتها، وتوافرها). كما تستند هذه الضوابط إلى أربعة محاور أساسية للأمن السيبراني: الاستراتيجية، الأشخاص، الإجراءات، والتقنية.

ثانياً: الإطار التشريعي للأمن السيبراني للمملكة العربية السعودية

أما ضوابط الأمن السيبراني للأنظمة الحساسة، ٢٠١٩ (CSCC)، وهي مجموعة من المتطلبات الإلزامية التي يجب على الجهات الحكومية، وكذلك الجهات المشغلة للبنى التحتية الحيوية في القطاع الخاص، الالتزام بها. وتهدف هذه الضوابط إلى الحد من المخاطر السيبرانية وحماية الأصول المعلوماتية والتقنية. وتشمل هذه الضوابط عدة مجالات رئيسية، من أبرزها (ضوابط الأمن السيبراني للأنظمة الحساسة، ٢٠١٩):

١-حوكمة الأمن السيبراني: عبر تحديد الأدوار والمسؤوليات، ووضع السياسات والإجراءات المنظمة.

٢-إدارة المخاطر السيبرانية: من خلال تقييم المخاطر بشكل دوري واتخاذ التدابير المناسبة لمعالجتها.

٣-حماية الأنظمة والبيانات: بتطبيق أفضل الممارسات التقنية لحماية الشبكات والأجهزة والبيانات.

٤-إدارة الحوادث السيبرانية: عبر إعداد خطط فعالة للاستجابة للحوادث والتعافي منها.

يعد نظام حماية البيانات الشخصية (PDPL) خطوة مهمة ضمن المنظومة التشريعية للأمن السيبراني في المملكة العربية السعودية، حيث يهدف إلى وضع إطار قانوني شامل يصون خصوصية بيانات الأفراد، حيث يلزم هذا النظام جميع الجهات في القطاعين العام والخاص التي تتولى جمع أو معالجة البيانات الشخصية بالحصول على موافقة صريحة من أصحاب البيانات قبل البدء في استخدامها، ويمنح الأفراد مجموعة من الحقوق، مثل حق الوصول إلى بياناتهم وتصحيحها أو طلب حذفها عند الحاجة، الأمر الذي يعزز النظام مكانة المملكة ويجعلها في مقدمة الدول التي تولي اهتماماً كبيراً بحماية الخصوصية والبيانات الشخصية. وتتكوّن المنظومة من لائحتين مترابطتين: الأولى هي اللوائح التنفيذية لقانون حماية البيانات الشخصية، والثانية هي لوائح نقل البيانات الشخصية خارج المملكة ومن أهمها (ضوابط الأمن السيبراني للبيانات، ٢٠٢٢):

١-حماية الخصوصية والبيانات: تقييد الوصول للمعلومات الحساسة باستخدام مبدأ الحد الأدنى من الصلاحيات والتشفير، مما يمنع التسريب أو الاستخدام غير المشروع.

٢-المشروعية وتقييد المراقبة: اشتراط وجود سياسات واضحة وموافقات رسمية لعمليات المراقبة، مع توثيقها، للحد من التعسف وضمان الالتزام بالقانون.

٣-المساءلة والشفافية: تحديد المسؤوليات وإلزام الجهات بالتدقيق والمراجعة، مما يتيح تتبع الانتهاكات ومحاسبة المسؤولين.

٤-سلامة البيانات ودقتها: حماية تكامل البيانات من التلاعب أو الإتلاف، لضمان اتخاذ قرارات صحيحة لا تضر بالأفراد.

٥-استمرارية الخدمات وحمايتها: توفير خطط للتعافي والصمود السيبراني لضمان عدم انقطاع الخدمات الحيوية التي يعتمد عليها الأفراد.

تعنى ضوابط الأمن السيبراني المعتمدة في المملكة العربية السعودية—مثل ضوابط الأنظمة الحساسة(CSCC) ، وضوابط الحوسبة السحابية(CCC) ، وضوابط العمل عن بُعد(TCC) ،

وضوابط حسابات وسائل التواصل الاجتماعي—(OSMACC) بحماية البيانات والأنظمة من التهديدات الرقمية. وتسهم هذه الأطر في دعم الحق في الخصوصية عبر تعزيز التحكم في الوصول وحماية المعلومات. كما تُبرز ضوابط الحوسبة السحابية والعمل عن بُعد اهتمامًا واضحًا بتأمين البيانات أثناء التخزين والنقل والمعالجة، بينما تُولي ضوابط الأنظمة الحساسة أهمية خاصة لحماية البنية التحتية الحيوية والبيانات عالية الأهمية. وفي المقابل، قد يترتب على بعض الضوابط—خصوصًا تلك المرتبطة بوسائل التواصل الاجتماعي—تأثيرات محتملة على حرية التعبير من خلال تنظيم المحتوى الرسمي. كما أن المعايير الوطنية للتشفير (NCS – 1 : 2020) تحدد الحد الأدنى من متطلبات التشفير للأغراض المدنية والتجارية وذلك لحماية البيانات (عند تخزينها أو معالجتها أو نقلها) والأنظمة والشبكات الوطنية، وبشكل عام، تعكس هذه الضوابط توجهًا يسعى إلى تحقيق توازن بين متطلبات الأمن وحماية الحقوق، مع تركيز أكبر على تعزيز الخصوصية والأمن (Othman Al-Salloum and Azizah A. Al-Zahrani, 2025).

وعليه تسهم هذه الضوابط في حماية حقوق الإنسان من خلال تحقيق توازن بين الأمن السيبراني والحقوق الفردية، إذ تضمن الخصوصية، وتمنع التعسف في استخدام السلطة الرقمية، وتعزز الشفافية والمساءلة، وتحافظ على استمرارية الخدمات الأساسية وسلامة البيانات.

المطلب الثاني: جهود العراق في مجال الأمن السيبراني:

أولاً: الإطار التنظيمي للأمن السيبراني في العراق

نتيجة لتزايد التهديدات الرقمية واعتماد الدولة على الأنظمة الإلكترونية، أطلق العراق استراتيجية الأمن السيبراني (٢٠١٧) كأول إطار رسمي لتنظيم هذا القطاع وتحديد نقاط الضعف ووضع حلول لها، وتعد المخاطر السيبرانية من أبرز التحديات التي تؤثر بشكل مباشر على الأمن القومي للدولة، نظراً لاعتماد الدول المتزايد على البنية التحتية الرقمية في مختلف القطاعات. وبما أن الفضاء السيبراني قائم على الترابط بين الدول والشبكات العالمية، فإن أي دولة، ومنها العراق، تبقى عرضة لتهديدات متوقعة وغير متوقعة، وتتفاقم هذه المخاطر مع وجود جهات فاعلة ذات نوايا خبيثة تستغل الثغرات التقنية لاستهداف الأنظمة الوطنية، مما يؤدي إلى المساس بسرية المعلومات وسلامتها وتوافرها. ولا يقتصر تأثير هذه التهديدات على الجانب التقني فقط، بل يمتد ليشمل المواطن بشكل مباشر، وينعكس سلباً على الاستقرار والأمن الوطني. كما تمثل الهجمات السيبرانية، مثل الاختراقات، والاحتيال الإلكتروني، والتجسس، والإرهاب الرقمي، والتخريب الاقتصادي، تهديداً حقيقياً للمصالح الاقتصادية للدولة. وتشمل هذه التهديدات

تعطيل الخدمات الإلكترونية، واستهداف المواقع الحكومية، واستغلال وسائل التواصل لنشر حملات مضللة، إضافة إلى الجرائم المالية وغسل الأموال. من هنا تأتي الاستراتيجية الوطنية للأمن السيبراني إلى حماية البنية التحتية الرقمية وتحقيق (السيادة الرقمية) حيث تهدف إلى (استراتيجية الامن السيبراني العراقية، ٢٠١٧):

١-حماية البنية التحتية الحيوية: تعزيز أمن الأنظمة الحكومية والخدمات الأساسية (مثل الكهرباء، الصحة، الاتصالات) من الهجمات السيبرانية.

٢-رفع مستوى الأمن السيبراني الوطني: تطوير قدرات الكشف عن التهديدات والاستجابة للحوادث وتقليل المخاطر الرقمية.

٣-تعزيز الحوكمة والتشريعات: وضع أطر وسياسات تنظيمية تنظم العمل السيبراني وتحدد المسؤوليات وتدعم سيادة القانون.

٤-بناء القدرات والكوادر البشرية: تدريب وتأهيل المختصين ونشر ثقافة الأمن السيبراني في المؤسسات والمجتمع.

٥-تعزيز التعاون الداخلي والدولي: التنسيق بين الجهات الحكومية والشراكات الدولية لمواجهة التهديدات السيبرانية.

وشهد العراق خلال العقد الأخير سلسلة من الإجراءات لتعزيز الأمن السيبراني، شملت تطوير الحوكمة الإلكترونية وتسهيل الخدمات للمواطنين، إضافة إلى حماية الأفراد والمؤسسات من التهديدات السيبرانية. ومن أبرز هذه الإجراءات (المركزالوطني للامن السيبراني، ٢٠٢٢-٢٠٢٧):

١-في عام ٢٠١٢، تم اعتماد الاستراتيجية الوطنية وخطة الحوكمة الإلكترونية، إضافة إلى إطار التشغيل البيني والتصميم المعماري الحكومي.

٢-إطلاق سياسة أمن الاتصالات والمعلومات، التي تناولت المفاهيم الأساسية والتحديات والإجراءات الوطنية ذات الصلة.

٣-في عام ٢٠١٥، تم تشكيل اللجنة العليا لأمن الاتصالات والمعلومات تحت إشراف مجلس الأمن الوطني.

٤-في عام ٢٠١٧، أُسس الفريق الوطني للاستجابة للحوادث السيبرانية (CERT) بهدف تعزيز القدرة على مواجهة الهجمات السيبرانية.

٥-مديرية الأمن السيبراني في وزارة الداخلية تأسست عام ٢٠٢٢ لحماية الأنظمة والبيانات وتعزيز الأمن الوطني وتعمل على منع الاختراقات وإدارة التهديدات وكشف الثغرات ونشر الوعي لضمان بيئة رقمية آمنة وموثوقة.

ثانياً: الإطار التشريعي للأمن السيبراني في العراق

رغم أهمية الموضوع، لا يزال العراق يفتقر إلى قانون شامل ومتكامل للأمن السيبراني، إلا أن هناك بعض القوانين والتشريعات التي تغطي جوانب محددة من الفضاء الإلكتروني، من أبرزها:

١-قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩

يتضمن هذا القانون بعض النصوص التي تُعاقب على الجرائم المرتبطة بالفضاء الرقمي، مثل الاحتيال والابتزاز. إلا أنه لا يغطي الجرائم السيبرانية الحديثة، كاختراق الأنظمة وسرقة البيانات أو الهجمات على البنى التحتية الرقمية (قانون العقوبات العراقي، ١٩٦٩).

٢-قانون مكافحة الإرهاب رقم ١٣ لسنة ٢٠٠٥

يُستخدم أحيانًا لملاحقة الجرائم الإلكترونية التي تمس الأمن القومي، مثل نشر محتوى تحريضي أو التجنيد الإلكتروني لصالح الجماعات الإرهابية، لكنه ليس موجّهًا بشكل خاص إلى قضايا الأمن السيبراني (قانون مكافحة الارهاب، ٢٠٠٥).

٣-مشروع قانون الجرائم المعلوماتية

ناقش البرلمان العراقي هذا المشروع عدة مرات، لكنه لم يُقر حتى الآن بسبب الجدل الواسع حوله، لا سيما فيما يخص تقييد حرية التعبير والرقابة على الإنترنت، ويهدف المشروع إلى مكافحة الجرائم الإلكترونية، إلا أن بعض مواده أثارت مخاوف من احتمال استخدامها لتقييد الحريات الرقمية بشكل مفرط (مشروع قانون مكافحة الجرائم الالكترونية، ٢٠١٩).

٤-قوانين تنظيم الاتصالات والمعلوماتية

تتولى هيئة الإعلام والاتصالات الإشراف على الفضاء الإلكتروني في العراق، حيث تنظم عمل مزودي خدمات الإنترنت وتفرض رقابة على المحتوى الرقمي، خاصة عندما يتعلق الأمر بالأمن القومي أو المعلومات الحساسة (قانون الاتصال والمعلوماتية، ٢٠٠٩).

على الرغم من تزايد الاهتمام بالأمن السيبراني، إلا أن العراق لا يزال يفتقر إلى إطار قانوني شامل ومتكامل ينظم هذا المجال بشكل واضح. وتعتمد الدولة حالياً على مجموعة من القوانين المتفرقة، مثل مشاريع قوانين مكافحة الجرائم المعلوماتية، وقوانين مكافحة الإرهاب التي تمتد لتشمل بعض أشكال الجرائم الإلكترونية، فضلاً عن تشريعات تتعلق بحماية البيانات

والاتصالات. هذا التشتت التشريعي يخلق فجوة قانونية واضحة، إذ لا توجد منظومة موحدة قادرة على مواكبة التطور السريع في التقنيات الرقمية. كما أن بطء تحديث القوانين مقارنة بالتقدم التكنولوجي يزيد من تعقيد المشهد، ويحد من فعالية الاستجابة للتهديدات السيبرانية. وفي ظل هذا الواقع، يبرز تحدٍ كبير يواجه المواطن العراقي، حيث يصبح أكثر عرضة لمخاطر مثل الاختراقات، والابتزاز الإلكتروني، وسرقة البيانات، دون وجود حماية قانونية رادعة وواضحة. لذلك، تبرز الحاجة الملحة إلى سنّ تشريعات حديثة وشاملة توفر حماية حقيقية للأفراد وتعزز الثقة في البيئة الرقمية.

يتضح أن كلًا من العراق والمملكة العربية السعودية يوليان اهتماماً متزايداً بقضايا الأمن السيبراني وحقوق الإنسان، غير أن نهج كل منهما يختلف إلى حد ما، ففي العراق، لا يوجد حتى الآن قانون موحد وشامل للأمن السيبراني في العراق مما يؤدي إلى غموض وتفاوت في تطبيق الحقوق، وأحياناً تعارض بين الأمن وحرية التعبير، مع محاولة تحقيق توازن بين متطلبات الأمن وصون الحقوق والحريات. أما في المملكة العربية السعودية، فيبرز تقدم مؤسسي أكثر وضوحًا، من خلال تبني استراتيجيات وطنية متكاملة للأمن السيبراني، وإنشاء هيئات متخصصة، إلى جانب تنظيم الفضاء الرقمي وفق سياسات أكثر شمولاً.

فضلاً عن ذلك، يمكن القول إن المملكة العربية السعودية تتفوق من حيث البنية التنظيمية والاستراتيجية في مجال الأمن السيبراني، في حين يركز العراق على إرساء دعائم هذا المجال وتطوير منظومته التشريعية، مع اتفاق البلدين على هدف مشترك يتمثل في تحقيق التوازن بين حماية الأمن الرقمي واحترام حقوق الإنسان في البيئة السيبرانية.

الخاتمة:

أصبح الأمن السيبراني وتكنولوجيا الحديثة ركيزة أساسية لعمل الحكومات والشركات على مستوى العالم، الأمر الذي جعل الأمن السيبراني في مقدمة الأولويات، إذ يساهم في الحد من التهديدات السيبرانية، وحماية البيانات الحساسة، وضمان سلامة البنى التحتية الحيوية والأنظمة الحكومية من الهجمات التي قد تهدد الأمن القومي والاستقرار المجتمعي، مع الالتزام بسيادة القانون وصون حقوق الإنسان وحرية التعبير.

ومع تصاعد التهديدات وتطورها، لم يعد من الممكن ضمان حماية كاملة، مما يستدعي من مختلف الجهات العمل على تقليل المخاطر والاستعداد المسبق عبر تعزيز إجراءات الحماية وتطوير قدرات الكشف المبكر، كما تبرز الحاجة إلى أطر قانونية وتنظيمية فعّالة تكرس حقوق الإنسان وتدعم التعاون وتبادل المعلومات بين القطاعين العام والخاص، وفي هذا الإطار،

ينبغي تحقيق توازن بين متطلبات الأمن السيبراني واحترام الحق في الخصوصية والحق في حرية التعبير، والتي تمثل امتدادًا لحقوق الإنسان الاساسية وتحظى باعتراف متزايد على الصعيد الدولي.

النتائج:

-الأمن السيبراني: هو ممارسة حماية أجهزة الكمبيوتر والشبكات والبرامج والبيانات من الوصول غير المصرح به أو إساءة الاستخدام أو الهجمات الإلكترونية. في عصرنا الرقمي، حيث تعتمد حياتنا وأنظمتنا الحيوية بشكل كبير على التكنولوجيا، أصبح الأمن السيبراني خط دفاع أساسي.

-الفضاء السيبراني يطرح تحديات جديدة تتعلق بالخصوصية وحرية التعبير والأمن السيبراني، مما يتطلب تكييف آليات حماية حقوق الإنسان لتلبية هذه التحديات.

-تبين إن تحقيق التوازن بين تعزيز الأمن السيبراني وحماية الحق في الخصوصية يُعد تحديًا جوهريًا، يتطلب أطرًا قانونية وتنظيمية تضمن الاستخدام المسؤول للتكنولوجيا، وتحافظ في الوقت ذاته على حقوق الإنسان وحرياته الأساسية.

-تُعد تدابير الأمن السيبراني الفعالة أمرًا بالغ الأهمية، بدءًا من حماية المعلومات الشخصية كأرقام بطاقات الائتمان وكلمات المرور، وصولًا إلى تأمين قواعد البيانات الحكومية والأسرار التجارية للشركات. يبحث المخربون، كالمخترقين ومجرمي الإنترنت وحتى الدول، باستمرار عن ثغرات أمنية لاستغلالها لتحقيق مكاسب مالية أو لأغراض خبيثة أخرى.

-تساعد التشريعات القانونية بروتوكولات والسياسات وأدوات الأمن السيبراني الفعّالة على منع اختراق البيانات، وسرقة الهوية، وأعطال الأنظمة، وغيرها من العواقب الوخيمة للهجمات السيبرانية الناجحة. ومع التطور السريع للتكنولوجيا، تتطور التهديدات السيبرانية التي نواجهها، مما يجعل الأمن السيبراني ممارسةً حيويةً ومتطورةً باستمرار لحماية حياتنا وأصولنا الرقمية.

التوصيات :

١-يجب أن يتمحور الأمن السيبراني حول حماية حقوق الإنسان، وليس تقييدها أو انتهاكها.

٢-يجب على الدول والجهات الفاعلة الأخرى في الفضاء السيبراني، مثل الشركات والمؤسسات الخاصة، تحمل مسؤولية احترام حقوق الإنسان.

٣-الحاجة إلى تحقيق توازن بين الأمن الوطني وحماية الحقوق الفردية، لاسيما الخصوصية وحرية التعبير، بما يضمن عدم المساس بها عند تعزيز الأمن، وهذا ما يتطلب إعادة صياغة التشريعات الحالية لتواكب هذا التوازن بشكل واضح وفعال.

٤- التأكيد على الجهات الحكومية المختصة، تضمين حقوق الإنسان المكرسة في الدستور العراقي لعام ٢٠٢٥ عند وضع السياسات والاستراتيجيات وآليات الحوكمة والمعايير والإرشادات المنظمة للأمن السيبراني.

٥-العمل على تطوير وتحديث الأطر التنظيمية للأمن السيبراني بشكل متواصل، وتعميمها على الجهات الحكومية وغير الحكومية لضمان توحيد الممارسات لضمان حماية حقوق الانسان وامن المجتمع وتنظيم الإبلاغ عن الحوادث السيبرانية المتعلقة بحقوق الإنسان.

٦-التأكيد على أن الدور الجهات المختصة لا يعفي أي جهة، سواء كانت عامة أو خاصة أو غيرها، من مسؤولياتها في مجال الأمن السيبراني، مع ضرورة تحديد الأدوار والمسؤوليات المتبادلة، بما يضمن التكامل والتنسيق الفعّال بين جميع الأطراف، بما يضمن عدم انتهاك حقوق الإنسان الأساسية.

٧-بناء قدرات فنية ومؤسسية وقانونية لتعزيز الأمن الرقمي على المستوى الحكومي والمجتمعي.

المصادر العربية والاجنبية:

أولاً: الصادر العربية:

١-أحمد بن علي الفيومي .المصباح المنير في غريب الشرح الكبير .بيروت، لبنان: المكتبة العلمية، بدون تاريخ.

٢-أديب ميالة، ومي محرزي. "السرية المصرفية في التشريع السوري ."مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد ٢٧، العدد ١، ٢٠١١، ص ١٢.

٣-مستشارية الأمن القومي العراقية .استراتيجية الأمن السيبراني العراقية .بغداد، العراق، ٢٠١٧. متاح على الموقع الإلكتروني . https://www.itu.int/en/ITU-D/Cybersecurity/ :تاريخ الزيارة: ٢٠٢٥/٠٤/٢١.

٤-جامعة الدول العربية، الأمانة العامة، إدارة الشؤون القانونية .الاتفاقية العربية لمكافحة جرائم تقنية المعلومات . 21/12/2010متاح على الموقع الإلكتروني . http://www.arablegalnet.org :تاريخ الزيارة: ٢٠٢٥/٠٥/١١.

٥-الأمم المتحدة .الإعلان العالمي لحقوق الإنسان، المادة (١٢): الحق في الخصوصية.1948 .

٦-الأمم المتحدة، الجمعية العامة .حرية التعبير عن الرأي عبر الإنترنت .2016 .متاح على الموقع الإلكتروني . https://digitallibrary.un.org/record/845728?ln=en :تاريخ الزيارة: ٢٠٢٥.

٧-الأمم المتحدة، مجلس حقوق الإنسان .تقرير مفوضية الأمم المتحدة السامية لحقوق الإنسان .2022 .متاح على الموقع الإلكتروني . https://docs.un.org/ar/A/HRC/51/17 :تاريخ الزيارة: ٢٠٢٥/٠٦/٢٣.

٨-الأمم المتحدة، مكتب مكافحة الإرهاب .برنامج الأمن السيبراني التابع لمركز الأمم المتحدة لمكافحة الإرهاب . 2024متاح على الموقع الإلكتروني: https://www.un.org/counterterrorism/cct/programme-projects/cybersecurity . تاريخ الزيارة: ٢٠٢٥/٠٤/١٩.

٩-الأمم المتحدة، مكتب المفوض السامي لحقوق الإنسان .الشرعة الدولية لحقوق الإنسان .2025 .متاح على الموقع الإلكتروني: https://www.ohchr.org/ar/what-are-human-rights/international-bill-human-rights . تاريخ الزيارة: ٢٠٢٥/٠٤/٢٥.

١٠-الأمم المتحدة، مكتب المفوض السامي لحقوق الإنسان .الخصوصية في العصر الرقمي والفضاء الرقمي وحقوق الإنسان .2025 .متاح على الموقع الإلكتروني . https://www.ohchr.org/ar تاريخ الزيارة: ٢٠٢٥/٠٦/١١.

١١-الأمم المتحدة، مجلس حقوق الإنسان .الحق في الخصوصية في العصر الرقمي، الوثيقة A/HRC/60/45. 2025 .متاح على الموقع الإلكتروني . https://docs.un.org/ar/A/HRC/60/45 : تاريخ الزيارة: ٢٠٢٥/١١/٢٥.

١٢-الأمم المتحدة، الجمعية العامة .العهد الدولي الخاص بالحقوق المدنية والسياسية: الحق في حرية الرأي والتعبير .1966 .

١٣-اللجنة الدولية للصليب الأحمر .القانون الدولي الإنساني .03/12/2014 .متاح على الموقع الإلكتروني : https://www.icrc.org . تاريخ الزيارة: ٢٠٢٥/٠٤/٢٩.

١٤-اللجنة الدولية للصليب الأحمر .حماية المدنيين وغيرهم من الأشخاص والأعيان المحميين من التكلفة البشرية المحتملة لأنشطة تكنولوجيا المعلومات والاتصالات خلال النزاعات المسلحة .المؤتمر الدولي الرابع والثلاثون للصليب الأحمر والهلال الأحمر، جنيف، ٢٠٢٤.

١٥-المركز الوطني للأمن السيبراني العراقي .استراتيجية الأمن السيبراني العراقي ٢٠٢٢-٢٠٢٧ .متاح على الموقع الإلكتروني . https://ncc.gov.iq :تاريخ الزيارة: ٢٠٢٦/٠٣/١٨.

١٦-الهيئة الوطنية للأمن السيبراني. "صدور أمر ملكي بإنشاء الهيئة الوطنية للأمن السيبراني ."وكالة الأنباء السعودية(SPA) ، 19/01/2019. متاح على الموقع الإلكتروني . https://www.spa.gov.sa :تاريخ الزيارة: ٢٠٢٦/٠٣/١٢.

١٧-باسم علي خريسان. "الهاكتفيزم: دراسة في العلاقة بين الشبكات الحاسوبية والسياسة ".مركز البيان للدراسات والتخطيط، 18/04/2022. متاح على الموقع الإلكتروني. https://www.bayancenter.org :

١٨-باسم محمد فاضل .الحق في الخصوصية بين الإطلاق والتقييد .الإسكندرية: دار الجامعة الجديدة، ٢٠١٨.

١٩-حسنين علاء محمد. "الإطار القانوني لحماية البيانات الشخصية في شبكات الاتصالات الحديثة ."جامعة المستقبل، 17/11/2025. متاح على الموقع الإلكتروني . https://uomus.edu.iq :تاريخ الزيارة: ٢٠٢٥/١٢/٢٥.

٢٠-حسين سليمان راشد الطيار. "الأمن السيبراني في منظور مقاصد الشريعة ."مجلة جامعة الطائف للعلوم الإنسانية، العدد ٢١، ٢٠٢٠، ص ٢٦٤.

٢١-ذياب موسى البداينة. "الجرائم الإلكترونية: المفهوم والأساليب". في :الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية .عمان، الأردن: كلية العلوم الاستراتيجية، ٢٠١٤، ص ٢-٤.

٢٢-رنا مصباح عبد المحسن. "آليات مكافحة الجرائم السيبرانية في المملكة العربية السعودية: دراسة تحليلية ". المجلة القانونية للدراسات والبحوث القانونية، المجلد ٥، ٢٠٢٣، ص ١٣٨٧.

٢٣-ستيف مور. "أربعة أنواع من استخبارات التهديد وكيفية استخدامها بفعاليةExabeam ."، .2026متاح على الموقع الإلكتروني . https://www.exabeam.com/ar/explainers :تاريخ الزيارة: ٢٠٢٦/٠٢/١٦.

٢٤-صلاح حيدر عبد الواحد .حروب الفضاء الإلكتروني: دراسة في مفهومها وخصائصها وسبل مواجهتها . رسالة ماجستير، جامعة الشرق الأوسط، عمان، الأردن، ٢٠٢١، ص ٢٢-٢٤.

٢٥-الهيئة الوطنية للأمن السيبراني .ضوابط الأمن السيبراني للأنظمة الحساسة .2019 (ECC). متاح على الموقع الإلكتروني . https://acs.uj.edu.sa :تاريخ الزيارة: ٢٠٢٦/٠٣/١٣.

٢٦-الهيئة الوطنية للأمن السيبراني .ضوابط الأمن السيبراني للبيانات .2022 (DCC). متاح على الموقع الإلكتروني . https://acs.uj.edu.sa :تاريخ الزيارة: ٢٠٢٦/٠٣/١٥.

٢٧-عبدالله يحيى سعيد الزهراني .استراتيجيات الأمن السيبراني في ضوء التقنيات والتحديات الحديثة .رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، المملكة العربية السعودية، ٢٠٢٠.

٢٨-علاء الدين فرحان. "من الردع النووي إلى الردع السيبراني ."مجلة الفكر، العدد ١٦، ٢٠٢١، ص ٢٢٤٦.

٢٩-فريق الاستجابة لحوادث الأمن السيبراني .(CERT) فريق الاستجابة لحوادث الأمن السيبراني العراقي . .2017متاح على الموقع الإلكتروني . https://cert.gov.iq/index.html :تاريخ الزيارة: ٢٠٢٥/٠٤/١٤.

٣٠-هيئة الإعلام والاتصالات .قانون الاتصالات والمعلوماتية .بغداد، العراق، ٢٠٠٩. متاح على الموقع الإلكتروني. https://archive3.parliament.iq/ar/2017/04/27/ :

٣١-هيئة الإعلام والاتصالات .قانون الاتصالات والمعلوماتية .بغداد، العراق، ٢٠٠٩. متاح على الموقع الإلكتروني. https://archive3.parliament.iq/ar/2017/04/27/ :

٣٢-قانون الجرائم الإلكترونية المعدل رقم (٣٠) لسنة ٢٠١٠ .الأردن، ٢٠١٠.

٣٣-قانون العقوبات العراقي رقم (١١١) لسنة ١٩٦٩ .المادة (٢٨٧) الخاصة بالتزوير والاحتيال. بغداد، العراق، ١٩٦٩.

٣٤-قانون تسجيل الولادات والوفيات العراقي رقم (١٤٨) لسنة ١٩٧١ .المادة (١٧). العراق، ١٩٧١.

٣٥-قانون مكافحة الإرهاب رقم (١٣) لسنة ٢٠٠٥ .بغداد، العراق، ٢٠٠٥.

٣٦-قانون مكافحة جرائم تقنية المعلومات المعدل رقم (٥) لسنة ٢٠١٢ .الإمارات العربية المتحدة، ٢٠١٢.

٣٧-قانون نقابة الصحفيين رقم (١٧٨) لسنة ١٩٦٩ المعدل .المادة (٢٥). العراق: الوقائع العراقية، ١٩٦٩.

٣٨-دستور جمهورية العراق لسنة ٢٠٠٥ .المادة (١٧). العراق، ٢٠٠٥.

٣٩-مجلس حقوق الإنسان .قرار تعزيز وحماية والتمتع بحقوق الإنسان على الإنترنت .الأمم المتحدة، ٢٠١٦. تاريخ الزيارة: ٢٠٢٥/٠٣/١٧.

٤٠-محمد بن أبي بكر الرازي .مختار الصحاح .المجلد ٤. بيروت، لبنان: المكتبة العصرية، ١٩٩٨.

٤١-محمد يوسف. "ماذا تعرف عن السيبراني المرتزق: الذراع القذر للشركات والدول؟ ."الجزيرة نت، 15/10/2024.

٤٢-محمود بري .السيبرانية: علم القدرة على التواصل والتحكم والسيطرة .ط١، بيروت، لبنان: المركز الإسلامي للدراسات، ٢٠١٩.

٤٣-مديرية الأمن السيبراني، وزارة الداخلية العراقية .مديرية الأمن السيبراني .04/12/2022 .متاح على الموقع الإلكتروني . https://moi.gov.iq :تاريخ الزيارة: ٢٠٢٥/٠٣/٠٥.

٤٤-جمهورية العراق .مشروع قانون مكافحة الجرائم الإلكترونية .بغداد، العراق، ٢٠١٩. متاح على الموقع الإلكتروني: https://menarights.org/sites/default/files/2022-06/New%20version_CyberCrimeDraftLaw%20%281%29.pdf .

٤٥-مكتب الأمم المتحدة لمكافحة الإرهاب .(UNCCT) أمن الفضاء الإلكتروني .2023 .متاح على الموقع الإلكتروني: https://www.un.org/counterterrorism/ar/cct/programme-projects/cybersecurity .تاريخ الزيارة: ٢٠٢٥/٠٥/٠٨.

٤٦-ميتيهان دورماز . "اتفاقية الأمم المتحدة الجديدة لمكافحة الجرائم الإلكترونية: الأهداف والثغراتSMEX ."، 12/12/2024.متاح على الموقع الإلكتروني . https://smex.org/ar/ :تاريخ الزيارة: ٢٠٢٥/٠٥/١٢.

٤٧-نزيه عبد المقصود، وهشام مصطفى. "الأمن الاقتصادي وأثره في تحقيق المستوى المعيشي الأمثل ."مجلة كلية الشريعة والقانون، 2023، ص ١١٨٩.

٤٨-يوسف بوغرارة. "الأمن السيبراني: الاستراتيجية الجزائرية للأمن والدفاع والفضاء السيبراني ."مجلة الدراسات الأفريقية وحوض النيل – المركز الديمقراطي العربي، المجلد ٣، ٢٠١٨، ص ١٠٦.

المصادر الأجنبية:

1- African Union. African Union Convention on Cyber Security and Personal Data Protection. 27 June 2014. Available at: https://ccdcoe.org/uploads/2018/11/AU-270614-CSConvention.pdf . Accessed on: 19 March 2026.

2- Gregg Lindemulder and Matt Kosinski. What Is Cybersecurity? IBM, 12 August 2024. Available at: https://www.ibm.com/think/topics . Accessed on: 2024.

3- Deborah Brown. Cybercrime is Dangerous, But a New UN Treaty Could Be Worse for Rights. Human Rights Watch, 13 August 2021.

4- Charlie Plumb. Understanding the UN's New International Treaty to Fight Cybercrime. UNU Centre for Policy Research, 30 July 2024. Available at: https://unu.edu/cpr/blog-post/understanding-uns-new-international . Accessed on: 18 February 2026.

5- Convention on Cybercrime (Budapest Convention). European Treaty Series – No. 185. Council of Europe, 23 November 2001. Available at: https://rm.coe.int . Accessed on: 20 March 2026.

6- Cybersecurity and Infrastructure Security Agency (CISA). What Is Cybersecurity?. CISA, 2009. Available at: https://www.cisa.gov/news-events/news/what-cybersecurity . Accessed on: 2 May 2025.

7- Helaine Leggat. A New Look at the Budapest Convention on Cybercrime. ICTLC Australia, 2024. Available at: https://www.ictlc.com/a-new-look-at-the-budapest-convention-on-cybercrime/?lang=en . Accessed on: 14 May 2025.

8- International Telecommunication Union (ITU). Cyber Security. International Telecommunication Union, Geneva, 2008.

9- João Valente Cordeiro and Paula Lobato de Faria. Health Data Privacy and Confidentiality Rights: Crisis or Redemption?. Public Health Journal, 2014, p. 142.

10- John Markoff. Step Taken to End Impasse Over Cybersecurity Talk. The New York Times, 17 July 2010, A7, col. 1.
11- Kali Robinson. How Israel's Pegasus Spyware Stoked the Surveillance Debate. Council on Foreign Relations, 8 March 2022. Available at: https://www.cfr.org/in-brief/how-israels-pegasus-spyware-stoked-surveillance-debate . Accessed on: 10 May 2025.
12- Matthew Kosinski. What Is a Data Breach?. IBM, 2026. Available at: https://www.ibm.com/think/topics/data-breach . Accessed on: 19 February 2026.
13- United Nations. Convention on Cybercrime. 2024. Available at: https://docs.un.org/ar/A/RES/79/243 .
14- Othman Al-Salloum and Azizah A. Al-Zahrani. Success Factors in Achieving Excellence in Cybersecurity. International Journal of Research and Studies Publishing, Vol. 68, 20 June 2025, pp. 72–73.
15- Palatty Nivedita James. 130+ Data Breach Statistics 2026 – The Complete Look. Astra, 6 January 2026. Available at: https://www.getastra.com/blog/security-audit/data-breach-statistics/ . Accessed on: 20 February 2026.
16- Robb Shawe. Cybersecurity and Human Rights: Navigating the Balance Between Security. Journal of Information Technology and Integrity, 2025, Vol. 110, p. 3.
17- Sohair Ahmed Shaikh. Surveillance of Cyber Security and Human Rights. International Journal for Legal Research & Analysis, 7 January 2025, p. 2.
18- Steve Morgan. Top 5 Cybersecurity Facts, Figures, Predictions and Statistics for 2021 to 2025. Cybersecurity Ventures, 5 February 2024. Available at: https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2021-to-2025/ . Accessed on: 10 May 2025.

Arabic and Foreign Sources:

First: Arabic Sources:

1- Ahmad ibn Ali al-Fayumi. Al-Misbah al-Munir fi Gharib al-Sharh al-Kabir. Beirut, Lebanon: Al-Maktabah al-Ilmiyyah, n.d.
2- Adib Mayaleh and Mai Mahrezi. "Banking Secrecy in Syrian Legislation." Damascus University Journal of Economic and Legal Sciences, Vol. 27, No. 1, 2011, p. 12.
3- Iraqi National Security Advisory. Iraqi Cybersecurity Strategy. Baghdad, Iraq, 2017. Available at: https://www.itu.int/en/ITU-D/Cybersecurity/. Accessed: April 21, 2025.
4- League of Arab States, General Secretariat, Department of Legal Affairs. Arab Convention on Combating Information Technology Crimes. December 21, 2010. Available at: http://www.arablegalnet.org. Accessed: May 11, 2025.
5- United Nations. Universal Declaration of Human Rights, Article 12: The Right to Privacy. 1948.
6. United Nations, General Assembly. Freedom of Expression Online. 2016. Available at: https://digitallibrary.un.org/record/845728?ln=en. Accessed: 2025.
7. United Nations, Human Rights Council. Report of the Office of the United Nations High Commissioner for Human Rights. 2022. Available at: https://docs.un.org/ar/A/HRC/51/17. Accessed: 23/06/2025.
8. United Nations, Office of Counter-Terrorism. United Nations Counter-Terrorism Centre Cybersecurity Programme. 2024. Available at: https://www.un.org/counterterrorism/cct/programme-projects/cybersecurity. Accessed: 19/04/2025.

9. United Nations, Office of the High Commissioner for Human Rights. International Bill of Human Rights. 2025. Available at: https://www.ohchr.org/ar/what-are-human-rights/international-bill-human-rights. Accessed: 25/04/2025.
10. United Nations, Office of the High Commissioner for Human Rights. Privacy in the Digital Age, Digital Space and Human Rights. 2025. Available at: https://www.ohchr.org/ar. Accessed: 11/06/2025.
11. United Nations, Human Rights Council. The Right to Privacy in the Digital Age, Document A/HRC/60/45. 2025. Available at: https://docs.un.org/ar/A/HRC/60/45. Accessed: 25/11/2025.
12. United Nations, General Assembly. International Covenant on Civil and Political Rights: The Right to Freedom of Opinion and Expression. 1966.
13- International Committee of the Red Cross. International Humanitarian Law. 03/12/2014. Available at: https://www.icrc.org. Accessed: 29/04/2025.
14- International Committee of the Red Cross. Protection of civilians and other protected persons and objects from the potential human cost of information and communication technology activities during armed conflicts. 34th International Conference of the Red Cross and Red Crescent, Geneva, 2024.
15- Iraqi National Cybersecurity Center. Iraqi Cybersecurity Strategy 2022–2027. Available at: https://ncc.gov.iq. Accessed: 18/03/2026.
16- National Cybersecurity Authority. "Royal Decree Establishing the National Cybersecurity Authority." Saudi Press Agency (SPA), January 19, 2019. Available at: https://www.spa.gov.sa. Accessed March 12, 2026.
17- Basem Ali Khraisan. "Hacktism: A Study of the Relationship Between Computer Networks and Politics." Bayan Center for Studies and Planning, April 18, 2022. Available at: https://www.bayancenter.org.
18- Basem Muhammad Fadel. The Right to Privacy: Between Absolute and Restrictive Rights. Alexandria: Dar Al-Jami'a Al-Jadeeda, 2018.
19- Hassanein Alaa Muhammad. "The Legal Framework for Protecting Personal Data in Modern Communication Networks." Future University, November 17, 2025. Available at: https://uomus.edu.iq. Accessed December 25, 2025.
20- Hussein Suleiman Rashid Al-Tayyar. "Cybersecurity from the Perspective of the Objectives of Sharia." Taif University Journal of Humanities, Issue 21, 2020, p. 264.
21- Dhiab Musa Al-Badayneh. "Cybercrimes: Concept and Methods." In: Emerging Crimes in Light of Regional and International Changes and Transformations. Amman, Jordan: College of Strategic Sciences, 2014, pp. 2–4.
22- Rana Misbah Abdul-Muhsin. "Mechanisms for Combating Cybercrimes in the Kingdom of Saudi Arabia: An Analytical Study." The Legal Journal for Legal Studies and Research, Volume 5, 2023, p. 1387.
23- Steve Moore. "Four Types of Threat Intelligence and How to Use Them Effectively." Exabeam, 2026. Available at: https://www.exabeam.com/ar/explainers. Accessed: 16/02/2026.
24- Salah Haider Abdul-Wahid. Cyber Warfare: A Study of its Concept, Characteristics, and Ways to Confront It. Master's Thesis, Middle East University, Amman, Jordan, 2021, pp. 22–24.
25. National Cybersecurity Authority. Cybersecurity Controls for Sensitive Systems (ECC). 2019. Available at: https://acs.uj.edu.sa. Accessed: March 13, 2026.

26. National Cybersecurity Authority. Cybersecurity Controls for Data (DCC). 2022. Available at: https://acs.uj.edu.sa. Accessed: March 15, 2026.
27. Abdullah Yahya Saeed Al-Zahrani. Cybersecurity Strategies in Light of Modern Technologies and Challenges. Master's Thesis, Naif Arab University for Security Sciences, Kingdom of Saudi Arabia, 2020.
28. Alaa El-Din Farhan. "From Nuclear Deterrence to Cyber Deterrence." Al-Fikr Magazine, Issue 16, 2021, p. 2246.
29- Cybersecurity Incident Response Team (CERT). Iraqi Cybersecurity Incident Response Team. 2017. Available at: https://cert.gov.iq/index.html. Accessed: April 14, 2025.
30. Communications and Media Commission. Communications and Information Technology Law. Baghdad, Iraq, 2009. Available at: https://archive3.parliament.iq/ar/2017/04/27/
31. Communications and Media Commission. Communications and Information Technology Law. Baghdad, Iraq, 2009. Available at: https://archive3.parliament.iq/ar/2017/04/27/
32. Amended Cybercrime Law No. (30) of 2010. Jordan, 2010.
33. Iraqi Penal Code No. (111) of 1969. Article (287) concerning forgery and fraud. Baghdad, Iraq, 1969.
34. Iraqi Births and Deaths Registration Law No. (148) of 1971. Article (17). Iraq, 1971.
35- Anti-Terrorism Law No. (13) of 2005. Baghdad, Iraq, 2005.
36- Anti-Cybercrime Law No. (5) of 2012, as amended. United Arab Emirates, 2012.
37- Journalists Syndicate Law No. (178) of 1969, as amended. Article (25). Iraq: Iraqi Gazette, 1969.
38- Constitution of the Republic of Iraq of 2005. Article (17). Iraq, 2005.
39- Human Rights Council. Resolution on the promotion, protection and enjoyment of human rights on the Internet. United Nations, 2016. Accessed: 17/03/2025.
40- Muhammad ibn Abi Bakr al-Razi. Mukhtar al-Sahah. Volume 4. Beirut, Lebanon: Al-Maktaba al-Asriya, 1998.
41- Muhammad Yusuf. "What Do You Know About the Cyber Mercenary: The Dirty Arm of Corporations and States?" Al Jazeera Net, October 15, 2024.
42- Mahmoud Berri. Cybersecurity: The Science of Communication, Control, and Domination. 1st ed., Beirut, Lebanon: Islamic Center for Studies, 2019.
43- Cybersecurity Directorate, Iraqi Ministry of Interior. Cybersecurity Directorate. December 4, 2022. Available at: https://moi.gov.iq. Accessed: March 5, 2025.
44- Republic of Iraq. Draft Law on Combating Cybercrime. Baghdad, Iraq, 2019. Available at: https://menarights.org/sites/default/files/2022-06/New%20version_CyberCrimeDraftLaw%20%281%29.pdf.
45- United Nations Office of Counter-Terrorism (UNCCT). Cybersecurity. 2023. Available at: https://www.un.org/counterterrorism/ar/cct/programme-projects/cybersecurity. Accessed: 08/05/2025.
46- Metehan Durmaz. "The New United Nations Convention on Combating Cybercrime: Objectives and Gaps." SMEX, 12/12/2024. Available at: https://smex.org/ar/. Accessed: 12/05/2025.

47- Nazih Abdel-Maqsoud and Hisham Mustafa. "Economic Security and its Impact on Achieving an Optimal Standard of Living." Journal of the Faculty of Sharia and Law, 2023, p. 1189.
48- Youssef Bougrara. "Cybersecurity: The Algerian Strategy for Security, Defense, and Cyberspace." Journal of African and Nile Basin Studies – Arab Democratic Center, Vol. 3, 2018, p. 106.
Foreign Sources:
- African Union. African Union Convention on Cyber Security and Personal Data Protection. 27 June 2014. Available at: https://ccdcoe.org/uploads/2018/11/AU-270614-CSConvention.pdf . Accessed on: 19 March 2026.
2- Gregg Lindemulder and Matt Kosinski. What Is Cybersecurity? IBM, 12 August 2024. Available at: https://www.ibm.com/think/topics . Accessed on: 2024.
3- Deborah Brown. Cybercrime is Dangerous, But a New UN Treaty Could Be Worse for Rights. Human Rights Watch, 13 August 2021.
4- Charlie Plumb. Understanding the UN's New International Treaty to Fight Cybercrime. UNU Centre for Policy Research, 30 July 2024. Available at: https://unu.edu/cpr/blog-post/understanding-uns-new-international . Accessed on: 18 February 2026.
5- Convention on Cybercrime (Budapest Convention). European Treaty Series – No. 185. Council of Europe, 23 November 2001. Available at: https://rm.coe.int . Accessed on: 20 March 2026.
6- Cybersecurity and Infrastructure Security Agency (CISA). What Is Cybersecurity?. CISA, 2009. Available at: https://www.cisa.gov/news-events/news/what-cybersecurity . Accessed on: 2 May 2025.
7- Helaine Leggat. A New Look at the Budapest Convention on Cybercrime. ICTLC Australia, 2024. Available at: https://www.ictlc.com/a-new-look-at-the-budapest-convention-on-cybercrime/?lang=en . Accessed on: 14 May 2025.
8- International Telecommunication Union (ITU). Cyber Security. International Telecommunication Union, Geneva, 2008.
9- João Valente Cordeiro and Paula Lobato de Faria. Health Data Privacy and Confidentiality Rights: Crisis or Redemption?. Public Health Journal, 2014, p. 142.
10- John Markoff. Step Taken to End Impasse Over Cybersecurity Talk. The New York Times, 17 July 2010, A7, col. 1.
11- Kali Robinson. How Israel's Pegasus Spyware Stoked the Surveillance Debate. Council on Foreign Relations, 8 March 2022. Available at: https://www.cfr.org/in-brief/how-israels-pegasus-spyware-stoked-surveillance-debate . Accessed on: 10 May 2025.
12- Matthew Kosinski. What Is a Data Breach?. IBM, 2026. Available at: https://www.ibm.com/think/topics/data-breach . Accessed on: 19 February 2026.
13- United Nations. Convention on Cybercrime. 2024. Available at: https://docs.un.org/ar/A/RES/79/243 .
14- Othman Al-Salloum and Azizah A. Al-Zahrani. Success Factors in Achieving Excellence in Cybersecurity. International Journal of Research and Studies Publishing, Vol. 68, 20 June 2025, pp. 72–73.
15- Palatty Nivedita James. 130+ Data Breach Statistics 2026 – The Complete Look. Astra, 6 January 2026. Available at: https://www.getastra.com/blog/security-audit/data-breach-statistics/ . Accessed on: 20 February 2026.

16- Robb Shawe. Cybersecurity and Human Rights: Navigating the Balance Between Security. Journal of Information Technology and Integrity, 2025, Vol. 110, p. 3.
17- Sohair Ahmed Shaikh. Surveillance of Cyber Security and Human Rights. International Journal for Legal Research & Analysis, 7 January 2025, p. 2.
18- Steve Morgan. Top 5 Cybersecurity Facts, Figures, Predictions and Statistics for 2021 to 2025. Cybersecurity Ventures, 5 February 2024. Available at: https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2021-to-2025/ . Accessed on: 10 May 2025.