تحديات حماية الخصوصية في الفضاء السيبراني: دراسة في القانون العراقي

م.م. زهراء محمد هادي

جامعة القادسية . كلية القانون

zhrahady849@gmail.com

الملخص

في ظل التحول الرقمي السريع الذي اجتاح العالم، أصبح الفضاء السيبراني ذا أهمية عالية وجزأ من حياتنا اليومية، فتتدفق من خلاله الكثير من المعلومات الشخصية أحيانا والحساسة التي تمس المؤسسات والدوائر الحكومية أحيانا أخرى، لذلك برزت مسائل قانونية جديدة ولعل من أبرزها حماية البيانات الشخصية من التعدي والاستغلال.

لذا تحظى مسألة حماية بيانات الأشخاص على أولويات سلم الدول بالاهتمام، حيث تلقى عناية كبيرة من قبل الدول، وتوجب عليها ذلك من اجل متابعة التطورات ومعالجتها لحمايتها من أي اختراق، ففي كل يوم يتم خلق واكتشاف أساليب جديدة تدعم هذه المنظومة المتطورة وبالتالي هناك هجمات مضادة تحاول خرقها، وبسبب هذه الهجمات الالكتروني تجد المؤسسات نفسها امام واجب عليها حماية معلوماتها، فأصبح يشكل هذا التطور تحدي كبير امام الدول والمؤسسات من اجل حماية بياناتها، لان أي خطر على هذه المعلومات والبيانات يشكل تهديدا للأمن الوطني.

الكلمات المفتاحية: حماية الخصوصية ، المعلومات الشخصية ، الفضاء السيبراني ، الهجمات الألكترونية ، الأمن السيبراني .

Abstract

In the midst of the rapid digital transformation sweeping across the world, cyberspace has become highly significant and an integral part of our daily lives. Vast amounts of personal—and sometimes sensitive—information flow through it, affecting both individuals and governmental and institutional entities. This reality has given rise to new legal challenges, most notably the protection of personal data from infringement and exploitation.

Therefore, the issue of safeguarding individuals' data has become a top priority for states, receiving considerable attention and prompting countries to keep pace with developments and implement measures to protect such data from breaches. Every day, new methods are developed and discovered to enhance this sophisticated ecosystem; however, there are also continuous counterattacks attempting to penetrate it.

As a result of these cyberattacks, institutions find themselves obliged to protect their information, making this technological evolution a significant challenge for both nations and organizations striving to secure their data. Any threat to such information and data constitutes a potential risk to national security.

Keywords: privacy protection, personal information, cyberspace, cyber-attacks, cyber security.

المقدمة

في العصر الحالي، لم يعد أحد بمنأى عن استخدام الفضاء السيبراني، إذ غدت الهواتف الذكية والحواسيب وأجهزة الاتصـــال المختلفة جزءاً لا يتجزأ من حياة الأفراد اليومية، وأصـــبحت في متناول أيدي الجميع بمختلف أعمارهم وفئاتهم. فقد أسـهم هذا التطور التكنولوجي في تسـهيل العديد من جوانب الحياة، مثل سـرعة التواصـل، والوصول إلى المعلومات، وتبادل البيانات، وحفظها بشكل آمن وسريع نسبياً.

ورغم هذه المزايا الهائلة، إلا أن الفضـاء السـيبراني بات يحمل في طياته تحديات ومخاطر متنامية، إذ أصـبحت حماية البيانات والمعلومات مسـألة بالغة التعقيد، لا سـيما في ظل التطورات المسـتمرة في أسـاليب الاختراق والقرصـنة الإلكترونية. فقد أصـبحت الخصـوصـية مهددة بشـكل غير مسـبوق، وصـار من السـهل نسـبياً على المجرمين السـيبرانيين الوصـول إلى المعلومات الشـخصـية أو الحسـاسـة، سـواء للأفراد أو المؤسـسـات أو حتى الحكومات.

ويُعد أي خلل أو ضعف في البنية التحتية الإلكترونية خطراً كبيراً يهدد أمن المعلومات ويُعرّضها للسرقة أو التلاعب أو التدمير، الأمر الذي قد يسبب خسائر مالية ضخمة، أو يلحق أضراراً معنوية ومجتمعية جسيمة، أو يؤدي إلى تسريب معلومات في غاية الحساسية قد تمس الأمن القومي للدول.

ونظراً لتزايد الهجمات الإلكترونية من قِبل قراصنة يسعون لاختراق البيانات وتحقيق مكاسب غير مشروعة أو حتى إحداث أضرار متعمدة، أصبحت الهجمات السيبرانية تشكل خطراً حقيقياً ومستمراً يجب التصدي له بطرق علمية وقانونية. ولهذا، سارعت الدول إلى تبني استراتيجيات أمنية متقدمة، وسنّ وتشريع القوانين الرادعة التي تُجرّم الجرائم السيبرانية وتحدد عقوباتها بوضوح، بهدف حماية الأفراد والمؤسسات من هذه المخاطر المتنامية، وضمان استقرار الأمن الوطني والاجتماعي والاقتصادي.

مشكلة الدراسة

تتمثل مشكلة الدراسة في السعي الى تحقيق استخدام امن للهواتف الذكية والحواسيب، مع الحفاظ على خصوصية الافراد وبياناتهم الشخصية، وضمان عدم انتهاك حقوقهم او المساس بحرياتهم عند التفاعل مع الفضاء السيبراني.

اهداف الدراسة

تهدف الدراسة الى تسليط الضوء على أبرز التحديات التي تواجه حماية البيانات في ظل التكنولوجي المتسارع، والتوصل الى حلول والتوصيات القانونية لتعزيز حماية البيانات وضمان عدم المساس بحقوق الافراد في البيئة الرقمية.

منهجية الدراسة

انتهجت الدراسة المنهج الوصفي التحليلي، من خلال تحليل النصوص القانونية الواردة في التشريعات ذات الصلة بحماية البيانات والمعلومات، مع وصف وتحليل الحالات الظاهرة المتعلقة بانتهاك الخصوصية، وذلك لتحديد مدى فعالية هذه النصوص في حماية الافراد داخل الفضاء السيبراني.

هيكلية البحث

المبحث الأول: الفضاء السيبراني واثر الامن السيبراني على حماية الخصوصية

المطلب الأول: أهمية الامن السيبراني وتميز الجرائم الالكترونية عن الجرائم التقليدية

المطلب الثاني: التحديات التي تهدد انتهاك الخصوصية في الامن السيبراني

المبحث الثاني: الإطار القانوني لحماية الخصوصية

المطلب الأول: وسائل حماية الأنظمة الالكترونية في الاتفاقيات الدولية

المطلب الثاني: وسائل حماية الأنظمة الالكترونية في التشريع العراقي

المبحث الأول

الفضاء السيبراني وأثر الامن السيبراني على حماية الخصوصية

ان الهدف الأســـمى الذي يختص به الامن الســـيبراني هو حماية البرامج والبيانات والشـــبكات وأجهزة الكمبيوتر، من الهجوم والضـرر او الوصـول الغير رسـمي للمعلومات والبيانات، وأيضـا من بين اهم اهداف الامن السـيبراني هو القوة على مواجهة التهديدات والهجمات العمدية او غير العمدية، لذلك اصـبح من أولويات الدول، وبالأخص بعد الحروب الالكترونية التي باتت تجوب العالم، وهذا ينبئ عن ظهور حروب جديدة بعيدة عن الحروب التقليدية، بهذا اصبح الامن السيبراني من أولويات الدول وخاصة الكبرى منها فهو وسيلة حماية الفضاء السـيبراني، ونحن في هذا المبحث سـنبين اهم ما يميزه وتميز الجرائم السـيبرانية عن التقليدية وذلك في المطلب الأول ، اما المطلب الثاني سنبين التحديات التي تواجه الامن السيبراني.

المطلب الأول

أهمية الامن السيبراني وتميز الجرائم السيبرانية عن التقليدية

ان مـا يميـز الامـن السـيبراني مجموعـة مـن الخصـائص حيـث يتصـف بانـه لـه خصـائص اجتماعيـة وأخـرى تقنيـة، وأيضـا يمتـاز بانـه شـبكة لا تملـك حجـم معـين وانمـا ذات نطـاق واسـع ولـيس لهـا حـدود محـددة، وقـدراتها تمتـد بشـكل واسـع، ولهـا سـرعة تفاعـل وتـرابط بـين المسـتخدمين، وغالبـا مـا تكـون محصـورة بيـد الـدول الكبـرى حيـث تكـون لهـا القـدرة الواسـعة علـى شـن الهجمـات السـيبرانية، وأيضـا إمكانيـة تطـوير البنـى التحتيـة الخاصـة بـالأمن السـيبراني مختصـر علـى الـدول الكبـرى اكثـر مـن غيرهـا، فالـدول هـي المـتحكم الأساسـي فـي هـذا العـالم الافتراضـي وتسـتطيع ممارسـة سـلطاتها داخـل حـدودها، ولهـا القـدرة علـى التفـوق التكنولـوجي ولهـا مـؤهلات تسـاعدها علـى تهيـأت البنـى التحتيـة لـه[1] حيـث يعمـل الامـن السـيبراني علـى مكافحـة الجريمـة الالكترونيـة او مـا يعـرف بالجريمـة السـيبرانية ويمكـن تعريفهـا (هـي جـرائم ذكيـة تنشـأ فـي البيئـة الالكترونيـة او الافتراضـية، والقـائمين عليهـا اشـخاص او منظمـات لـديهم

[1] . د. فارس محمد العمارات، الامن السـيبراني مفهوم وتحديات العصـر، الطبعة الأولى، دار الخليج، الأردنـــــ عمان، 2022، ص25.

درجـة عاليـة مـن الـذكاء ويمتلكـون المعرفـة والتقنيـة، ممـا يتسـبب بخسـائر فادحـة للمجتمـع، وتظهـر أهميتـه نتيجـة التـرابط القـائم بـين دول العـالم باسـتخدام الشـبكة العنكبوتيـة).[1] ولـذلك يجـب حجـب هـذه التقنيـة عـن الأشـخاص غيـر المخـولين بصـفة رسـمية، وحصـرها بيـد الـدول؛ الا انهـا مـا يصـعب السـيطرة علـى الجريمـة المعلوماتيـة هـو وجـود مسـتخدمون غيـر الـدول يسـتخدمون القـوة السـيبرانية، لأغـراض غيـر سـوية تهـدد امـن واقتصـاد وسياسـة الـدول وخصوصـية الأشـخاص سـواء كـان عـامون او اشـخاص عـاديون، وهنـاك شـركات تمتلـك قـوة تكنلوجيـة قـد تضـاهي القـوة الموجـودة لـدى الـدول ، وقـد تفوقهـا فـي بعـض الأحيـان، الا ان مـا يقلـل مـن هـذه القـوة هـو عـدم إضـفاء الشـرعية لهـا، فخـوادم شـركات(فيس بـوك face book ، جوجـل google، مايكروسـوفت Microsoft) لهـا قواعـد بيانـات عملاقـة تسـتطيع مـن خلالهـا تسـتغل الأسـواق، وتـؤثر علـى اقتصـاديات وحتـى علـى عقليـة ومعتقـدات شـبابها وبالتـالي ثقافـات المجتمـع وتوجهاتـه، الا انهـا ينقصـها الشـرعية وإمكانيـة ان تتصـرف بحريـة، فهـي لا تسـتطيع الا ان تتصـرف ضمن حدود تمنحها لها الدولة صاحبة الشأن.[2]

نتيجـة تطـور أجهـزة الحواسـيب والشـبكات وانتشـار اسـتخدامها بشـكل واسـع، أصـبحت عصـب الحيـاة الـذي لا يسـتطيع شـخص الاسـتغناء عنهـا، ورقمنـة الـدوائر الحكوميـة مـن اجـل سـهولة الوصـول للبيانـات والمعلومـات، كـل هـذا أدى الـى نمـو الجـرائم السـيبرانية بشـكل واضـح، وقـد نمـت وانتشـرت بأوجهـا فـي العقـدين الماضـيين، وتحولـت مـن جريمـة ثانويـة الـى ظـاهرة عالميـة، وادت الـى خسـائر ماليـة طائلـة وحـالات إيـذاء وتتعـدى لتشـمل سـرقة الهويـة والاحتيـال، وهنـاك جـرائم خاصـة مثـل الابتـزاز و والتحـرش عبر الانترنيت و العاب الكترونية انتشرت بين الأطفال والمراهقين قد تؤدي الى الانتحار.[3]

وبذلك فان الجرائم السيبرانية تختلف عن الجرائم التقليدية في عدة معايير ومنها؛

---

[1] علاء الدين فرحان، من الردع النووي الى الردع السيبراني: دراسة لمدى تحقيق مبدأ الردع في القضاء السيبراني، بحث منشور في مجلة الفكر . جامعة بسكرة ، المجلد 16، العدد الأول، 2021،ص 273.

[2] د. فارس محمد العمارات، مصدر سابق، ص26.

[3] د راشد محمد المري، الامن السيبراني وحماية الأنظمة الالكترونية دراسة تحليلية تأصيلية، بحث منشور في مجلة الشريعة والقانون بدمنهور، العدد40، 2023، ص18.

أولاـ طبيعـة البيئـة التـي تنشـأ بهـا الجريمـة: ان طبيعـة الجريمـة السـيبرانية التـي تنشـأ فـي بيئـة مختلفـة تمامـا عـن تلـك التـي تنشـأ بهـا الجريمـة التقليديـة، فميـدان ارتكـاب الجريمـة الالكترونيـة يتطلـب تـوفر حـد أدنـى مـن المعرفـة بالتقنيـة الالكترونيـة فـي مجـال الاعـلام الالـي لارتكابهـا، بينمـا الجريمـة التقليديـة لا تتطلب مثل هذه التقنية. [1]

ثانياـ الجريمـة الالكترونيـة ذات بعـد دولـي: فهـذا النـوع مـن الجـرائم لا تحـد بحـدود دولـة معينـة، بينمـا تكـون عـابرة لحـدود الـدول ويرجـع ذلـك الـى اسـتخدام شـبكات الانترنيـت العنكبوتيـة، وهـي بـذلك تثيـر الكثيـر مـن التحـديات القانونيـة وأيضـا السياسـية، وسـبب صـعوبة مواجهتهـا يعـود الـى الإشـكاليات السياسـية بملاحقـة المـرتكبين عبـر الحـدود الدولـة الواحـدة الـى دولـة الأخـرى وقـد تمتـد اضـرارها لتشـمل أقـاليم عـدة ورقع جغرافية واسعة.[2]

ثالثاـ جـرائم سـرية المصـاعب فـي الكشـف عـن هويـة الجـاني فـي الجريمـة السـيبرانية جعلهـا مـن الجـرائم السـرية، الا بأسـاليب متطـورة وعاليـة الجـودة وتتطلـب خبـرة كبيـرة فـي مجـال التقنيـات، ومعقـدة الاكتشـاف لانهـا فـي الغالـب لا تتـرك اثـار ماديـة، وحتـى الاثـار المعلوماتيـة اذا وجـدت صـعوبة الوصـول اليهـا، لان يمكـن تشـفيرها فـي حالـة الاحتفـاظ بهـا وسـهولة حـذفها مـن قبـل الجـاني اذا تطلـب ذلـك، فهـي تعتبـر مـن الجرائم الغامضة ايضا[3].

رابعاـ جـرائم تبتعـد عـن العنـف والـذي نقصـد بـه هنـا هـو العنـف الجسـدي امـا العنـف بالالفـاظ فهـو كثيـر الحـدوث هـذا النـوع مـن العنـف، ان هـذا النـوع مـن الجـرائم لا يتطلـب قـوة جسـدية او العضـلية لارتكابهـا يكفـي الجلـوس خلـف الجهـاز الحاسـب او التليفـون واسـتخدامه فـي ارتكـاب الجريمـة او انتهـاك خصوصـية او ارتكاب على شخص او ما الى ذلك من تشهير وتعرض وتحريض.[4]

---

[1] مهدي رضـا، الجرائم السـيبرانية واليات مكافحتها في التشـريع الجزائري، بحث منشـور في مجلة اليزا لبحوث والدراسـات، المجلد السادس، العدد الثاني، 2021، ص114.

[2] إبراهيم رمضان، الجريمة الالكترونية وسبل مواجهتها في التشريع الإسلامي والأنظمة الدولية- دراسة تحليلية تطبيقية، بحث منشور في مجلة كلية الشريعة القانون، المجلد 30، العدد الثاني، 2015، ص2015.

[3] كوثر عروس، الجريمة السـيبرانية في صـورها المسـتحدثة، بحث منشـور في مجلة القانون والتنمية، المجلد الرابع العدد الأول، 2022، ص53.

[4] مهدي رضا، مرجع سابق ، ص116.

وهنـاك أسـباب وجيهـة أدت الـى ضـرورة وجـود نظـام فعـال يعمـل علـى المحافظـة علـى المعلومـات وإيجـاد البيئـة القانونيـة التـي تحميهـا، لعـل مـن ابرزهـا هـو الحاجـة الـى الارتبـاط بشـبكات الانترنيـت وعـد م إمكانيـة البقـاء بشـكل معـزل عـن العـالم، فشـبكات الانترنيـت أصـبحت عصـب الحيـاة ولا يمكـن الاسـتغناء عنهـا، فالشـركات والمؤسسـات وحتـى فـي الحيـاة اليوميـة اعتمـدت بشـكل رئيسـي علـى المعلومـات و البيانـات المتداولـة عبـر هـذه الشـبكات، واصـبح مـن الصـعب السـيطرة عليهـا لـذا يجـب التعامـل معهـا امـر واقـع، و تذليل التحديات والعقبات وخلق بيئة قانونية تضمن استخدامها بشكل امن.

المطلب الثاني

التحديات التي تهدد انتهاك الخصوصية في الامن السيبراني

يمثل الفضاء السيبراني بشكل عام عنصر جذب للمنتهزين من اجل استغلال الثغرات، وانتهاك خصوصية الاخرين سواء كان من اجل مصلحة فردية لهم او من اجل التخريب بشكل عام، وهذا يؤدي الى ضرورة الحرص الشديد من اجل المحافظة وحماية البيانات الشخصية او المعلومات العامة، بسبب إمكانية استغلالها من قبل النفوس الضعيفة او المتطرفين او حتى الجماعات الإرهابية، لان إمكانية توظيفها في عمليات إرهابية اكثر سهولة وسرعة، ويمكن الاستهداف من خلالها المراكز والمؤسسات الحكومية الحساسة وتدمير بنى التحتية لشبكاتها المعلوماتية، وينتج عنها خسائر كبيرة قد تتجاوز خسائر الجرائم التقليدية.[1]

وان من اهم التحديات التي يمكن ان تهدد خصوصية الأشخاص في الفضاء السيبراني، ويتمكن من خلالها المتطرفين او المخربين او المغرضين وحتى الارهابين من استغلالها، وسوء استخدام الفضاء السيبراني مما يوجب تفعيل الامن السيبراني من اجل المحافظة عليها وحمايتها من الهجمات المضادة لها، وتوفير بيئة امنة للمعلومات والبيانات:

أولا. ضعف البنى التحتية للشبكات والمعلومات وإمكانية اختراقها

الأصـل ان الشـبكات وجدت من اجل الرغبة في سـهولة التواصـل بين المسـتخدمين، وتيسـير الوصـول لاي معلومات او البيانات، لذلك صـممت بشـكل مفتوح بدون قيود وحواجز امنية عالية الدقة، وان إمكانية وجود ثغرات واستغلالها من قبل المغرضين ممكن.[2]

---

[1] د. اسعد طارش عبد الرضا، على إبراهيم مشجل المعموري، الامن السيبراني ودوره في انتشار ظاهرة الإرهاب في العراق بعد العام 2003، بحث منشور في مجلة الدراسات الدولية، العدد الثمانون ، 2020، ص161.

[2] د. اسعد طارش عبد الرضا، على إبراهيم مشجل المعموري، مصدر سابق، ص162.

فالجرائم السيبرانية ممكن ان تهدد الامن الوطني للدولة، والهجمات المستمرة على البنى التحتية تضعف مواجهتها، وان أي اخفاق في مواجهة هذا التهديد يؤثر بشكل سلبي على استقرارها السياسي والاقتصادي، لذا ان القدرة على مواجهة الهجمات السـيبرانية مهمة جدا في المحافظة على الدفاع الوطني، وهذا يعتمد على قوة الامن السـيبراني من اجل ردع الهجمات ووقف التهديدات لحماية المؤسسات الحكومية، وقد اشارت الدراسات بعض الأدوات التي من الممكن ان تعزز الامن السـيبراني وسـاعدت في صـد الهجمات ومنها (الذكاء الاصـطناعي). [1] فان دمج الذكاء الاصطناعي مع الامن السيبراني يعمل على تسهيل مهمة اكتشاف الهجمات وتلافي عواقبها، وعلى الدول ان تعمل بشكل مستمر من اجل تطوير وتعزيز البني التحتية للامن السيبراني، فأي تهدير يشكل تحديا للمؤسسات الحكومية من اجل الكشف عن مدى قوتها في حماية مؤسساتها و حجب معلوماتها.

اما من جانب حماية الخصـوصـية فان المحافظة على خصـوصـية الأشـخاص تعد من الأمور المؤثرة على حياة الفرد وعائلته ومكانته الاجتماعية، وذلك من خلال اختراق أجهزة الحواسـيب او الدخول للهواتف الشـخصـية عن طريق البريد الالكتروني، عن طريق نشر صور مخلة بالشرف تمس السمعة والشرف وقد تكون الصور حقيقية او حتى مزيفة عن طريق البرامج تقوم بتعديل الصـور، وقد يكون عن طريق التشـهير والسـب والقذف، وتعتبر هذه المسائل من المسائل المهمة التي تشكل حطرا واضح على ترابط المجتمع العراقي لذا يجب على المشرع العراقي العمل على السـيطرة ومكافحة مثل هذه الأمور والتشـديد على مرتكبين وتوعدهم بأقصـى العقوبات ، وبما يلائم الجرم المرتكب.

ثانيا. انتشار الأسلحة السيبرانية

ان انتشـار برامج صـممت من اجل تنفيذ بعض المهام مثل إزالة او تخريب، الغرض منها تدمير أجهزة مؤسسات الدول او الشركات، او تخريب البنى التحتية لشبكات المعلومات، او الاعتماد على برامج صغيرة هدفها قطع الاتصـال او سـرقة البيانات اثناء تصـفح المسـتخدمين، وأيضـا قد يتم اللجوء الى شـفرات مخبئة في برامج واسعة الانتشار ومتداول شعبيا، يستخدم لنشر فايروس او يعمل على سرقة كلمات المرور الخاصة بالمستخدمين، او التجسـس على معلومات سـرية دون تدميرها، بهدف الوصـول الى الخطط العسـكرية والاسـرار الحربية، او

[1] د. علاء عبد الخالق حسين واخرون، الامن السيبراني المبادئ والممارسات لضمان سلامة المعلومات، الطبعة الأولى، دار السرد، العراق . بغداد، 2024، ص156.

الاطلاع على خرائط الحواسيب الالية لاستخدامها في شن هجوم الكتروني، وانتشرت بعض الأسلحة السيبرانية على استحداث برامج مهمتها مسح البيانات يمكن تسليطها لمسح بيانات الأشخاص المستهدفة.[1]

ثالثا . غياب الحدود الجغرافية

ان اتصاف الشبكات الالكترونية بانها عابرة للحدود ولا توجد حدود تحدها او تضعف السيطرة عليها، و يمكن استخدامها على نطاق واسع دون فرض سيطرة دولة محددة عليها، وإمكانية التخفي بهوية غير محددة او غير حقيقية، بالإضافة الى قلة الكلفة و توفر الشبكات على نطاق واسع في العالم، فهي لا تحتاج الى مصادر تمويل ضخمة كل ما تحتاج اليه الخبرة والتقنية في مجال الالكترونيات، يعطي للمغرضين فرصة استغلال الفرص و تنفيذ مخططاتهم المختلفة من تدمير وتجسس وعمليات إرهابية، وفي الوقت نفس يصعب على السلطات الأمنية المختصـــة الســـيطرة عليها، او ملاحقة المرتكبين وتحديد هوياتهم ، ويوفر لهم ســـهولة التنقل تداخل المواقع والتطبيقات .[2]

رابعا . ضعف التشريعات والقوانين الرادعة لهذا النوع من الجرائم في بعض الدول

ان التطور في الهجمات الالكترونية السريع يتطلب تطور بنفس السرعة تشريعات تعمل على صد كل ما ممكن ان يحدث من خرق الكتروني او جريمة، الا ان هذا التطور بالتشـــريع لم ينفذ من كل الدول فالعراق مثلا يفتقر لحد الان من صدور قوانين تشريعية تواجه الجرائم الالكترونية، الامر الذي كان مدعاة لظهور خلايا إرهابية ومظاهر شاذة في المجتمع العراقي، فهناك جماعات تعمل بشكل مكثف ومؤثر بإشاعة الفتن والبغضاء والطائفية، وأخرى إرهابية تتسـلط وتتجسـس من اجل تخريب المواقع الحكومية، والعمل على تجنيد عناصـر من اجل تهديد الامن وزعزعت النظام.

---

[1]ـ د. فارس محمد العمارات، إبراهيم الحمامصة، الامن السيبراني المفهوم والتحديات، الطبعة الأولى، دار الخليج، الأردن ـ عمان، 2022، ص137.

[2] انيس حسـيب المصـلاوي، الخبرة القضـائية في الجرائم المعلوماتية والرقمية دراسـة مقارنة، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2016، ص177.

وفي تقرير لقناة (DW) الألمانية في 2006/6/15 جاءت به مؤكدتا بان 4500 موقع الكتروني على الشبكات الالكترونية له نشـــاط ذا طابع إرهابي، ومواقع الكترونية أخرى بأعداد مقاربة تعمل على نشـــر الفتن والطائفية وتضليل عقول الشباب ونشر الأفكار المتطرفة. [1].

المبحث الثاني

الإطار القانوني لحماية الخصوصية

أصبح الفضاء السيبراني يلعب دورًا جوهريًا في حياة الإنسان في ظل عصر العولمة، ولم يعد منفصلًا عن تفاصيل الحياة اليومية، إذ بات يشمل مختلف مجالاتها، مما جعل العالم بمثابة "قرية صغيرة". ومع هذا التوسع الهائل، تنامت المخاطر والتهديدات المرتبطة به، خاصة مع بداية تسعينيات القرن الماضي التي شهدت انطلاق الثورة التكنولوجية والمعلوماتية، والتي تسللت إلى جميع الميادين السياسية والاجتماعية والاقتصادية.

وقد ازدادت الأهمية الاستراتيجية للفضاء السيبراني مع اتجاه معظم الدول، بما فيها المؤسسات الحكومية والشركات، نحو الرقمنة الكاملة. هذا التطور السريع في مجالات التداول الإلكتروني أدى إلى تصاعد الاهتمام بقضايا الأمن السيبراني، لا سيما من قِبل الدول الكبرى، التي تسعى لحماية فضائها الرقمي من الهجمات السيبرانية، من خلال وضع وتنفيذ استراتيجيات أمنية متطورة تهدف إلى تعزيز الحماية الإلكترونية وصدّ محاولات الاختراق؛ ونحن في هذا المبحث سنسلط الضوء على الوسائل المتبعة لحماية الأنظمة الالكترونية في الاتفاقيات الدولية وذلك في المطلب الأول، وسائل حماية الأنظمة الالكترونية في التشريع العراقي وسنتطرق له تباعا في المطلب الثاني.

المطلب الأول

وسائل حماية الأنظمة الالكترونية في الاتفاقيات الدولية

أدى التطور الكبير في وســائط النقل بشــكل عام عبر الدول، والتطور بشــكل خاص بوســائل التواصــل الاجتماعية الى سـهولة انتقال المعلومات بين الدول، وصـعوبة السـيطرة على الحدود الدولية من أي اختراق امني وتسـريب لمعلومات او تأثير المجتمع على الاخر، وبالتالي تأثير الهجمات المضـادة من إرهاب او إشـاعة فتن او تجسـس ليس بمعزل عن إمكانية هذا الانتقال عبر حدود الدول، الامر الذي يتطلب وضـع خطوات جدية لمعالجة هذا التأثير وكان منها؛

[1] د. اسعد طارش عبد الرضا، على إبراهيم مشجل المعموري، مصدر سابق، ص163.

أولا . ربط شبكات الاتصال والمعلومات

حيث تعمل بعض الدول جعل هناك وســـائل اتصـــال ممكنة بين أجهزة العدالة الجنائية الوطنية وأجهزة الشرطة هذا على مستوى الدولة الواحدة، والعمل على ربط هذه الأجهزة في أجهزة الدول الأخرى عن طريق السلك الدبلوماسـي وبموجب اتفاقيات دولية واضـحة، لذلك وجب على الدول ان تطور نظم الاتصـال وتبادل المعلومات فيما بينها، من اجل ان يتم تعقب المجرمين بمجرد خروجهم من دولة ارتكاب الجريمة، فتقوم شـــرطة الدولة التي وقع فيها وتم خروج المجرم منها بإبلاغ الدولة المتفق معها امنيا بملاحقة المجرمين في حدود دولتهم التي هرب منها.[1]

وان من اهم أســـاليب التعاون الشـــرطي الدولي هي المنظمة الدولية للشـــرطة الجنائية(الانتربول)، ويعد الانتربول من اهم طرائق التنظيمية لمكافحة أي اعتداء عابر للحدود، ومن احد مهام الانتربول توحيد إجراءات التسليم حول العالم، وذلك من خلال تنسيق عالي وتجميع بيانات وتبادل المهمات من اجل تيسير خدمات التحقيق وملاحقة المجرمين والتخلص من فكرة عدم إمكانية ملاحقتهم وانهم بامان في حالة فرارهم الى بلدان أخرى.

ويجب على كل دولة العمل الدؤوب على تطوير نظم المعلومات، وان تكون هناك مؤسـسـات مركزية تحتوي على قواعد بيانات وتقديم خبرات ودورات تدريبية في حيز التصـــدي للجرائم الالكترونية، وذلك من خلال المتابعة مع الخبراء والمختصين الدوليين وافتتاح مختبرات ومراكز تطوير وتدريب، وان تكون جميعها ذات مركزية واحدة.

ثانيا . شرطة "الويب" الدولية

أنشـــئت هذه المؤســـســـة في الولايات المتحدة الامريكية عام 1986، وكان الهدف منها تلقي شـــكاوى المستفيدين من الشبكات العنكبوتية، ومتابعة الجناة والمتجسسين على المعلومات والبيانات الشخصية او العامة، من اجل حماية خصوصياتهم، والبحث عن الأدلة والمعلومات التي تدينهم وتقديمهم للمحاكمة، ويعملون بها فريق متكون من (61) دولة حول العالم وهذا يسـهل على فريق العمل بتتبع النشـاطات الاجرامية، التي تتم في مختلف دول العالم، شريطة ان يعمل ضمن ضوابط لا تمس بحقوق وحريات الاخرين، وان لا تستخدم هذه الشبكات في بشكل ينافي القواعد القانونية من انتهاك خصوصية او محاول استخدامها بمواقع مسيئ للأدب والأخلاق، وان لا

[1] د فارس محمد العمارات، د. إبراهيم الحمامصة، مصدر سابق، ص149. \\\

تحرض على التطرف او العمليات الإرهابية ولا حتى تشـجع على التظاهرات او الانقلابات بحجة ممارسـة حقوق الانسان، فواجبها المحافظة على الاستقرار والهدوء العام.[1]

الاتفاقيات الدولية في حماية الأنظمة الالكترونية

تعتبر الاتفاقيات والمواثيق الدولية من اهم صور التعاون الدولي، ويتجلى هذا التعاون بشكل مخصوص في حقل مكافحة الجرائم السيبرانية، ومن بين هذه المعاهدات التي تسعى الى التعاون الدولي في حيز مكافحة الجرائم السيبرانية، "معاهدة بوداست لمكافحة جرائم الانترنيت وتوصيات المجلس الأوربي بشأن مشاكل الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات "

وتعد معاهدة بودابسـت أولى المعاهدات التي عالجت الجرائم السـيبرانية، وقد اقامت في العاصـمة المجرية بودابســـت، وذلك بتاريخ 2003/11/23، والتي كان هدفها التعاون والتضـــامن الدولي في مواجهة الانتهاكات الالكترونية، ويعتبر التوقيع على المعاهدة اللبنة الأولى في مجال انشاء تعاون الدولي لصد أي انتهاك او استخدام ســـيئ يتم عن طريق الشـــبكات العنكبوتية، وقد وقع على هذه المعاهدة (26) دولة اوربية، والولايات المتحدة الامريكية، وكندا واليابان وجنوب افريقا، وتتكون من 48 مادة موزعة على اربع فصـــول، وقد كان القســـم الأول يتعلق بالنصوص الجنائية الموضوعية، ويتضمن الجرائم الخاصة بشأن الخصوصية وانتهاك المعلومات والبيانات، والجرائم المتصـلة بالحاسـب شـاملة اسـتعمال الحواسـيب من اجل التزوير والافعال الاحتيالية، وقد جرمت أيضـا الأفعال التي تتعلق بالمضـــمون والمحتوى، والجرائم المتصـــلة بالتعدي على حقوق المؤلف، والقســـم الثاني كان خاص بالقانون الاجرائي فيما يتعلق بالإجراءات الجنائية، وأيضـــا تشـــمل المحافظة على المعلومات والبيانات الخاصـة والاوامر الخاصـة بالتسليم، وتتضـمن كذلك مراقبة وتفتيش بيانات الحواسيب التي تخزن تلك المعلومات، وأيضـا حددت المعاهدة الطرق الملزمة باتخاذها في التحقيق في الجرائم الالكترونية، وكان التعهد بين الدول مبني على التعاون واتكاتف من اجل مواجهة هذا النوع من الجرائم . [2]

---

[1] مفرح الزاهراني يحي، الابعاد الاستراتيجة والقانونية للحرب السيبرانية، مجلة البحوث والدراسات، العدد الأول، المجلد 14، 2017، 235.

[2] د فارس محمد العمارات، د. إبراهيم الحمامصة، مصدر سابق، ص162.

اما على المســـتوى الإقليمي، فهناك الاتفاقية العربية لمكافحة تقنية المعلومات، وتهدف الى تعزيز التعاون بين الدول العربية، لمواجهة الهجمات والتحديات المنتشـرة باسـتخدام التكنلوجيا، وقد صـادق العراق عليها بموجب قانون تصديق الاتفاقية العربية لمكافحة جرائم تقنية رقم (31) لسنة 2013.[1]

المطلب الثاني

وسائل حماية الأنظمة الالكترونية في التشريعات العراقي

ونعني بذلك ضـرورة تدخل تشـريعي من خلال تجريم أي اعمال الكترونية تمس خصـوصـية الافراد مما ينعكس سـلبا على المجتمع العراقي، واصـبح من الضـروري مواجهة هكذا أفعال من خلال التشـريعات القانونية، والمواكبة للفضـاء السـيبراني من خلال التشـريعات القانونية غير التقليدية والضـرورية لتصـدي للجرائم المعلوماتية ووافية للتعامل بها وعند تتبع موقف المشـــرع العراقي نجد خلو الميادين القانونية العراقية من أي قانون خاص بالتصدي للجريمة المعلوماتية لمواجهة التطورات الناتجة عن الجرائم السيبرانية.[2]

الا ان هناك محاولات لازالت قيد المصـادقة عليها، وهي مشـروع فقانون الجرائم المعلوماتية لسـنة 2012، ولعل من اهم تحتاج الى تعديل بعض القوانين التي ترتكز عليها القوانين الأخرى، وتتوخى اللجان واضـــعة هذا القانون الحذر من المســاس بحقوق وحريات الاخرين، عند النص على هكذا قوانين لان الفارق بسـيط جدا بين المحافظة على الحريات ومصادراتها.[3]

الا ان إقليم كردستان العراق بادر المشرع الكردستاني اصدار قانون الجرائم المعلوماتية، وجاءت المادة الثانية منه "يعاقب بالحبس مدة لا تقل عن سـتة اشـهر ولا تزيد على خمس سـنوات وبغرامة لا تقل عن ملين دينار ولا تزيد عن خمس ملايين او بأحدي هاتين العقوبتين كل من اسـاء اسـتعمال الهاتف الخلوي او أي جهة اتصـالية سـلكية او لا سـلكية او انترنيت او البريد الالكتروني وذلك عن طريق تهديد او القذف او السـب او نشـر اخبار مختلفة"

---

[1] قانون تصديق الاتفاقية العربية رقم (31) لسنة 2013 ، نشر في الجريدة الرسمية "الوقائع العراقية"، العدد 4292، بتاريخ 2013/9/30.

[2] محمود صـباح العادلي، الفراغ التشـريعي، في مجال مكافحة الجرائم، 2009، بحث متاح شـبكة المعلومات الدولية(الانترنيت)، على الموقع

http://www.shaimaatalla.com/v6/showthred.php?t=9377

[3] خليل يوسف جندي، المواجهة التشريعية للجرائم المعلوماتية على المستويين الدولي والوطني (دراسة مقارنة)، مجلة كلية القانون للعلوم القانونية والسياسية، المجلد السابع العدد 26، جامعة كركوك/2018، ص110.

وكذلك إشارة المادة الثالثة من نفس القانون " يعاقب بالحبس مدة لا تقل عن ثلاثة اشهر ولا تزيد عن سنة وبغرامة لا تقل عن ســـبعمائة وخمســـون الف دينار ولا تزيد عن ثلاثة ملايين دينار او بإحدى هاتين العقوبتين كل من تسبب عمدا باستخدام واستغلال الهاتف الخلوي او أي أجهزة اتصالية سلكية او لا سلكية ا الانترنيت او البريد الالكتروني في ازعاج غيره في غير الحالات الواردة بالمادة ثانيا من هذا القانون" [1]

اما على المستوى التشريعي الوطني فهناك مشروع قانون مكافحة الجريمة المعلوماتية لسنة 2012، مقدم لمجلس النواب خاص لمواجهة هذا النوع من الجرائم، ويسعى ايضا هذا القانون توفير الحماية القانونية للاستخدام المشروع للحواســيب الالكترونية والعمل على حماية شــبكات المعلومات، من اجل تحقيق الامن والاســتقرار وحمايتها من الاعتداء وسوء الاستخدام والهجمات الالكترونية للمحافظة على خصوصية الافراد.

اتخذ عدة وسـائل واليات فنية وتقنية يمكن اسـتخدامها لضـمان سـرية المعلومات وضـمان سـهولة الرجوع اليها، وللوقاية من خطر تهديداتها الالكترونية او الحد من الاضـــرار حجم الخســـائر، وتختلف هذه التقنيات الحماية فبعضــها وقاية قبل حدوث الخلل والأخرى للحد من الخســائر والاضــرار. ومنها؛ التوقيع الالكتروني الغاية منه زيادة سرية البيانات والمعلومات والمحافظة على خصوصية المعلومات، وعدم إمكانية أي من الأشخاص الاطلاع او تعديل او مراسـلة أي شـخص اخر، وذلك عن طريق تحديد هوية المرسـل والمسـتقبل الالكتروني، من جل منع التلاعب والتحايل على الاخرين، وقد عرف التوقيع الالكتروني في مســـودة قانون مكافحة الجرائم المعلوماتية العراقي سنة 2012، ،بانه (علامة شخصية تتخذ شكل حروف او ارقام او رموز او إشارات او أصوات وغيرها وله طابع منفرد يدل على نسبته الى الموقع ويكون معتمدا من جهة تصدق على ذلك).[2]

ويجب التوعية والتشـديد على ضـرورة حماية الحسـابات وتوفير نظم التحقق من الهوية، من خلال كلمات السـر الطويلة والمعقدة وأسماء المستخدمين الصريحة، وتأكيد الحسابات بالهويات الشخصية وان هذه الطريقة وان كانت هذه هي الطريقة الأكثر اسـتخداما، الا انها بدأت تفقد قوتها بسـبب قوة المسـتخدمين في مجال التكنلوجيا وأصـبح من السـهولة اختراقها، وذلك لتمتعهم بالخبرة التقنية في مجال المعلومات، وصـار بعد ذلك الى التشفير الالكتروني كوسيلة اكثر دقة وتوفر حماية اكبر لضمان سرية المعلومات، فالتشفير عبارة عن ترميز الملفات والبيانات وحتى

---

[1] قانون اساء استعمال أجهزة الاتصال، رقم (6) لسنة 2008.

[2] المادة الأولى/ عاشرا من مسودة قانون مكافحة الجرائم المعلوماتية 2012، متاح على الموقع http://www.Iraqja.iq/view.1645

الرسـائل بل حتى تشـفير كلمات السـر والبرامج التي يعمل عليها، والغاية منه المحافظة على المعلومات المهمة خصوصا في المرافق والمنشأة الحيوية مثل الامن والدفاع.[1]

لذلك من اجل حماية الفضـاء السـيبراني في العراق وبالتالي المحافظة على خصـوصـية المعلومات، العمل على الإسراع بانتهاء من وضـع القوانين الخاصـة بأمن المعلومات والمصـادقة عليها، وتعديل القوانين الداخلية في حالة تعارضـها، العمل على التطور في هذا الجانب من خلال فتح مراكز يتدرب بيها وتوعية الأشـخاص تقنيا عليها، وتوحيد جهود القطاعين الخاص والعام في هذا الجانب.

الخاتمة

سنتناول في الخاتمة اهم النتائج والتوصيات التي تم التوصل اليها من خلال بحثنا وكالاتي:

اولاً: النتائج

1. ان المحافظة على خصـوصـية الأشـخاص تعد من الأمور المؤثرة على حياة الفرد وعائلته ومكانته الاجتماعية، تتطلب المحافظة على البنى التحتية الالكترونية وان أي اخفاق في تقوية البنى التحتية يؤثر بشـكل سـلبي على اسـتقرارها السـياسـي والاقتصـادي، لذا ان القدرة على مواجهة الهجمات السـيبرانية مهمة جداً في المحافظة على خصوصية الأشخاص في الفضاء السيبراني.
2. ضـعف التشـريعات والقوانين الرادعة لهذا النوع من الجرائم في بعض الدول، مشـروع قانون مكافحة الجرائم المعلوماتية لسـنة 2012، حيث يسـعى هذا القانون توفير الحماية القانونية للاسـتخدام المشـروع للحواسـيب الالكترونية والعمل على حماية شبكات المعلومات، من اجل تحقيق الامن والاستقرار وحمايتها من الاعتداء وسوء الاستخدام والهجمات الالكترونية للمحافظة على خصوصية الافراد.

المقترحات

1. ضرورة وجود نظام فعال يعمل على المحافظة على المعلومات وإيجاد البيئة القانونية التي تحميها، لعل من ابرزها هو الحاجة الى الارتباط بشـبكات الانترنيت وعد م إمكانية البقاء بشـكل معزل عن العالم، فشـبكات الانترنيت أصـبحت عصـب الحياة ولا يمكن الاسـتغناء عنها، والعمل على اعداد دورات تعمل على تثقيف المسـتخدمين والأفضل ان تكون الكترونية ويتم بثها من خلال برامج شائعة الاستخدام.

---

[1] طارق بن عبدالله، مقدمة في الحاسب الالي وتقنية المعلومات، الطبعة الثانية، دار الوطن العربي، الرياض، 1996، ص189.

2. ضـرورة تدخل تشـريعي من خلال تجريم أي اعمال الكترونية تمس خصـوصـية الافراد مما ينعكس سـلبا على المجتمع العراقي، واصبح من الضروري مواجهة هكذا أفعال من خلال التشريعات القانونية، والإسراع بالمصادقة على مسودة قانون الجريمة المعلوماتية لسنة 2018.

المصادر

أولا: الكتب والمراجع القانونية

7. انيس حسيب المصلاوي، الخبرة القضائية في الجرائم المعلوماتية والرقمية دراسة مقارنة، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2016،
8. د. علاء عبد الخالق حسين واخرون، الامن السيبراني المبادئ والممارسات لضمان سلامة المعلومات، الطبعة الأولى، دار السرد، العراق . بغداد، 2024.
9. طارق بن عبد الله، مقدمة في الحاسب الالي وتقنية المعلومات، الطبعة الثانية، دار الوطن العربي، الرياض، 1996.
10. د. فارس محمد العمارات، إبراهيم الحمامصة، الامن السيبراني المفهوم والتحديات، الطبعة الأولى، دار الخليج، الأردن . عمان، 2022.

ثانيا : البحوث القانونية

3. د. اسعد طارش عبد الرضا، على إبراهيم مشجل المعموري، الامن السيبراني ودوره في انتشار ظاهرة الإرهاب في العراق بعد العام 2003، بحث منشور في مجلة الدراسات الدولية، العدد الثمانون ، 2020، ص161.
4. إبراهيم رمضان، الجريمة الالكترونية وسبل مواجهتها في التشريع الإسلامي والأنظمة الدولية دراسة تحليلية تطبيقية، بحث منشور في مجلة كلية الشريعة القانون، المجلد 30، العدد الثاني
5. راشد محمد المري، الامن السيبراني وحماية الأنظمة الالكترونية دراسة تحليلية تأصيلية، بحث منشور في مجلة الشريعة والقانون بدمنهور، العدد 40 ، 2023.
6. خليل يوسف جندي، المواجهة التشريعية للجرائم المعلوماتية على المستويين الدولي والوطني (دراسة مقارنة)، مجلة كلية القانون للعلوم القانونية والسياسية، المجلد السابع العدد 26، جامعة كركوك،2018.

7. مفرح الزهراني يحي، الابعاد الاستراتيجية والقانونية للحرب السيبرانية، مجلة البحوث والدراسات، العدد الأول، المجلد 14، 2017.

8. ـــــ كوثر عروس، الجريمة السيبرانية في صورها المستحدثة، بحث منشور في مجلة القانون والتنمية، المجلد الرابع العدد الأول، 2022.

9. مهدي رضـا، الجرائم السـيبرانية واليات مكافحتها في التشـريع الجزائري، بحث منشـور في مجلة اليزا لبحوث والدراسات، المجلد السادس، العدد الثاني، 2021.

ثالثا: البحوث القانونية المنشورة

رابعا: القوانين

1. قانون اساء استعمال أجهزة الاتصال، رقم (6) لسنة 2008 .
2. مشروع قانون الجرائم المعلوماتية 2018.

الاتفاقيات

اتفاقية بودابست Budapest Convention .