Journal Of the Iraqia University (73-5) March (2025)

ISSN(Print): 1813-4521 OnIine ISSN:2663-7502
Journal Of the Iraqia University
available online at: https://www.mabdaa.edu.iq

تأثير الهجمات السيبرانية على الحقوق المدنية والرقمية

د. غلامعلى قاسمى الاستاذ المشارك في القانون الدولي جامعة قم ، كلية القانون ، قم ،

هاشم حسين علي كاظم الحسون طالب دكتوراه في القانون الدولي العام جامعة قم ، كلية القانون ، قم

The impact of cyber attacks on civil and digital rights Hashim hussein ali kadhim alhasoon

Phd student in public International Law
Qum Univerzity , faculty of la , Com, Iran
hashimalhasoon1@gmail .com
Dr. Gholamali Ghasemi
Associate Professor of International Law
Qom University, Faculty of Law, Qom, Iran
g.ghasemi43@gmail.comg.

Abstract

Technological development and digital transformation have facilitated access to information, but have created major challenges related to individual rights by launching cyber attacks that expose civil and digital rights to serious violations, as they lead to the violation of personal data privacy, access to information, leakage, and spying on users, threatening individuals and institutions, which weakens confidence in digital systems and government and private institutions, and disrupts and restricts the exercise of civil rights. Cyber attacks become a tool that threatens the basic principles of human rights in the digital age and negatively affects social and political stability, which calls for updating legislation and addressing the legal vacuum to ensure respect for the privacy of individuals and their rights in light of the widespread use of digital technologies, achieving international cooperation, and developing comprehensive policies that protect digital infrastructure and enhance the protection of civil and digital rights for individuals and institutions. It is also necessary to increase community awareness about the risks of cyber attacks to ensure a balance between security requirements and the preservation of rights **Keywords:** Cyber attacks, civil rights, digital rights, artificial intelligence

المستخلص

ان التطور التكنولوجي والتحول الرقمي عمل على سهولة الوصول الى المعلومات الا انه خلق تحديات كبيرة تتعلق بحقوق الافراد من خلال القيام بشن الهجمات السيبرانية التي تعرض الحقوق المدنية والرقمية للانتهاكات الخطيرة, اذ يؤدي الى انتهاك خصوصية البيانات الشخصية والوصول الى المعلومات و تسريبها والتجسس على المستخدمين ويهدد الافراد والمؤسسات, مما يضعف الثقة بالأنظمة الرقمية والمؤسسات الحكومية والخاصة واحداث خلل في ممارسة الحقوق المدنية وتقييدها, وتصبح الهجمات السيبرانية اداة تهدد المبادئ الاساسية لحقوق الانسان في العصر الرقمي وتؤثر سلبا على الاستقرار الاجتماعي والسياسي, مما يستدعي الى تحديث التشريعات ومعالجة الفراغ القانوني بما يضمن احترام خصوصية الافراد وحقوقهم في ظل الانتشار الواسع للتقنيات الرقمية, وتحقيق التعاون الدولي ووضع سياسات شاملة تحمي البنى التحتية الرقمية ولتعزيز حماية الحقوق المدنية والرقمية للأفراد والمؤسسات كما لابد من زيادة الوعي المجتمعي حول مخاطر الهجمات السيبرانية لضمان تحقيق توازن بين متطلبات الامان والحفاظ على الحقوق. **الكلمات المفتاحية:** الهجمات السيبرانية, الحقوق المدنية, الحقوق الرقمية, الذكاء الاصطناعي.

بيان المسألة

المقدمة

تعد الهجمات السيبرانية من أخطر التحديات التي تواجه حقوق الإنسان في العصر الحديث ، إذ أنها تمثل تهديداً متزايداً للعديد من الأفراد والمجتمعات ،فقد تجاوزت هذه الهجمات مجردا الأنظمة والسرقات الالكترونية لتصبح سلاحاً يؤثر على حقوق الإنسان بشكل عام ، وعلى الحقوق الأساسية للأفراد بشكل خاص ومنها الحقوق المدنية والحقوق الرقمية ، كما ان الهجمات السيبرانية على البيانات الشخصية والمعلومات الحساسة انتهاكاً مباشراً لحقوق الخصوصية، حيث يتم استخدام هذه البيانات في أغراض غير مشروعة مثل التجسس أو التلاعب بالأفراد. كما تؤثر تلك الهجمات على حق الإنسان في حماية واحترام كيانه المعنوي، ولا ريب أنها تؤدي إلى انتهاك الحق في الخصوصية, وتنعكس الهجمات سلباً وبشكل كبير على حق الإنسان في الوصول إلى المعلومات والذي بات اليوم من أهم حقوق الإنسان اتصالًا بواقعه ومساهمته في الحياة الاجتماعية ، كما تؤثر الهجمات السيبرانية سلبا على الحقوق الرقمية وبشكل كبير، اذ تؤدي إلى خرق الخصوصية والسرية وسرقة البيانات الشخصية والمالية للأفراد والمؤسسات، كما يمكن أن تؤدي هذه الهجمات إلى تعطيل الخدمات الرقمية التي يعتمد عليها المستخدمون كالخدمات المصرفية عبر الإنترنت والتجارة الإلكترونية والاتصالات، لذلك يجب على الحكومات اتخاذ التدابير اللازمة لمكافحة الهجمات السيبرانية من خلال تطوير التشريعات والسياسات والأنظمة التقنية التي تحد من انتشار هذه الهجمات وتعزز أمان وسلامة الأنظمة والشبكات الرقمية.

أهمية البحث

تبرز أهمية هذا البحث من خلال إلقاء المزيد من الضوء على مخاطر الهجمات السيبرانية على الحقوق المدنية والرقمية نظرا لانتشارها المتزايد في العصر الحديث, كما يساهم في تقييم القوانين والتشريعات, ونشر الوعي بين الافراد والمؤسسات لمواجهة التحديات وحماية المستخدمين.

أهداف البحث

يهدف البحث إلى دراسة تأثير الهجمات السيبرانية على الحقوق المدنية والرقمية من خلال :

١. التعرف على تأثير الهجمات السيبرانية على الحقوق المدنية والتي تستهدف فيها الافراد كانتهاك الخصوصية والوصول الى المعلومات.

٢. التعرف على تأثير الهجمات السيبرانية على الحقوق الرقمية والتي تؤدي انتهاك الحق في الخصوصية الرقمية والتي تستهدف بيانات المستخدمين في المؤسسات من خلال عمليات الاختراق باستخدام برامجيات التجسس وسرقة الهوية الرقمية واستخدامها لاغراض غير قانونية.

مشكلة البحث

إن مشكلة البحث تكمن في السؤال الآتي :

١- مامدى تاثير الهجمات السيبرانية على الحقوق المدنية والرقمية ؟

منهجية البحث

تم إعتماد المنهجين الوصفي و التحليلي للدراسة تأثير الهجمات السيبرانية الحقوق المدنية والرقمية.

خطة البحث

تم تقسيم خطة البحث إلى مطلبين تناولنا في المطلب الأول تأثير الهجمات السيبرانية الحقوق المدنية والذي قسم إلى فرعين تناولنا في الفرع الأول منه اختراق الهجمات السيبرانية للبيانات الشخصية واما الفرع الثاني تناولنا فيه تأثير الهجمات السيبرانية على حق احترام الكيان المعنوي للفرد ، أما المطلب الثاني تناولنا فيه تأثير الهجمات السيبرانية الحقوق الرقمية والذي تم تقسيمه إلى فرعين تناولنا في الفرع الأول منه انتهاك الخصوصية الرقمية و الحق في الوصول إلى المعلومات، اما الفرع الثاني تناولنا فيه التلاعب بالهوية الرقمية ، ثم ختمنا بحثنا بالاستنتاجات والتوصيات.

المطلب الأول :- تأثير الهجمات السيبرانية على الحقوق المدنية

إن الهجمات السيبرانية تؤثر بشكل كبير على الحقوق المدنية بطرق متعددة، حيث يمكن أن تساهم في تقييد الحريات الشخصية وتعريض الحقوق الأساسية للخطر، وإن إقرار حقوق الأفراد داخل دولة ما، إلا وفيه اعتراف صريح بالسهر على حماية هؤلاء الأفراد من أي اعتداء أو انتهاك خارجي قد يصيبهم، فالفرد منذ أن يولد تولد معه للعالم المحسوس حقوقاً تتعلق بالنسب والجنسية وغيرها، نفس الشيء بالنسبة للمواطنين الموجودين في دولة ما، فالدول تحاول جاهدة حماية مصالح رعاياها أينما حلوا وارتحلوا، وهذه الحماية لا تنشأ هي الأخرى من فراغ بل إن الفرد هو من يكتسبها من خلال حصوله على جنسية البلد الذي ترعرع فيه. ولذلك فمنح الحقوق والحريات له ما هو إلا اعتراف به وبوجوده ضمن مواطني الدولة، غير إنه أحيانا قد يتم المساس بهذه الحقوق المدنية التي يتمتع بها الأفراد وعلى ضوء ما تقدم سوف نقوم بتقسيم هذا المطلب إلى فرعين نتناول في الفرع الأول منه اختراق الهجمات السيبرانية للبيانات الشخصية وفي الفرع الثاني سنتناول فيه تأثير الهجمات السيبرانية على حق احترام

الكيان المعنوي للفرد كالآتي :

الفرع الأول:- اختراق الهجمات السيبرانية للبيانات الشخصيةإن الإنسان كان منذ القدم هدفاً وموضوعا للمعلومات، سواء بإرادته الحرة أو بفعل الإكراه فهذه المعلومات تتضمن معطيات شخصية، وتعد عاملًا أساسياً في التواصل، وفي التعرف على سلوك الأفراد داخل المجتمع، ولولاها لما استطاع أحد التعرف على أحد، فهي تعد من أهم المعلومات التي يمكن أن يتميز بها كل فرد من أفراد المجتمع، والتي تختلف من شخص لآخر، فالهجمات السيبرانية يمكن أن تؤدي إلى انتهاك خصوصية الأفراد، حيث قد تُستخدم لسرقة البيانات الشخصية، مثل المعلومات الصحية أو المالية. هذا قد يؤدي إلى إساءة استخدام هذه البيانات بطرق تؤثر على حقوق الأفراد في التحكم في معلوماتهم الشخصية [١]وقبل هذا وذاك، فالكل يتفق على أن الانتشار الواسع في استعمال التكنولوجيا، أدى إلى تزايد حدة التهديدات التي يمكن أن تمس خصوصية البيانات الشخصية للأفراد في المجال الرقمي أو الافتراضي، حيث إن بيانات الأشخاص لم تعد حبيسة ومدونة في الأوراق التقليدية، بل إن كل فرد أصبح بمجرد ما يتصفح عالم الأنترنت، قد يقوم هذا الأخير تلقائيا بتخزين معلوماته الشخصية بشكل آلي دون الحاجة في ذلك لأخذ الإذن من صاحبها. ولذلك فإن العالم الرقمي وتطوراته أسهم بشكل كبير في تعريض معطيات الأفراد الشخصية إلى الانتهاك، أي أن كل فرد قد يصبح معملًا لإنتاج المعلومات حول نفسه سواء عبر تطبيقات الأنترنت المنتشرة أو تطبيقات الهاتف النقال، ولا يبقى سوى أن يتم تنظيمها وجمعها عبر استخدام خوارزميات ذكية تمكن من تصنيفها وتميزها، لإعداد في النهاية دليلًا متكاملًا لكل فرد مع بياناته الشخصية ومراقبة تحركاته وغيرها [٢]فتبادل المعلومات إذن بين الدول اعتبر مسألة لا غنى عنها، خصوصا وأن هذا يدخل في مجال التعاون القضائي بينهما، فأحيانا قد يكون لهذا التبادل محاسن عدة إذا ما تعلق الأمر بمسألة البحث عن المتطرفين ومرتكبي الجرائم الخطيرة أو في مسألة نظام تسليم المجرمين، فهنا نجد أن أمن المجتمع يصيبه تهديد وزعزعة استقراره، غير أنه قد يصل أحيانا هذا التبادل إلى درجة يمكن معه المس بحقوق الأفراد، وإلحاق بهم أضرارا كثيرة نتيجة إفشاء معلوماتهم الشخصية للعموم أو إظهارها في مواقع رقمية ما كان أصحابها ليظهروها حتى وإن تم الحصول على إذن منهم.وأمام هذا التطور التكنولوجي ونتيجة لإمكانية تعريض بيانات الأفراد الشخصية للانتهاك، وبالنظر إلى أنه أضحى من الصعب محاصرة التقنيات الجديدة، فقد دفع هذا الأمر إلى إصدار نصوص تشريعية وقوانين تضفي نوع من الحماية القانونية للمعطيات ذات الطبيعة الشخصية، وإن هاجس الدول حالياً ينحو منحى تكريس حقوق الإنسان والحفاظ عليها من أي انتهاك وهو ما يتضح من خلال تكريسها لعدة حقوق منها الحق في حماية المعطيات والبيانات الشخصية، حيث إن أغلب الدول قامت بإصدار قوانين ملائمة تنظم هذا الحق[٣]كالتشريع الفرنسي الذي نظم قانونا سنة 1978 أسماه حماية البيانات والحريات، بالإضافة إلى التشريع المصري الذي أصدر القانون رقم 151 لسنة 2020 المتعلق بحماية البيانات الشخصية[٤]، ويلاحظ أن حماية المعطيات الشخصية أضحت ضرورة تشريعية لكل الدول، فالحق في الحماية يبدأ بمجرد ما تتم معالجة هذه المعطيات، ولذلك فالقوانين الواردة أعلاه تشكل مرجعاً أساسيا لحماية هذا الحق، لكونها تورد مجموعة من المبادئ والمقتضيات التي تكرس الحماية، بل حتى الاتحاد الأوربي قام بالمصادقة سنة 2016 على اللائحة العامة لحماية البيانات, (GDPR)الشخصية للأفراد داخل الاتحاد الأوربي، وهي تتضمن متطلبات قوية ترفع معايير حماية البيانات وامانها وامتثالها وتؤلف بينها.وفي القانون العراقي، إن تأثير الهجمات السيبرانية يظهر بوضوح في عدة مجالات، منها حماية البيانات الشخصية والسرية الطبية، وكذلك في مجال حقوق الملكية الفكرية والتجارية. فالهجمات السيبرانية قد تؤدي إلى سرقة المعلومات والبيانات الحساسة، مما يعرض حقوق الأفراد والشركات للخطر، ويؤثر على النظام الاقتصادي والتجاري.كما إن الحد من انتهاك حقوق الإنسان أمر سهل على كل دولة؛ بل إن القوانين ماهي إلا وسيلة لمحاولة زجر كل من يتجرأ على المساس بحقوق الإنسان، والتقليص من هذه الظاهرة التي تعد مسألة أساسية، غير إن النصوص القانونية السالفة الذكر، فبالرغم من وجودها إلا أن الأفراد ما زالوا يتعرضون لانتهاك أبسط حقوقهم خصوصاً مع التزايد التكنولوجي الذي يعرفه العالم [٥] هذا، ونظراً للتكنولوجيا المتطورة التي ما فتئت في تزايد مستمر لم يقف الأمر هنا في المجال الرقمي أو الافتراضي، بل أصبحنا نتحدث عن تقنيات أخرى والتي ترتبط بشكل وثيق بمجال الذكاء الاصطناعي، فالاستعمالات المتعددة في مختلف المجالات لتقنيات الذكاء الاصطناعي، قد يكون هو الآخر فيه مساس ببيانات الأشخاص التي تعد حقا من حقوق الإنسان.ذلك إن المحور العصبي للذكاء الاصطناعي يعتمد بالضرورة على قاعدة البيانات التي تتوافر لهذا الذكاء، فكلما توسعت هذه القاعدة كلما تعمق مفهوم الذكاء لديه وأصبح أكثر حرفية وفاعلية في أداء الغايات المرجوة، وطالما أن البيانات تتسم بالعموم، فليس ثمة مشكلة قانونية تصور غير أن الإشكالية تبرز فيما يتعلق بالبيانات الخاصة، ذلك أن الهجمات السيبرانية في بعده المدني أو التجاري إنما يعتمد على قاعدة بيانات هائلة عن الأشخاص الذين يتعامل معهم، من حيث الأسماء والمهن، والجنس، والحالة الصحية والتاريخ العائلي، وأرقام الحسابات المصرفية[٦]وتماشياً مع هذا، فإن المشرع الفرنسي حاول في القانون رقم١٧ لعام ١٩٧٨بالعمل على تنظيم بيانات الأشخاص، ونص في المادة الأولى من هذا القانون على أن : " تكنولوجيا المعلومات

يجب أن تكون في خدمة كل مواطن، وأن يتم تطويرها في إطار التعاون الدولي، وأن لا تنتهك أيضاً الهوية الإنسانية، ولا حقوق الإنسان، ولا الخصوصية ولا الحريات الفردية، بحيث أوجب على المتعاملين مع هذه البيانات، بما فيها مجال الذكاء الاصطناعي احترامه، لاسيما بالنسبة للآلات الذكية ذات التخزين الرقمي بحيث لا يساء استخدام هذه البيانات أو يتم التهاون في الحفاظ عليها، واستخدامها لغير الأغراض التي أحدث لها، خصوصا في القضايا ذات الطابع التجاري.والمادة السادسة تنص على أن معالجة المعطيات الشخصية تعتبر مشروعة إذا ما تمت بطريقة عادلة وقانونية، أو تجميعها لأغراض محددة وصريحة ومشروعة ولا تتم معالجتها مرة أخرى بطريقة لا تتوافق مع هذه الأغراض، أي أن معالجة البيانات للأغراض الإحصائية أو الأغراض البحث العلمي أو التاريخي فهي تعتبر متوافقة مع مبدأ المشروعية، غير أنه علق معالجة هذه البيانات على ضرورة موافقة الشخص المعني، أو الخضوع للشروط الأساسية المنصوص عليها قانونًا، فالمشرع الفرنسي حاول سن مقتضيات صارمة تتعامل مع مسألة معالجة البيانات الشخصية، ونفس الأمر ينطبق على مجال الهجمات السيبرانية، بحيث لابد أن يتم استخدام بيانات الأشخاص لأغراض مشروعة، وإلا اعتبر انتهاكاً منه لحق من حقوق الإنسان إن موقف المشرع الفرنسي تم تدعيمه بموجب التوجه الحديث للتشريع الأوربي الصادر سنة 2016، والذي دخل حيز التنفيذ في ايار 2018، والمتعلق بحماية البيانات الخاصة للأشخاص الطبيعيين وتداولها ، والذي يهدف إلى خلق مجموعة قواعد قانونية موحدة بين دول الاتحاد الأوربي، وتعزيز الثقة بين المواطنين والشركات في الفضاء الرقمي، وبموجب هذه اللائحة RGPD، فإن معالجة المعطيات الشخصية أضحت معلقة على موافقة مسبقة ومكتوبة وواضحة من المستخدمين قبل الشروع فيها ، مما يعني أن التشريع الأوربي يشدد في الإجراءات القانونية الخاصة بالبيانات الشخصية، بحيث أضحت الحماية القانونية لها تتناول محاور ثلاثة : الجمع، والتحليل والتداول. إن المشرع المصري بمقتضى قانون حماية البيانات الشخصية ذهب في نفس التوجهين السالفين الذكر، بحيث سن مقتضيات قانونية صارمة تعمل على حماية البيانات الشخصية المعالجة الكترونياً جزئيا أو كلياً لدى أي حائز أو متحكم أو معالج لها، وذلك بالنسبة للأشخاص الطبيعية والتي علق هو الآخر إمكانية جمعها أو معالجتها أو الإفصاح أو الإفشاء عنها بأي وسيله من الوسائل بموافقة صريحة من الشخص المعني، كما أن كل دخول غير مرخص له لبيانات شخصية أو وصول غير مشروع يعتبر خرقا وانتهاكا لهذه البيانات، مما يوجب معه حماية قانونية في مواجهة المعتدي على البيانات الشخصية[٧]وبالتالي، يلاحظ على أن جل التشريعات عملوا على تنظيم المعطيات ذات الطابع الشخصي، وجعلوا إمكانية المعالجة الآلية معلقة على موافقة صريحة من طرف المعنى بالأمر، مما يعني أنه في الهجمات السيبرانية على الحقوق المدنية، والذي يعد مجالًا حساساً لكونه يتغدى على البيانات الشخصية للأفراد، أن يتم مراعاة فيه جانب الشفافية في الحصول على هذه البيانات، وأن تراعى فيه الشروط المنصوص عليها قانونًا، وتولى هذه البيانات وكيفية حمايتها وطرق معالجتها أساليب متعددة ومهمة[٨]ويعني هذا إنه بالرغم من غياب نص قانوني ينص صراحة على حماية المعطيات الشخصية التي قد تنتهك نتيجة الهجمات السيبرانية، إلا أنه من وجهة نظرنا فإن هذه النصوص المعمول بها من قبل مختلف الدول، كفيلة لأن تنظم كذلك هذا المجال، مادام أن المجال الإلكتروني يشبه إلى حد كبير تقنيات الهجمات السيبرانية في المعالجة الآلية لبيانات الأشخاص، وهذا يدل على أن النصوص القانونية المتعلقة بحماية بيانات الأشخاص من أي انتهاك الموجودة الآن تصلح للتطبيق على تقنيات الذكاء الاصطناعي، اللهم إذا تعلق الأمر في مستقبل الأيام بتفريد هذه التقنيات بنصوصها الخاصة، لاسيما في هذا الجانب المتعلق بمعالجة بيانات الأشخاص وعدم استغلالها أو انتهاكها. فالقائمين على الهجمات السيبرانية يمكنهم هنا وضع حواجز افتراضية في عمليات التداول الرقمي لهذه البيانات بين المستفيدين والمعنيين فيها، بمعنى أن عملية الهجمات السيبرانية قد تجد الآليات القانونية والبرمجية في توظيف وتصنيف هذه البيانات بين المتاح وغير المتاح، بين المشفر وغير المشفر، وذلك بحسب المتعاملين مع هذه البيانات في البيئة الرقمية، بين مبرمج ومصنع، ومرد ومشتري، ومستهلك [٩]، وهذا ما أكده القرار الأوربي المتعلق بالإنسالة لسنة 2017، ونظيره المتعلق بالسياسة الصناعية الأوربية المتعلقة الهجمات السيبرانية والانسالات لسنة 2019، بحيث أكدوا على احترام مبدأ الشفافية في التعامل مع أي من البيانات التي تستخدم في الذكاء الاصطناعي. ليقترح هذا القرار الأوربي المتعلق بالربوتات اقتراحاً مفاده أن يكون في كل مسألة ما يمكن تسميته ب "العلبة السوداء"، التي تحتوي على جميع المعلومات المتعلقة بالبيانات المخزنة لديه الآليات اللوغاريتمية التي تم استخدامها في عملية المعالجة السمعية لهذه البيانات، وصولا الى والآليات اللوغاريتمية التي تم استخدامها في عملية المعالجة البرمجية لهذه البيانات، وصولا إلى العمل على وضع إطار قانوني مرجعي لتعامل أنترنت الأشياء مع مختلف هذه البيانات والحفاظ على طابع السرية والأمان في مختلف هذه البيانات، بما يضمن الوصول لمنتجات آمنة ومأمونة ومتكيفة مع الاستخدام المقصود بها[١٠]وحسب القانون المدني للروبوتات الصادر عن الاتحاد الأوربي سنة 2017 يجب أن تنفذ على جميع أنواع الهجمات السيبرانية معايير الخصوصية، والتي من المحتمل فيها أن تتعامل مع معلومات بيانات شخصية حساسة، ويتم تصميمها وتجهيزها بأجهزة وأنظمة برامج لتشفير البيانات الخاصة وتخزينها بشكل أمن مع الأخذ بعين الاعتبار أن إتلاف تلك البيانات من شأنه

أن يلحق ضررا قابلا للتعويض، مما يساعد معها على إضفاء طابع حماني على البيانات الشخصية وفي حالة عدم احترام هذه الضوابط السالفة الذكر في الهجمات السيبرانية سيؤدي مما لا شك فيه إلى التأثير بشكل سلبي على الأشخاص، وستلحق بهم أضراراً جسيمة، لكون أن الوسيلة الأساسية لتطوره تقوم بالدرجة الأولى على تغذيته من هذه البيانات الشخصية(١١)

الفرع الثاني:- تأثير الهجمات السيبرانية على حق احترام الكيان المعنوي للفرد

إن حماية الانسان في كيانه المعنوي هي من الحقوق الأساسية التي بدونها لا يكون الانسان آمناً وحراً في حياته، وهي تتناول بشكل رئيسي احترام كرامته. فالكرامة الانسانية هي جوهر الكيان المعنوي لكل انسان لأنها تبدأ حتى قبل ولادته ولا تنتهي بوفاته، والحرمان التعسفي من الحياة لا يقتصر على فعل القتل المحظور، وإنما يتعداه ليشمل الحرمان من الحق في العيش بكرامة، و "لا يمكن وال يجوز تقسيم كرامة الفرد، إلى مجالين – مجال مدني وسياسي، ومجال اقتصادي واجتماعي وثقافي. إذ يجب أن يتمتع الفرد بالتحرر من العوز والخوف. ولا يمكن تحقيق الهدف النهائي المتمثل في ضمان احترام كرامة الفرد، إلا إذا تمتع بجميع حقوقه(١٢)كتب الفقيه الفرنسي "أرثر ميلر Arthur Mullor" ، أن الكومبيوتر بشراهته لجمع المعلومات على نحو لا يمكن وضع حد لها، وما يتصف به من دقة ومن عدم نسيان ما يخزن فيه، قد يحول حياتنا رأسا على عقب، يخضع فيها الأفراد لنظام رقابة صارم ويتحول المجتمع بذلك إلى عالم شفاف تصبح فيه بيوتنا ومعاملاتنا المالية وحياتنا العقلية والجسمانية عارية لأي مشاهد"، ولو كان يدرك "ميلر" ما ستؤول إليه فتوحات عصر المعلومات، وما سيتحقق في بيئة شبكات المعلومات العالمية والعالم الافتراضي الإلكتروني، لأدرك ما قاله أصبح يسيراً على التقنيات الجديدة التي أضحت تجمع شتات المعلومات عن كل فرد من أفراد المجتمع وتنظيمها وتحليلها، وهو ما قد يؤدي لا محالة فيه إلى خرق الخصوصية من خلال استغلالها ونشرها حيث تستعمل لغايات غير مشروعة أو لا أخلاقية(١٣)فقد أصبح كيان الأفراد المعنوي ومن ضمنه خصوصيتهم في إطار التطور التكنولوجي معرضا للاختراق والانتهاك بمعنى أن فكرة المساس بالخصوصية المادية البيانات أو المعطيات الشخصية قد تم تجاوزها لتمس وتستنتج بواعث وميول الإنسان، وبالتالي تمس كيان الأفراد المعنوي، لتصبح في النهاية إمكانية انتهاك الحياة الخاصة للأفراد أكثر سهولة من ذي قبل وأكبر مجالًا، أي المساس بواحد من أعرق الحقوق المخولة للإنسان والمنصوص عليها قانونًاويعتبر حق الشخص في احترام كيانه المعنوي سابقاً لعصر انتشار النظم الصناعية من خلال حق الفرد في حماية البيئة الخاصة به، إلا أنه في ظل تطور الهجمات السيبرانية وسهولة انتهاك هذا الحق أصبحت حماية كيان الأفراد ضرورة ملحة سواء من خلال الاتفاقيات الدولية أو الإقليمية، فتنامي تقنيات الهجمات السيبرانية سيؤدي إلى التغلغل أكثر في خصوصيات الأفراد على نحو سيصبح فيه العديد من مظاهر هذه الخصوصية صيداً سهلًا لغير أصحابها (١٤) ويظهر جلياً أن مسألة انتهاك الحق في الكيان المعنوي قد تسود في العديد من المجالات، غير أنه لا نذهب بعيدا بل يمكننا تسليط الضوء عما مر به العالم جراء انتشار فيروس كورونا المستجد المسمى Covid 19-، حيث إن أغلب الدول سنت مجموعة من التدابير الاستباقية التي تقوم بتتبع وتعقب المواطنين أينما حلوا كالتطبيقات الذكية، زد على ذلك قامت بتسخير إنسان الى يقوم بتشخيص حالات المصابين بالفيروس فهل ستوفر الدول الحماية الكافية لاستخدام تقنيات ضد الهجمات السيبرانية دون أن تؤدي للمساس بخصوصيات الأفراد من خلال النصوص القانونية قد عملت الدول على إنشاء تطبيقات ذكية تسهم في القضاء على انتشار العدوى، يتبين لنا، أنه بالرغم من قيام الدول بإنشاء تطبيقات ذكية تستجيب لحاجيات المجتمع من أجل الحفاظ على سلامته ومنع انتشار فيروس كورونا المستجد، وحتى إن أكدت هذه الدول على جدية هذه التطبيقات الذكية، وأنها لا تنتهك خصوصية مستخدميها، إلا أنها في نهاية المطاف تبقى مسألة مفترضة، ولا يمكن القول على إن حماية الخصوصية هي قائمة في حد ذاتها، بل إن المعطيات التي يتم تجميعها في هذه التطبيقات وجعلها في سجلات إلكترونية تحتوي على جميع المعلومات المتعلقة بالمريض، والتي من شأن الهجمات السيبرانية أن يستخدمها ويدعم بها اتخاذ قراراته وهو ما يتضح من خلال إشعاره للمخالطين مع المصاب، وهذا سيؤدي إلى نفي حماية الخصوصية ويكون فيه خطورة على هذه الأخيرة، إذا ما تم استغلالها في مسائل غير مشروعة(١٥)وغير بعيد عن المجال الطبي، فإن التطور التكنولوجي أضحى أمرا لا غنى عنه والأفراد لم يعودوا بمعزل عن التكنولوجيا، وأينما تواجدنا نسخر التكنولوجيا، ونخص هنا بالذكر خوارزميات الفيس بوك Facebook، التي تعد من بين تقنيات الذكاء الاصطناعي، فكل فرد لا يستطيع استخدامها أو الدخول لها إلا بعد القيام بالاشتراك فيه.فالاشتراك في تطبيق الفايسبوك يتطلب من المشترك ضرورة الإفصاح عن بعض البيانات ذات الطبيعة الشخصية وثيقة الصلة بخصوصية صاحبها، ولذلك من المؤكد أن هذه البيانات أو الكثير منها على الأقل أصبح متوفراً بحوزة شركات الدعاية التجارية ومواقعها الإلكترونية المخصصة لذلك، وهو ما يتضح من خلال العديد من محتوياتها الإعلانية التي لا تحترم لا الآداب ولا الأخلاق العامة، لما فيها من معروضات خادشه بالحياء (١٦)وفي خضم هذه النقطة يمكن القول إن الحق في الكيان المعنوي هو من أهم الحقوق التي لابد على كل التشريعات حمايتها من أي اختراق واعتداء أو انتهاك خصوصاً في الجانب المتعلق

بالحماية من تقنيات الهجمات السيبرانية التي تعد مجالًا خصباً للتطور بفعل التزايد السريع للتكنولوجيا، مما يوجب معه حماية كبرى لحقوق الأفراد سواء تعلق الأمر بمعطياتهم الشخصية أو حياتهم الخاصة.وهذا يعني أنه بالرغم من تطرق التشريعات لتنظيم الحق في الكيان المعنوي وحمايته من أي انتهاك قد يتعرض له، إلا أن هذا التنظيم للحق من الضروري حمايته ضد هذه الهجمات، فإنه بالمقابل موازاة مع خصوصيات هذه التقنيات تفرض على المشرع أن يعزز هذا الحق بحماية أكثر مما هي عليه الآن، لكون أن الهجمات السيبرانية هو مجال دقيق، وأن مجرد خطأ بسيط سيصبح الشخص عاريًا ومكشوفا للجميع، وستصبح حياته الخاصة متاحة للجميع، الأمر الذي يفرض إصدار نصوص قانونية أكثر حماية لهذا الحق، حتى يتمكن أي مستخدم لهذه التقنيات استخدامها باطمئنان[١٧]إن تقنيات الهجمات السيبرانية تختلف تماما عن الأخطار الأخرى من ناحية تأثيرها على حقوق والتعامل معها في ظل القواعد العامة، مما يستوجب إما تعديل القوانين الحالية وتحيينها أو استصدار قوانين التقنيات الذكية بشكل كبير وسيتم الاعتماد عليها في جميع المعاملات اليومية للأفراد. وما تجب الإشارة إليه هنا، أن خوارزميات الهجمات السيبرانية لا تنتهك فقط حقوق الإنسان بل حتى حريات الأفراد قد تلحقها انتهاكات من جراء استخدام هذه التقنيات، كحرية التصرف أو الاختيار، ذلك أن رغباتنا قد تكون موجهة للقيام بعمل معين وتحقيقه، لكن خوارزميات الذكاء الاصطناعي تقوم بالتصرف مكاننا دون الحاجة من تدخلنا أو أن تسمح لنا بالفرصة في الاختيار، كون التقنيات الذكية لا نجد فيها ضميرا إنسانيا مما يوحي تماما أن حرية الضمير هي الأخرى ستنتهك إذا ما تم اعتماد هذه الخوارزميات.وعليه فإن الهجمات السيبرانية تعتبر تهديداً متزايداً على الحقوق المدنية في العالم الرقمي المتزايد الاعتماد عليه، مما يجعل الحاجة ملحة لتطوير سياسات وتشريعات لحماية هذه الحقوق. فتؤثر الهجمات السيبرانية بشكل كبير على الحقوق المدنية، حيث تؤدي إلى انتهاك خصوصية الأفراد وسرقة معلوماتهم الشخصية. فمن خلال اختراق قواعد البيانات والشبكات، يمكن للمهاجمين الوصول إلى معلومات حساسة مثل البيانات الطبية والمالية والشخصية، مما يعرض حقوق الأفراد للخطر. بالإضافة إلى ذلك، تؤثر الهجمات السيبرانية على حق الإنسان في احترام كيانه المعنوي، وتؤدي الهجمات السيبرانية إلى تشويش حياة الأفراد والتدخل في شؤونهم الشخصية، ويمكن للهجمات السيبرانية أن تؤثر بشكل كبير على حرية الأفراد وقدرتهم على التعبير عن آرائهم وأفكارهم بحرية، حيث قد يشعرون بالقلق من تعرض بياناتهم للاختراق والاستخدام ضدهم. وهو ما نتناوله تالياً.

المطلب الثاني:- تأثير الهجمات السيبرانية على حقوق الإنسان الرقمية

تعد الهجمات السيبرانية أحد التحديات الرئيسية التي تواجه حقوق الرقمية في العصر الحديث، فمع تزايد استخدام التكنولوجيا والتحول نحو الحياة الرقمية، أصبحت البيانات والمعلومات الحساسة أكثر عرضة للاختراق والاستغلال، وتشمل الهجمات السيبرانية جميع الأنشطة غير المشروعة التي تستهدف الأنظمة الإلكترونية والشبكات والبيانات بهدف التسبب في أضرار مالية أو تعطيل الخدمات أو سرقة المعلومات، حيث تتسبب الهجمات السيبرانية في تأثيرات سلبية على حقوق الرقمية بشكل كبير، حيث تؤدي إلى خرق الخصوصية والسرية وسرقة البيانات الشخصية والمالية للأفراد والمؤسسات، كما يمكن أن تؤدي هذه الهجمات إلى تعطيل الخدمات الرقمية التي يعتمد عليها المستخدمون في حياتهم اليومية، مثل الخدمات المصرفية عبر الإنترنت والتجارة الإلكترونية والاتصالات[١٨]بالإضافة إلى ذلك، قد تؤدي الهجمات السيبرانية إلى تشويش التواصل الرقمي وانتشار المعلومات غير الصحيحة والتضليل الشخصية والمالية للأفراد والمؤسسات، كما يمكن أن تؤدي هذه الهجمات إلى تعطيل الخدمات الرقمية التي يعتمد عليها المستخدمون في حياتهم اليومية، مثل الخدمات المصرفية عبر الإنترنت والتجارة الإلكترونية والاتصالات[١٩]بالإضافة إلى ذلك، قد تؤدي الهجمات السيبرانية إلى تشويش التواصل الرقمي وانتشار المعلومات غير الصحيحة والتضليل الشخصية والمالية للأفراد والمؤسسات، كما يمكن أن تؤدي هذه الهجمات إلى تعطيل الخدمات الرقمية التي يعتمد عليها المستخدمون في حياتهم اليومية، مثل الخدمات المصرفية عبر الإنترنت والتجارة الإلكترونية والاتصالات[٢٠]بالإضافة إلى ذلك، قد تؤدي الهجمات السيبرانية إلى تشويش التواصل الرقمي وانتشار المعلومات غير الصحيحة والتضليل، مما يؤثر سلباً على حقوق الاطلاع والحصول على معلومات دقيقة وموثوقة.وبناء على ما سبق سنبحث في فرعين ندرس في الفرع الاول انتهاك الخصوصية الرقمية و الحق في الوصول إلى المعلومات ونخصص الفرع الثاني لدراسة التلاعب بالهوية الرقمية وكما يأتي.

الفرع الأول:- انتهاك الخصوصية الرقمية و الحق في الوصول إلى المعلومات

ان الهجمات السيبرانية والحقوق الرقمية تشكل تحديًا كبيراً في عصرنا الحالي، حيث أصبحت التكنولوجيا جزءاً أساسياً من حياة الأفراد والمؤسسات على حد سواء، وتعتبر الهجمات السيبرانية من أخطر التهديدات التي تواجه العالم الرقمي، حيث يمكن أن تتسبب في خسائر مالية هائلة وتأثيرات سلبية على سمعة الشركات والأفراد ومن الآثار الرئيسية للهجمات السيبرانية على اهم هذه الحقوق هي كالآتي:

اولاً:-انتهاك الخصوصية الرقميةإن الهجمات السيبرانية غالباً ما تستهدف البيانات الشخصية الحساسة، مثل معلومات الهوية، الحسابات المصرفية، أو السجلات الصحية، هذا يؤدي إلى انتهاك الحق في الخصوصية، حيث تُستخدم البيانات الشخصية بشكل غير مشروع، مثل بيعها أو استخدامها للابتزاز أو الاحتيال، حيث تعد انتهاكات الخصوصية الرقمية من خلال الهجمات السيبرانية أمراً يستحق الاهتمام والتوعية، حيث تشير الإحصائيات إلى ازدياد حالات اختراق البيانات وسرقة المعلومات الشخصية عبر الإنترنت بشكل ملحوظ وتعد هذه الانتهاكات تهديدًا خطيرًا على الأفراد والمؤسسات على حد سواء[٢١]يمكن أن تشمل الهجمات السيبرانية اختراق قواعد البيانات، واستخدام برامج خبيثة لسرقة المعلومات الحساسة، والاحتيال الإلكتروني، والتجسس على البيانات، وقد تؤدي هذه الهجمات إلى تسرب معلومات شخصية حساسة مثل البيانات المالية، والمعلومات الطبية، والمعلومات الشخصية الأخرى التي يمكن استخدامها في أنشطة احتيالية، بالإضافة إلى ذلك يمكن أن تؤدي الهجمات السيبرانية إلى تعطيل خدمات الإنترنت وأنظمة المعلومات، مما يؤثر على سير العمل في المؤسسات ويتسبب في خسائر مالية كبيرة، وبالتالي فإن حماية الخصوصية الرقمية أصبحت ضرورة ملحة لضمان سلامة المعلومات والبيانات[٢٢]ولحماية الخصوصية الرقمية، يجب على الأفراد والمؤسسات اتخاذ تدابير أمنية فعالة مثل استخدام كلمات مرور قوية، وتحديث برامج الحماية، وتشفير المعلومات الحساسة. كما يجب تعزيز التوعية حول مخاطر الهجمات السيبرانية وكيفية التعامل معها بشكل صحيح، ففي نهاية المطاف، يجب أن تكون مكافحة انتهاكات الخصوصية الرقمية من خلال الهجمات السيبرانية أولوية قصوى لضمان سلامة المعلومات والحفاظ على الثقة في بيئة الإنترنت[٢٣].

ثانياً:- الحق في الوصول إلى المعلومات تقوم الهجمات السيبرانية بتعطل الوصول إلى الخدمات الرقمية مثل مواقع الحكومة أو منصات التعليم أو وسائل الإعلام، وهذا يؤثر على الحق في الحصول على المعلومات والخدمات الضرورية، وخاصة في الأوقات الحرجة، كما تعتبر الحصول على المعلومات الخاصة بالهجمات السيبرانية من هلال الحقوق الأساسية للأفراد والمؤسسات، وتقوم بضمان سلامة البيانات والمعلومات الحساسة. ومع ذلك، قد يتم تعطيل هذا الحق من خلال عدة وسائل، مثل استخدام التكنولوجيا لحجب الوصول إلى المعلومات أو تقييد الحريات الشخصية على الإنترنت [٢٤]وتعتبر الهجمات السيبرانية وسيلة فعالة لتعطيل حق الوصول إلى المعلومات، حيث يمكن للمهاجمين استخدام البرامج الضارة والاختراقات لتعطيل أنظمة الاتصال ومنع الوصول إلى المواقع والبيانات، وبالتالي يمكن أن تؤدي هذه الهجمات إلى تقييد حرية التعبير وحق الوصول إلى المعلومات، ولحماية حق الوصول إلى المعلومات من خلال الهجمات السيبرانية، يجب اتخاذ تدابير أمنية فعالة، مثل تطبيق بروتوكولات الأمان واستخدام برامج مضادة للاختراق. كما يجب تعزيز التوعية بأهمية الحفاظ على سلامة البيانات وتعزيز الثقافة الرقمية الآمنة بين جميع المستخدمين [٢٥]بالإضافة إلى ذلك، يجب على الحكومات والجهات ذات الصلة اتخاذ التدابير اللازمة لضمان حرية الوصول إلى المعلومات وحمايتها من الهجمات السيبرانية، وينبغي أن تكون هناك قوانين وسياسات فعالة تحدد المسؤوليات والإجراءات الواجب اتخاذها لحماية المعلومات وضمان حق الوصول إليها، وفي الختام يجب أن ندرك أهمية حق الوصول إلى المعلومات كحق أساسي، ونعمل على تعزيز الأمان السيبراني وحماية البيانات من التهديدات المختلفة. حيث يساهم ذلك في تعزيز حرية التعبير وضمان سلامة المعلومات للأفراد والمؤسسات على حد سواء.

الفرع الثاني:- التلاعب بالهوية الرقمية تعد سرقة الهوية من خلال الهجمات السيبرانية أحد أخطر التهديدات التي تواجه الأفراد والمؤسسات في العصر الحديث، فمن خلال استخدام تقنيات متطورة، يقوم المهاجمون بالاستيلاء على معلومات شخصية حساسة مثل الأسماء، والعناوين، وأرقام الضمان الاجتماعي، والمعلومات المصرفية، وغيرها من البيانات الهامة التي يمكن استخدامها في عمليات احتيالية وسرقة الأموال.

تتضمن أساليب سرقة الهوية السيبرانية عدة تقنيات مثل الاحتيال الإلكتروني، والبرمجيات الخبيثة، والتصيد الإلكتروني، واختراق قواعد البيانات، والاختراقات اللاسلكية، والهجمات على شبكات التواصل الاجتماعي. كما يمكن للمهاجمين استخدام تقنيات الهندسة الاجتماعية لاستدراج الأفراد إلى كشف المعلومات الخاصة بهم بطرق غير مشروعة [٢٦]، لحماية أنفسهم ومؤسساتهم من هذه التهديدات، يجب على الأفراد والشركات اتخاذ إجراءات أمان متقدمة يشمل ذلك استخدام برامج مضادة للاختراق وتحديثها بانتظام، وتشفير المعلومات الحساسة، وتبني سياسات قوية لإدارة الهوية والوصول، وتوعية الموظفين حول مخاطر سرقة الهوية وكيفية التعامل معها.بالإضافة إلى ذلك، يجب على المؤسسات تطبيق إجراءات رصد واستجابة فورية للاشتباه في حالات سرقة الهوية، بما في ذلك إجراء تحقيقات دقيقة وإبلاغ الجهات المعنية، كما ينبغي للأفراد أن يكونوا حذرين في التعامل مع المعلومات الشخصية على الإنترنت وتجنب مشاركتها مع أطراف غير موثوق بهاكما إن الأفراد يفقدون السيطرة على معلوماتهم الشخصية عندما يتم سرقتها أو التلاعب بها، مما يؤثر على حقهم في إدارة هويتهم الرقمية وحمايتها، عد التحكم بالمعلومات الشخصية من خلال الهجمات السيبرانية أمرًا بالغ الأهمية في عصرنا الحالي، حيث تتزايد حالات اختراق البيانات وسرقتها بشكل مستمر يتطلب الأمر تبني

استراتيجيات وسياسات فعالة لحماية البيانات الشخصية للأفراد والشركات من تلك الهجمات. يجب أن تكون هذه الاستراتيجيات مبنية على أحدث التقنيات والأساليب الأمنية، مع مراعاة الامتثال للقوانين والتشريعات المتعلقة بحماية البيانات الشخصية [٢٧]وتعد تقنيات التشفير والحماية من البرمجيات الخبيثة والتحقق المتعدد العوامل من بين الوسائل الفعالة للحماية ضد الهجمات السيبرانية، كما يجب على الأفراد والمؤسسات توعية الموظفين والعملاء بأهمية حماية البيانات الشخصية وتبني ممارسات أمنية سليمة. بالإضافة إلى ذلك، يجب على الشركات والمؤسسات إجراء تقييم دوري للضعف في نظام الأمان السيبراني واتخاذ التدابير اللازمة لتعزيزه.لا يمكن تجاهل أهمية التحكم بالمعلومات الشخصية في ظل تزايد التهديدات السيبرانية، ولذلك يجب على كافة الأطراف اتخاذ الإجراءات الضرورية لحماية هذه البيانات من خلال تبني استراتيجيات أمنية قوية وتوعية جميع السيبرانية والحفاظ على سلامة المعلومات الأطراف بأهمية حماية البيانات، يمكن تقليل مخاطر الهجمات الشخصي[٢٨]

الخاتمة

اولا:- الاستنتاجات

١- مع التقدم التكنولوجي اصبحت الهجمات السيبرانية تشكل تهديد حقيقيا على الأفراد والمؤسسات, والذي اثر بشكل مباشر على الحقوق المدنية والرقمية.

٢- ان من أخطر التهديدات التي تواجه الأفراد والمؤسسات في العصر الحديث، هي سرقة الهوية من خلال الهجمات السيبرانية وتتم من خلال استخدام تقنيات متطورة، اذ يقوم المهاجمون بالاستيلاء على المعلومات الشخصية الحساسة مثل(الأسماء، والعناوين، أرقام الضمان الاجتماعي، المعلومات المصرفية)، وغيرها من البيانات الهامة التي يتم استخدامها في عمليات الاحتيال وسرقة الأموال.

٣- تؤدي الهجمات السيبرانية الى انتهاكات خطيرة لخصوصية الافراد كاختراق البيانات الشخصية والمعلومات واستغلالها في عمليات الاحتيال والابتزاز, كما يمكن للمهاجمين استخدام البرامج الضارة والاختراقات لتعطيل أنظمة الاتصال ومنع الوصول إلى المواقع والبيانات.

٤-هناك تفاوت بين الدول في مستوى الحماية مما يؤدي الى وجود ثغرات قانونية يستغلها المخترقون.

ثانيا:- التوصيات

١-ضرورة تعزيز التعاون الدولي لمكافحة الهجمات السيبرانية من خلال اتخاذ تدابير أمنية فعالة، كتطبيق بروتوكولات الأمان واستخدام برامج مضادة للاختراق, كما يجب تعزيز التوعية بأهمية الحفاظ على سلامة البيانات وتعزيز الثقافة الرقمية الآمنة بين جميع المستخدمين.

٢- قيام الدول بوضع استراتيجيات قانونية وأمنية اكثر صرامة وتطوير القوانين لحماية حقوق الافراد والمؤسسات من مخاطر الهجمات السيبرانية ووضع عقوبات رادعة للمخترقين .

٣- انشاء مؤسسات خاصة لمراقبة وحماية البني التحتية الرقمية والعمل على معالجة الاختراقات بسرعة, وفرض سياسات واضحة للشركات الرقمية حول كيفية التخزين والاستخدام لبيانات المستخدمين.

قائمة المصادر والمراجع

أولا: الكتب.

.سماء حسين مكاوي، اخلاقيات التواصل في العصر الرقمي، هبرماس انموذجاً، المركز العربي للأبحاث ودراسة السياسات، بيروت، 2017.

١- اسلام هديب، الأمن السيبراني الهجمات السيبرانية والجرائم السيبرانية، دار مصر للنشر والتوزيع، مصر، 2024.

٢- سليم عبد الله الجبوري، الحماية القانونية لمعلومات شبكة الأنترنت، منشورات الحلبي الحقوقية، لبنان، 2011.

٣- عادل موسى عوض جاب الله، وسائل حماية الأمن السيبراني دراسة فقهية تأصيلية مقارنة بالنظم المعاصرة، كلية الشريعة والدراسات الإسلامية، مصر، 2022.

٤- عاطف عباس عبد الحميد، جرائم تقنية المعلومات وحقوق الملكية الفكرية، المؤسسة العربية للعلوم والثقافة، مصر، 2022.

٥- عبد الفتاح بيومي حجازي، الجرائم المستحدثة في نطاق تكنلوجيا الاتصالات الحديثة، المركز القومي للإصدارات القانونية، القاهرة،2011.

٦- علي حسن الطوالبة، أبحاث في جرائم تقنية المعلومات، دار الكتب العربية، الأردن، 2018، ص85. (2) قانون حماية البيانات والحريات الفرنسي رقم 152 لعام 2020.

٧- علي عبود جعفر، جرائم تكنولوجيا المعلومات الواقعة على الأشخاص والحكومة، ط1، منشورات زين الحقوقية، بيروت، 2013.

٨- علي نعمة جواد الزرفي، الجريمة المعلوماتية الماسة بالحياة الخاصة دراسة مقارنة، المكتب الجامعي الحديث، القاهرة، 2019.

٩- عمار عباس الحسيني، جرائم الحاسوب والإنترنت، منشورات الحلبي الحقوقية، بيروت، 2019.

١٠- ماجد عزيز إسكندر، التوظيف السياسي للهجمات السيبرانيَّة ومخاطرها على الأمن القومي، ط1، مركز الإمارات للدراسات والبحوث الاستراتيجية، 2023.

١١- محمود بري، السيبرانية علم القدرة على التواصل والتحكم والسيطرة، المركز الإسلامي للدراسات الاستراتيجية، ط 1، بيروت – لبنان، 2019.

١٢- محمود رجب فتح الله، شرح قانون مكافحة جرائم تقنية المعلومات وفقاً للقانون المصري الحديث، دار الجامعة الجديدة، مصر، 2019.

ثانيا: الابحاث والمجلات.

١-بلعسل بنت نبي ياسمين، الحق في الخصوصية الرقمية، مجلة المستقبل للدراسات القانونية والسياسية، العدد1، المجلد 5، مصر، 2021.

٢-توبي مندل وآخرون، دراسة استقصائية عالمية حول خصوصية الانترنت وحرية التعبير، منظمة الأمم المتحدة للتربية والتعليم والثقافة، فرنسا، 2012.

٣-حازم محمد خليل، استغلال الفضاء السيبراني في الحروب غير التقليدية: دراسة في الوكالة السيبرانية والإرهاب السيبراني، المجلة العلمية لكلية الدراسات الاقتصادية والعلوم السياسية، المقالة 7، المجلد 8، العدد 15، يناير 2023.

٤-خالد وليد محمود، الهجمات عبر الانترنت ساحة الصراع الالكتروني الجديدة، المركز العربي للأبحاث ودراسة السياسات، الدوحة،2013.

٥-عمر محمد عمر، الحرب الإلكترونية في القانون الدولي الإنساني، مجلة دراسات علوم الشريعة والقانون، المجلد 46، عدد 3، 2019.

٦-محمد عرفان الخطيب، الذكاء الاصطناعي والقانون، دراسة نقدية في التشريعين المدني والقطري في ضوء القواعد الأوروبية في القانون المدني للإنسالة، مجلة الدراسات القانونية، قطر، 2020.

رابعا: المواقع الالكترونية.

١- أحمد عنتر، تقنيات الأمن السيبراني والتحديات المستقبلية، مقال منشور على موقع الجزيرة الإخباري، متاح على الرابط الإلكتروني :الزيارة تاريخ ،https://www.aljazeera.net/tech/2023/12/4

٢-منظمة العفو الدولية، حقوق الإنسان من أجل كرامة الإنسان، مطبوعات منظمة العفو الدولية، 2014، متاح على الرابط الإلكتروني: ' https://www.amnesty.org/en/wp-content/uploads /sites/9/2021 /06 /pol300012014ar.pdf

خامسا: الرسائل والاطاريح

١- حمام عبد اللطيف عبد الشافي حنفي معوض، الحماية الجنائية للبرامج والبيانات المعالجة الكترونياً دراسة مقارنة، أطروحة قدمت لنيل درجة الدكتوراة، جامعة القاهرة، 2017.

سادساً: المراجع الاجنبية.

(1) Babkak akhgar , Andrew staFrancesccrandcyberrinvestigator shandbook , by , elsevvier ,use, 2014 , p201.

هوامش البحث

(١) سماء حسين مكاوي، اخلاقيات التواصل في العصر الرقمي، هبرماس انموذجاً، المركز العربي للأبحاث ودراسة السياسات، بيروت، 2017،ص90

(٢) عادل موسى عوض جاب الله، وسائل حماية الأمن السيبراني دراسة فقهية تأصيلية مقارنة بالنظم المعاصرة، كلية الشريعة والدراسات الإسلامية، مصر، 2022، ص98.

(٣) علي حسن الطوالبة، أبحاث في جرائم تقنية المعلومات، دار الكتب العربية، الأردن، 2018، ص85. (2) قانون حماية البيانات والحريات الفرنسي رقم 152 لعام 2020.

(٤) علي عبود جعفر، جرائم تكنولوجيا المعلومات الواقعة على الأشخاص والحكومة، ط1، منشورات زين الحقوقية، بيروت، 2013، ص92.

(٥) محمد عرفان الخطيب، الذكاء الاصطناعي والقانون، دراسة نقدية في التشريعين المدني والقطري في ضوء القواعد الأوروبية في القانون المدني للإنسالة، مجلة الدراسات القانونية، قطر، 2020، ص20.

(٦) علي نعمة جواد الزرفي، الجريمة المعلوماتية الماسة بالحياة الخاصة دراسة مقارنة، المكتب الجامعي الحديث، القاهرة، 2019، ص120.

(٧) محمود رجب فتح الله، شرح قانون مكافحة جرائم تقنية المعلومات وفقاً للقانون المصري الحديث، دار الجامعة الجديدة، مصر، 2019،.ص65

(٨) أحمد عنتر، تقنيات الأمن السيبراني والتحديات المستقبلية، مقال منشور على موقع الجزيرة الإخباري، متاح على الرابط الإلكتروني :الزيارة تاريخ ،https://www.aljazeera.net/tech/2023/12/4

(٩) ماجد عزيز إسكندر، التوظيف السياسي للهجمات السيبرانيَّة ومخاطرها على الأمن القومي، ط1، مركز الإمارات للدراسات والبحوث الاستراتيجية، 2023، ص55.

(١٠) اسلام هديب، الأمن السيبراني الهجمات السيبرانية والجرائم السيبرانية، دار مصر للنشر والتوزيع، مصر، 2024، ص100.

(١١) عادل موسى عوض جاب الله، وسائل حماية الأمن السيبراني دراسة فقهية تأصيلية مقارنة بالنظم المعاصرة، مرجع سابق، ص105.

(١٢) منظمة العفو الدولية، حقوق الإنسان من أجل كرامة الإنسان، مطبوعات منظمة العفو الدولية، 2014، متاح على الرابط الإلكتروني: ' https://www.amnesty.org/en/wp-content/uploads /sites/9/2021 /06 /pol300012014ar.pdf

(١٣) سماء حسين مكاوي، اخلاقيات التواصل في العصر الرقمي، هبرماس انموذجاً، مرجع سابق، ص93.

(١٤) اسلام هديب، الأمن السيبراني الهجمات السيبرانية والجرائم السيبرانية، مرجع سابق، ص103.

(١٥) عمر محمد عمر، الحرب الإلكترونية في القانون الدولي الإنساني، مجلة دراسات علوم الشريعة والقانون، المجلد 46، عدد 3، 2019،ص63.

(١٦) عمار عباس الحسيني، جرائم الحاسوب والإنترنت، منشورات الحلبي الحقوقية، بيروت، 2019، ص79.

(١٧) توبي مندل وآخرون، دراسة استقصائية عالمية حول خصوصية الانترنت وحرية التعبير، منظمة الأمم المتحدة للتربية والتعليم والثقافة، فرنسا، 2012، ص65.

(١٨) حازم محمد خليل، استغلال الفضاء السيبراني في الحروب غير التقليدية: دراسة في الوكالة السيبرانية والإرهاب السيبراني، المجلة العلمية لكلية الدراسات الاقتصادية والعلوم السياسية، المقالة 7، المجلد 8، العدد 15، يناير 2023، ص50.

(١٩) حازم محمد خليل، استغلال الفضاء السيبراني في الحروب غير التقليدية: دراسة في الوكالة السيبرانية والإرهاب السيبراني، المجلة العلمية لكلية الدراسات الاقتصادية والعلوم السياسية، المقالة 7، المجلد 8، العدد 15، يناير 2023، ص50.

(٢٠) حازم محمد خليل، استغلال الفضاء السيبراني في الحروب غير التقليدية: دراسة في الوكالة السيبرانية والإرهاب السيبراني، المجلة العلمية لكلية الدراسات الاقتصادية والعلوم السياسية، المقالة 7، المجلد 8، العدد 15، يناير 2023، ص50.

(٢١) بلعسل بنت نبي ياسمين، الحق في الخصوصية الرقمية، مجلة المستقبل للدراسات القانونية والسياسية، العدد1، المجلد 5، مصر، 2021،.ص250

(٢٢) عبد الفتاح بيومي حجازي، الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة، المركز القومي للإصدارات القانونية، القاهرة،2011.

(٢٣) محمود بري، السيبرانية علم القدرة على التواصل والتحكم والسيطرة، المركز الإسلامي للدراسات الاستراتيجية، ط 1، ، 2019، ص59.

(24) Babkak akhgar , Andrew staFrancesccrandcyberrinvestigator shandbook , by , elsevvier ,use, p201.

(٢٥) عاطف عباس عبد الحميد، جرائم تقنية المعلومات وحقوق الملكية الفكرية، المؤسسة العربية للعلوم والثقافة، مصر، 2022، ص59.

(٢٦) سليم عبد الله الجبوري، الحماية القانونية لمعلومات شبكة الأنترنت، منشورات الحلبي الحقوقية، لبنان، 2011، ص69.

(٢٧) خالد وليد محمود، الهجمات عبر الانترنت ساحة الصراع الالكتروني الجديدة، المركز العربي للأبحاث ودراسة السياسات، الدوحة،2013، ص55.

(٢٨) حمام عبد اللطيف عبد الشافي حنفي معوض، الحماية الجنائية للبرامج والبيانات المعالجة الكترونياً دراسة مقارنة، أطروحة قدمت لنيل درجة الدكتوراة، جامعة القاهرة، 2017، ص155.