تأثير الفضاء السيبراني على مبدأ سيادة احكام القانون في إطار القانون الدستوري

م.د. كريم زيدان خلف
جامعة كركوك - كلية القانون والعلوم السياسية

The impact of cyberspace on the principle of the rule of law within the framework of constitutional law

Mr.Dr.Kareem Zaidan Khalaf
University of Kirkuk-College of Law and Political science

المستخلص: يتناول هذا البحث تأثير الفضاء السيبراني على مبدأ سيادة أحكام القانون في إطار القانون الدستوري، عبر تحليل التحديات القانونية الناشئة عن الطبيعة العالمية للفضاء السيبراني. يناقش البحث كيفية تأثير الفضاء السيبراني على الأنظمة القانونية المختلفة، مع التركيز على حماية البيانات الشخصية والخصوصية، والاختصاص القضائي في النزاعات ذات العنصر الأجنبي. يستعمل البحث المنهج الوصفي لتحليل مفهوم الفضاء السيبراني وخصائصه، فضلاً عن المنهج المقارن لدراسة كيفية تعامل الأنظمة القانونية مع هذه التحديات. يقدم البحث توصيات لتعزيز الأطر القانونية وضمان حماية حقوق الأفراد والدول في الفضاء السيبراني، مع التركيز على أهمية التعاون الدولي وتوحيد القوانين لمواجهة التحديات السيبرانية بفعالية. **الكلمات المفتاحية:** الامن، الدستور، السيادة.

Abstract: This research explores the impact of cyberspace on the principle of the rule of law in sovereign states by analyzing the legal challenges arising from the global nature of cyberspace. The study discusses how cyberspace affects different legal systems, focusing on data protection, privacy, and jurisdiction in disputes involving foreign elements. It employs a descriptive approach to analyze the concept and characteristics of cyberspace, alongside a comparative method to examine how various legal systems address these challenges. The research offers recommendations to enhance legal frameworks and ensure the protection of individuals' and states' rights in cyberspace, emphasizing the importance of international cooperation and legal

harmonization to effectively tackle cyber challenges. **Keywords:** security, constitution, sovereignty.

المقدمة

لقد أصبح الفضاء السيبراني، مع تطور التكنولوجيا الرقمية وانتشار الإنترنت، جزءًا لا يتجزأ من حياتنا اليومية، إذ أثر بشكل كبير على مختلف جوانب الحياة بما في ذلك الجوانب القانونية. يتمتع الفضاء السيبراني بخصائص فريدة، مثل الطابع العالمي، والسرعة الفائقة في نقل المعلومات، والقدرة على إخفاء الهوية، مما يثير تساؤلات حول كيفية تطبيق وتنفيذ القوانين التقليدية في هذا المجال الافتراضي. يشكل الفضاء السيبراني تحديًا كبيرًا لمبدأ سيادة أحكام القانون، إذ إن الطبيعة العابرة للحدود للإنترنت تُعقّد تنفيذ القوانين الوطنية والدولية. يمكن للأنشطة السيبرانية، مثل الجريمة الإلكترونية والاحتيال والقرصنة، أن تنشأ في دولة وتؤثر على أفراد أو مؤسسات في دولة أخرى، مما يثير تساؤلات حول الولاية القضائية وتطبيق القانون. تتطلب حماية البيانات الشخصية والخصوصية في الفضاء السيبراني تكييف التشريعات التقليدية لتتوافق مع التهديدات السيبرانية الحديثة، وهذا يفرض على الدول التعاون لتوحيد الجهود القانونية والتنظيمية. فضلاً عن ذلك، تواجه الحكومات تحديات في فرض سيادة القانون في الفضاء السيبراني بسبب الافتقار إلى حدود واضحة وتعريفات دقيقة للجرائم السيبرانية. يؤدي هذا إلى اختلافات في كيفية تعامل الدول مع هذه الجرائم، مما يعزز من مشكلة الإفلات من العقاب. تبرز الحاجة إلى تطوير اتفاقيات دولية وقوانين موحدة لمكافحة الجرائم السيبرانية بفعالية. تُعتبر التهديدات السيبرانية للأمن القومي وتزايد الاعتماد على البنية التحتية الرقمية من العوامل التي تضغط على الحكومات لتعزيز تشريعاتها السيبرانية. تُظهر الهجمات السيبرانية على البنية التحتية الحيوية مثل شبكات الكهرباء والمياه والاتصالات أن تأثير الفضاء السيبراني على سيادة أحكام القانون يتجاوز الحدود التقليدية، مما يتطلب استجابة قانونية مرنة ومتعددة الأطراف.

أهمية البحث: تتجلى أهمية هذا البحث في الكشف عن التحديات التي يفرضها الفضاء السيبراني على مبدأ سيادة أحكام القانون، وهو مبدأ جوهري لضمان العدالة والحفاظ على النظام القانوني. يعتبر فهم هذه التحديات ضروريًا لتطوير أطر قانونية تتناسب مع الواقع الرقمي الجديد وتحافظ على حقوق الأفراد والدول في الفضاء السيبراني. يهدف البحث إلى تحليل تأثير الفضاء السيبراني على سيادة القانون، واقتراح حلول قانونية مبتكرة لمواجهة هذه التحديات.

مشكلة البحث: مشكلة هذا البحث تتمحور حول السؤال التالي: كيف يؤثر الفضاء السيبراني على مبدأ سيادة أحكام القانون في الدول ذات السيادة؟

منهجية البحث: يعتمد هذا البحث على المنهج الوصفي للفضاء السيبراني ومحاولة تحديد أبرز خصائصه. بالإضافة إلى ذلك، سيتم استخدام المنهج المقارن لمقارنة كيفية تعامل الأنظمة القانونية المختلفة مع التحديات القانونية سيادة القانون في الفضاء السيبراني.

هيكلية البحث: المبحث الأول: الإطار المفاهيمي للفضاء السيبراني. المطلب الأول: تعريف الفضاء السيبراني. المطلب الثاني: خصائص الفضاء السيبراني. المبحث الثاني: التحديات القانونية لمبدأ سيادة القانون في الفضاء السيبراني. المطلب الأول: التحديات المتعلقة بالاختصاص القضائي. المطلب الثاني: التحديات المرتبطة بحماية البيانات الشخصية في الفضاء السيبراني.

المبحث الأول: الإطار المفاهيمي للفضاء السيبراني

يعد الفضاء السيبراني من أكثر المفاهيم حداثة وتعقيداً في عصرنا الرقمي، حيث يشير إلى البيئة الافتراضية التي تنشأ من تفاعل الشبكات الرقمية وتكنولوجيا المعلومات والاتصالات. يتشابك هذا الفضاء الافتراضي مع عالمنا المادي بشكل معقد، مما يخلق تأثيرات متبادلة ومتشابكة بين العالمين. تكتسب دراسة الفضاء السيبراني أهمية متزايدة في ظل الاعتماد المتزايد على الإنترنت والتكنولوجيا الرقمية في مختلف جوانب الحياة، من الاقتصاد إلى الأمن الوطني. تتضمن الأطر المفاهيمية للفضاء السيبراني تحليل الأبعاد التقنية والاجتماعية والسياسية

والقانونية لهذا الفضاء، وكيفية تأثيرها على الأفراد والمجتمعات والدول. يهدف هذا المبحث إلى تقديم فهم شامل للإطار المفاهيمي للفضاء السيبراني، من خلال تسليط الضوء على تعريف الفضاء السيبراني ومحاولة التعرف على أبرز خصائصه وذلك من خلال المطلبين التاليين.

المطلب الأول: تعريف الفضاء السيبراني

الفضاء السيبراني هو بيئة إلكترونية غير ملموسة تتسم بتفاعلات معقدة، حيث يتم بناء نماذج وصور إلكترونية لظواهر تشبه الواقع من خلال التفاعلات البعيدة. تُعرف "السَّيْبَرة" كعملية انعكاسية نشطة تعكس مدخلات التفاعلات الإلكترونية في بيئة غير مدركة للإنسان. بعبارة أخرى، هو شبكة إلكترونية لمجموعة من الخوادم الإلكترونية التي تتفاعل مع بعضها باستخدام وسائل تواصل افتراضية، متجاوزة الحواجز الجغرافية والسياسية، بهدف تحسين قدرة الاتصال والتعامل الإلكتروني. تمثل هذه البيئة عادةً محاكاة حاسوبية في صورة بيئة افتراضية لمستخدمي العالم الافتراضي. يعرف البعض الفضاء السيبراني كعالم افتراضي يتشابك مع العالم المادي، يتأثر به ويؤثر فيه بشكل معقد، حيث تتكامل العلاقتان بين العالمين وتحتوي على مزايا ومخاطر مستمرة. وُصف الفضاء السيبراني أيضًا بالذراع الرابعة للجيوش الحديثة بجانب القوات البرية والبحرية والجوية، حيث يشهد الإنترنت معارك حقيقية في هذا العالم الافتراضي. يعتبر البعض الفضاء السيبراني البعد الخامس للحرب، ويُعرف أيضًا بالمجال المادي وغير المادي الذي يتكون من أجهزة الكمبيوتر والشبكات والبرمجيات والمعلومات والمحتوى ومعطيات النقل والتحكم ومستخدمي هذه العناصر. تُعد هذه العناصر العامل المشترك في جميع استخدامات الفضاء السيبراني، سواء كانت الجهات المستخدمة تسعى لتعظيم قيمها وقدراتها ورفع كفاءة العنصر البشري أو كانت في مرحلة متأخرة[1]. يمكن تعريف الفضاء السيبراني أيضًا كحيز سوسيو–مكاني نتج عن دمج التكنولوجيات الوسائطية والإنترنت ضمن مصفوفة تشابكية، تتيح إنتاج وتبادل مختلف أشكال البيانات والمضامين النصية والسمعية والبصرية والتفاعل بين

[1] – شريفة كلاع: الأمن السيبراني وتحديات الجوسسة والاختراقات الإلكترونية للدول عبر الفضاء السيبراني، مج١٥، ع١، مجلة الحقوق والعلوم الإنسانية، جامعة زيان عشور الجلفة، الجزائر، ٢٠٢٢، ص٢٩٤.

المستخدمين بطرق محكومة بأطر الواقع الاجتماعي وثقافته ورموزه التداولية. هذا التعريف يركز على البعد الفني للفضاء السيبراني من خلال انتفاء مفهومي الزمان والمكان، ويبرز البعد السوسيو–ثقافي لمستخدميه من أفراد مجتمع المعرفة المعلوماتية، ضمن حدود افتراضية لا يمكن تأمينها إلا بتدخل تكنولوجيا المعلومات وامتلاك أدوات المعرفة الرقمية. يمكن القول أيضًا إن الفضاء السيبراني هو مصطلح حديث ظهر نتيجة الثورة الرقمية، ويشمل جميع الحواسيب والمعلومات التي تحتويها والأنظمة والبرامج والشبكات المفتوحة للجمهور العام، بالإضافة إلى تلك الشبكات المصممة لاستخدام فئة محددة من المستعملين والمنفصلة عن شبكة الإنترنت العامة[١]، أي أن الفضاء السيبراني هو المجال المادي وغير المادي الذي يتكون وينتج عن عناصر تشمل: أجهزة الكمبيوتر، الشبكات، البرمجيات، حوسبة المعلومات، المحتوى، معطيات النقل والتحكم، ومستخدمي كل هذه العناصر. تعرف وزارة الدفاع الأمريكية الفضاء السيبراني بأنه "مجال يتسم باستخدام الإلكترونيات، أي تكنولوجيا المعلومات، والطيف الكهرومغناطيسي في تخزين البيانات وتعديلها وتبادلها عن طريق أنظمة الشبكات والاتصال والبنية التحتية المادية المرتبطة بها." بناءً على هذا التعريف، تعمل الكيانات المدنية والعسكرية والإرهابية في الفضاء السيبراني لتنفيذ أنشطتها وعملياتها[٢].

كما عرّفته الوكالة الفرنسية لأمن أنظمة الإعلام (ANSSI)، وهي وكالة حكومية مكلفة بالدفاع السيبراني الفرنسي، بأنه فضاء تواصل يتكون من الربط البيني العالمي لمعدات معالجة البيانات الرقمية[٣]. كما عرف بعض الباحثين مصطلح الفضاء السيبراني بأنه عالم افتراضي يتشابك مع العالم المادي، حيث يتأثر به ويؤثر فيه بشكل معقد، اذ كانت الصراعات سابقا سواء الاقليمية او الدولية تدار على ارض الواقع ، الا انه بتقدم التكنلوجيا الحديثة بدأت العلاقة بين العالمين

[١] – د. دلالي جيلالي و د. بلبشير يعقوب: رهانات الأمن السيبراني الوطني في ظل التحول الرقمي، مجلة كلية القانون الكويتية العالمية–السنة العاشرة–العدد١–العدد التسلسلي ٣٧–ربيع الثاني/جمادى الأولى١٤٤٣هـ–ديسمبر ٢٠٢١، ص٥٣٠–٥٣٢.

[٢] – شريفة كلاع، مصدر سابق، ص٢٩٤.

[٣] – د. دلالي جيلالي و د. بلبشير يعقوب، مصدر سابق، ص٥٣١.

تقوم على نظرة تكاملية تحمل مزايا ومخاطر مستمرة[١]، وهناك من وصفه بالذراع الرابعة للجيوش الحديثة بجانب القوات الجوية والبحرية والبرية، خاصة مع ظهور معارك حقيقية تدور في هذا العالم الافتراضي منذ بداية الحديث عن الإنترنت[٢]. شكلت هذه المعارك نمطاً جديداً من التهديدات والمخاطر والنزاعات غير التقليدية، مما أثر بشكل كبير في تغيير مفاهيم الصراع والقوة والسيادة. يمكن استنتاج أن التعريفات المختلفة للفضاء السيبراني تطورت عبر تراكم معرفي، منتقلة من منطلقات تقنية بحتة إلى ربطه بمفاهيم متعددة التخصصات ذات أبعاد سوسيولوجية، سياسية، وأمنية. ومع ذلك، لم تبتعد هذه التعريفات كثيراً عن مفهوم الفضاء المعلوماتي، خاصة عند رسم معالم وحدود هذا الفضاء ومكوناته.

المطلب الثاني: خصائص الفضاء السيبراني

الفضاء السيبراني هو مجال افتراضي من صنع الإنسان يعتمد على شبكات الإنترنت وأنظمة الكمبيوتر، بالإضافة إلى كم هائل من الأجهزة والمعلومات والبيانات. يمكن اعتباره ذراعًا للجيوش الحديثة، وهناك من يرى أنه البعد الأساسي للحرب الحديثة، لذا أصبح أحد المؤثرات الأساسية في النظام الدولي. رخص التكلفة وسهولة الاستخدام زادا من قدرته على التأثير في المجالات السياسية والاقتصادية والعسكرية. إن من يمتلك آليات التحكم في الفضاء السيبراني يصبح أكثر قدرة على التأثير في سلوك الآخرين لتحقيق الأهداف المرجوة[٣]. لكن هناك عدد من الخصائص والعناصر للفضاء السيبراني تميزه عن الفضاء العام التقليدي، إذ أصبح يشكل

[١] – د. صدام مرير حمد الجميلي، الحروب الهجينة واثرها في مستقبل الصراع العالمي، مجلة تكريت للعلوم السياسية،المجلد(١)، العدد(٣٤)، ٢٠٢٤، ص ١١٢.

[٢] – عباس بدران: الحرب الإلكترونية الاشتباك في عالم المعلومات، مركز دراسات الحكومة الإلكترونية، بيروت، لبنان، ٢٠١٠، ص ٤

[٣] – اسراء شريف جيجان وصفا عباس فاضل: تأثير الفضاء السيبراني على الحروب الحديثة، ع٦٥، مجلة دراسات تربوية، وزارة التربية العراقية، ٢٠٢٤، ص٣٣١.

الفضاء السيبراني ساحة جديدة للحرب بشكله التقليدي ولكنه ذا طابع سيبراني، والحروب السيبرانية تقع داخل شبكات الاتصال والمعلومات عابرة للحدود التقليدية وسيادة الدول، على الرغم من أن الحرب الفعلية تستعمل جميع أنواع الأسلحة المتاحة، فأنها لم تتوان عن استخدام الفضاء السيبراني. يمكن تلخيص سمات وخصائص عدة للفضاء السيبراني والحروب السيبرانية على النحو الآتي:

١- **الحرية وغياب السيطرة الحكومية:** يتيح الفضاء السيبراني للأفراد والجماعات فرصًا أوسع للتواصل والتفاعل وبناء مجتمعات افتراضية بطرق متنوعة، مما يمكنهم من التأثير في القضايا عبر وسائل التواصل الاجتماعي والمنتديات الإلكترونية وغيرها، اضف الى ذلك ان معظم قضايا الارهاب المعاصرة التي حققت وتحقق فيها المحاكم الجنائية اثبتت استخدام الجناة للانترنت كوسيلة لوضع الخطط والحصول على المعلومات وتحقيق التواصل بين الجناة ومعرفة مواعيد تنفيذ مخططاتهم بدقة متناهية[١].، تتميز هذه القدرة عن المجال العام التقليدي، حيث تفرض الأنظمة السلطوية قيودًا صارمة على عملية التنظيم التي قد يقدم عليها الأفراد والجماعات[٢]. وبسبب هذه الخصيصة، فإن الاعتداءات التي تتم في الفضاء السيبراني تتجاوز الحدود الإقليمية بسهولة؛ إذ يمكن شنها دون مواجهة أي عقبات طبيعية أو جغرافية، وضد أي عدو بغض النظر عن موقعه الجغرافي مقارنة بدولة الهجوم، ودون الاعتبار لميزان القوة العسكرية بين الدولتين. كما أن الأثر المترتب على الحرب السيبرانية غير

[١] – د. راجي يوسف محمود البياتي، الارهاب السيبراني(نماذج من الجهود الدولية للحد منه)، مجلة تكريت للعلوم السياسية، المجلد (٢)، العدد(٢٨)، ٢٠٢٢، ص١٠٤.

[٢] – محمد اكرم محسن ود. مروان سالم علي: السيبرانية "الماهية–الخصائص–الفواعل–الابعاد الاستراتيجية"، ع٤٣، س١١، مجلة حمورابي للدراسات، ٢٠٢٢، ص٣٩١.

محدود، حيث يمكن أن تتسبب في أضرار للأهداف العسكرية أو المدنية، سواء كانت أهدافًا معلنة أو استخباراتية، وقد تطال المنشآت الحيوية في الدولة[١].

٢- **الطبيعة الطوعية وليس الجبرية:** هذه الخاصية ممتدة من المجال العام التقليدي إلى السيبراني، لكنها اتسعت في المجال السيبراني، بل أيضاً تفسر الإقبال الشديد عليه خصوصاً بأنه خال من الإجبار الذي يعانيه المواطن في العديد من مجالات حياته اليومية، خاصةً في علاقته بالدولة والقوانين، هذا ما يُساعد على خلق ساحة صراع جديدة بين الدول يتشارك فيها المدنيين والعسكريين وترتبط بالتطورات المادية والعسكرية على الارض بأقل تكلفة وأكثر تحديداً للهدف[٢].

٣- **صعوبة الردع السيبراني:** يُعرّف "الردع السيبراني" بأنه منع الأعمال الضارة ضد الأصول الوطنية في الفضاء السيبراني. على الرغم من التعريف الدقيق لهذا المفهوم، فإنه يرتبط ارتباطًا وثيقًا بسياسات القوى الكبرى والأبعاد الأمنية للفضاء السيبراني. فعلى سبيل المثال، تُفضل الولايات المتحدة استخدام مصطلح "الأمن السيبراني" (Cyber Security) للتركيز على التكنولوجيات، والشبكات، والأجهزة الآلية، في حين تفضل كل من الصين وروسيا استخدام مصطلح أوسع هو "أمن المعلومات" (Information Security)، ليشمل المعلومات التي تمر عبر الشبكات وكذلك التقنيات المعلوماتية. يؤثر هذا التباين بشكل جذري في مفهوم الردع السيبراني، إذ أن عدم الاتفاق على المصطلحات الرئيسية يؤدي إلى جدل حول كيفية استخدام الإنترنت، وطبيعة الهجمات السيبرانية التي يجب ردعها، واستراتيجيات الردع وسبل تحقيقه. ومع ذلك، تُقدم اتفاقية "الجريمة السيبرانية" (Convention on Cybercrime) لعام ٢٠٠١ إطارًا يمكن التوافق من خلاله على مصطلحات الجريمة

[١] – إسلام رمضان هديب: مفهوم الحرب السيبرانية في ظل القانون الدولي وتحديد خصائصها والنتائج المترتبة عليها، مج٣٦، ع١، مجلة البحوث القانونية والاقتصادية، كلية الحقوق جامعة بنى سويف، ٢٠٢٤، ص١١٨.

[٢] – محمد اكرم محسن ود. مروان سالم علي، مصدر سابق، ص٣٩١.

والردع السيبراني من قبل جميع الدول الموقِّعة، البالغ عددها ٤١ دولة. ومن الجدير بالذكر أن روسيا لم تُصدِّق على الاتفاقية، بينما لم تنضم الصين إليها، بعد أن رفضت المصطلحات التي وافقت عليها الدول الغربية.[١].

٤- **غياب الشفافية وقابلية الانكار**: من الصعب تحديد هوية المجموعة التي تنفذ الهجمات السيبرانية في العديد من الحالات، بالإضافة إلى غياب التشريعات الدولية التي تُخضع الدول أو المؤسسات أو الجماعات التي تقوم بمثل هذه الأنشطة للمساءلة بموجب القانون الدولي، مما يجعل من الصعب ملاحقتهم قانونيًا مقارنة بمجالات الحرب التقليدية. تشير "القابلية للإنكار" إلى صعوبة تيقن الدول من هوية الطرف المهاجم، إذ تتسم الحروب السيبرانية بطبيعة خاصة حيث تُشن الهجمات دون إعلان أي طرف عن مسؤوليته. لذا، في معظم الحالات، يصعب تحديد مصدر الهجوم. ويلاحظ أن إنكار أو إخفاء هوية المجموعة التي تقف وراء الهجوم السيبراني يتم أحيانًا تضمينه في البرامج المستخدمة في الهجوم. فعلى سبيل المثال، برنامج "ستاكس نت" الذي استخدم في مهاجمة أجهزة الطرد المركزي الإيرانية، كان مبرمجًا بحيث يمتلك القدرة على محو آثاره بشكل ذاتي، مما حال دون تحديد ومعرفة هوية الطرف المهاجم حتى بعد رصد وتحليل إيران لفيروس "ستاكس نت". كما أصبح من الصعب على الدول التمييز بين الهجمات التي تشنها الدول وتلك التي تشنها الجماعات الإجرامية بناءً على طبيعة الهجوم. ففي الماضي، كانت العصابات السيبرانية توظف برامج الفدية للحصول على أموال بصورة غير مشروعة، بدلاً من جمع المعلومات

[١] – د. رغدة البهي: الردع السيبراني: المفهوم والاشكاليات، المركز المصري للفكر والدراسات الاستراتيجية، مقال منشور على الرابط التالي: https://ecss.com.eg/6203/ (٢٠٢٤/٦/٣).

الاستخباراتية أو التسبب في أضرار عبر السيطرة على أنظمة التحكم الصناعية، وهي النوعية من الهجمات التي عادة ما تتورط فيها الجماعات السيبرانية المرتبطة بالدول[1].

المبحث الثاني: التحديات الدستورية لمبدأ سيادة القانون في الفضاء السيبراني

تشمل التحديات القانونية في الفضاء السيبراني مجموعة معقدة من القضايا الناشئة عن الطبيعة العالمية والتفاعلية للإنترنت. أحد أبرز هذه التحديات هو حماية البيانات الشخصية وخصوصية المستخدمين في ظل التزايد المستمر للاختراقات الأمنية والهجمات السيبرانية. بالإضافة إلى ذلك، تواجه الحكومات صعوبة في وضع وتطبيق قوانين تنظيمية متسقة عبر الحدود الدولية، مما يعقد عملية مكافحة الجريمة الإلكترونية والاختصاص القضائي.

المطلب الأول: التحديات المتعلقة بالاختصاص القضائي في الفضاء السيبراني

قد تنشأ عن العلاقة القانونية ذات العنصر الأجنبي مسألة عرضية تتمثل في نشوء نزاع يتعلق بتلك العلاقة، مما يستدعي تحديد المحكمة المختصة بالفصل فيه. يؤدي هذا إلى خلاف بين محاكم عدة دول، حيث تدعي كل منها حق النظر في النزاع والبت في العلاقة القانونية، وهو ما يعرف بتنازع الاختصاص. يختلف تنازع الاختصاص عن تنازع القوانين، حيث لا يظهر الأخير إلا عند نشوء نزاع بين أطراف العلاقة القانونية بعد قيامها. وهذه حالة عرضية لا تحدث في جميع الحالات، ولكن عند حدوثها يجب اللجوء إلى محكمة ذات ولاية للنظر في النزاع. مسألة تنازع الاختصاص التي تلي نشوء العلاقة القانونية تتطلب قواعد قانونية تحدد ما إذا كانت المنازعة تدخل ضمن ولاية محاكم دولة القاضي المرفوع أمامه النزاع أم لا. الفصل في اختصاص المحكمة يجب أن يسبق تحديد القانون الواجب التطبيق، حيث يبت القاضي بدايةً في اختصاصه. تُعتبر قواعد تنازع الاختصاص من وضع المشرع الوطني، الذي يحدد

[1] – د. شادي عبد الوهاب: السيناريو الكارثي: متى تتحول الحرب السيبرانية إلى حرب شاملة؟، المستقبل للأبحاث والدراسات المتقدمة، مقال متاح على الرابط التالي: https://futureuae.com/ar-AE/Mainpage/Item/6992 (٢٠٢٤/٦/٣).

اختصاص المحاكم الوطنية ويحدد بصورة غير مباشرة اختصاص المحاكم الأجنبية عند تخليه عن هذا الاختصاص. في كل دولة، يرسم المشرع قواعد الاختصاص القضائي للمحاكم الوطنية سواء كان هذا الاختصاص داخلياً أو دولياً. يتم تحديد الاختصاص الداخلي وفق قواعد المرافعات المدنية، أما الاختصاص الدولي للعلاقات القانونية ذات العنصر الأجنبي فيتحدد بموجب قواعد الاختصاص الدولي، التي تحدد اختصاص المحاكم الوطنية بالمنازعات المتعلقة بالعلاقات القانونية ذات العنصر الأجنبي[١]. على الرغم من التصنيف الصحيح للفضاء السيبراني كمجتمع عالمي، واعتباره من الناحية القانونية مجتمعا مشتركا، لا يخضع لسيادة دولة واحدة أو مجموعة دول، ونظرا لخصائصه بوصفه محصنا من الاستيلاء، فإن ممارسات الدول تقدم أدلة كافية على أن الفضاء السيبراني، أو بالأحرى مكوناته، ليست محصنة ضد السيادة ومن ممارسة الولاية القضائية. ومع ذلك، فإن الإنترنت وشبكات الكمبيوتر لها مواقع مادية تحت الولاية القضائية الإقليمية لدولة واحدة أو أكثر، والجهات الفاعلة فيه لديها جنسية بغض النظر عما إذا كانوا أفرادا أو شركات. فمن ناحية، لقد مارست الدول وستواصل ممارسة ولايتها القضائية الجنائية فيما يتعلق بالجرائم السيبرانية، وتواصل تنظيم الأنشطة في الفضاء السيبراني. ومن ناحية أخرى، من المهم أن نأخذ في الاعتبار أن الفضاء السيبراني يتطلب وجود بنية مادية. وعادة ما تكون المعدات المعنية موجودة داخل أراضي الدولة مملوكة من قبل الحكومة أو من قبل الشركات. في هذا الصدد لا يمكن تفسير دمج المكونات المادية، أي البنية التحتية الإلكترونية الموجودة داخل أراضي الدولة، في "المجال العالمي" للفضاء الإلكتروني بأنه تنازل عن ممارسة السيادة الإقليمية. وفي ضوء البنية الحقيقية للفضاء السيبراني قد يكون من الصعب ممارسة السيادة. ومع ذلك، فإن المشاكل التقنية التي ينطوي عليها الأمر لا تمنع الدولة من ممارسة سيادتها، ولاسيما سلطتها القضائية الجنائية، على البنية التحتية السيبرانية الواقعة في

[١] – حسن الهداوي: القانون الدولي الخاص: تنازع القوانين، المبادئ العامة والحلول الوضعية في القانون الأردني، دار الثقافة للنشر والتوزيع، عمان، ١٩٩٥، ص٢٣٣.

المناطق التي تغطيها سيادتها الإقليمية[1]. فيما يتعلق بالتحديات القانونية، يواجه تطبيق القوانين السيبرانية العديد من العقبات نظرًا للتعقيدات الفنية والجغرافية التي تنطوي عليها الجرائم السيبرانية. إذ يمكن أن تتم هذه الجرائم عبر الحدود، مما يجعل من الصعب تحديد الولاية القانونية المسؤولة عن معاقبة الجناة. بالإضافة إلى ذلك، قد تكون التشريعات الحالية غير كافية لمواجهة التحديات الحديثة في مجال الأمن السيبراني، وتحتاج إلى تحديث دوري لمواكبة التطورات التكنولوجية وأنماط الهجمات الجديدة. ففيما يتعلق بالاختصاص القضائي يصعب تحديد الولاية القضائية في الجرائم السيبرانية، خاصة عندما تتم عبر الحدود الوطنية. اما فيما يتصل بقوانين مكافحة الجرائم السيبرانية تختلف قوانين مكافحة الجرائم السيبرانية بين الدول، مما يُعيق التعاون الدولي في مكافحة هذه الجرائم[2].

بشكل عام، تؤثر الهجمات السيبرانية على مبدأ سيادة أحكام القانون من خلال زيادة التحديات الأمنية والتكنولوجية التي تواجهها الحكومات والمؤسسات القانونية، مما يتطلب تكيفًا مستمرًا وتحديثات للتشريعات والسياسات الأمنية. الهجمات السيبرانية على الأنظمة القضائية يمكن أن تؤدي إلى تعطيل العمليات القضائية، بما في ذلك تسجيل القضايا، وإدارة الجلسات، وحفظ السجلات. هذا يعيق سير العدالة ويؤدي إلى تأخير في البت في القضايا. كما ان الهجمات السيبرانية على نظم الانتخابات يمكن أن تؤثر على نتائج الانتخابات وتضعف ثقة الجمهور في العمليات الديمقراطية. هذا يهدد مبدأ سيادة القانون من خلال التأثير على شرعية الحكومة المنتخبة. مما تقدم يظهر للباحث ان الاختصاص القضائي يمثل واحدة من أبرز التحديات في الفضاء السيبراني. يتعين على السلطات القانونية تحديد أي نظام قانوني يجب أن يُطبّق على الأنشطة السيبرانية التي تمتد عبر حدود متعددة. قد تنشأ نزاعات بين الدول حول من يمتلك

[1] – علاء الدين فرحات وعمارة عمروس: الفضاء السيبراني وتأكل مفهوم السيادة الوطنية، مج٨، ع٢، المجلة الجزائرية للدراسات السياسية، الجزائر، ٢٠٢١، ص١٧٦-١٧٧.

[2] – باقر كريم سالم: التحديات الأخلاقية والقانونية في مجال الأمن السيبراني، مقالة علمية، متاح على الرابط التالي: https://uomus.edu.iq/NewCol.aspx?newid=24796 (٢٠٢٤/٧/٣).

الحق في محاكمة المتهمين، خصوصًا إذا كانت الجرائم تؤثر على عدة دول. هذا يستدعي وجود اتفاقيات دولية واضحة وتعاون مشترك لتحديد الاختصاص القضائي المناسب.

المطلب الثاني: التحديات المرتبطة بحماية البيانات الشخصية في الفضاء السيبراني: يعد الفقيه (آلان ويستون) من أوائل الفقهاء الأمريكيين الذين عنوا بحماية البيانات الشخصية، وقام بتعريف خصوصية البيانات عام ١٩٦٧، في مؤلفه الخصوصية والحرية، بأنها حق الفرد في تحديد متى وكيف وإلى أي مدى تصل البيانات الخاصة به إلى الآخرين. بينما عرفها الفقيه (ميلر) في مؤلفه عام ١٩٧١ بعنوان (الإعتداء على الخصوصية)، بأنها: قدرة الفرد في التحكم في دورة المعلومات المتعلقة به، أي حق الفرد في منع الآخرين من الإطلاع أو التصرف في المعلومات المتعلقة بحياته الخاصة. فيما عرف المشرع المصري البيانات الشخصية في المادة (١) من الفصل الأول من القانون الخاص بحماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠، وعرفها بأنها: أي بيانات متعلقة بشخص طبيعي محدد أو يمكن تحديده بشكل مباشر أو غير مباشر عن طريق الربط بين هذه البيانات وأي بيانات أخرى، كالإسم أو الصوت أو الصورة، أو رقم تعريفي أو محدد للهوية عبر الإنترنت أو أى بيانات تحدد الهوية النفسية أو الصحية أو الإقتصادية أو الثقافية أو الإجتماعية[١]. أما الدستور العراقي لسنة ٢٠٠٥ لم يرد فيه الحق في حماية البيانات الشخصية بصورة صريحة في الدستور انما تناول بالتنظيم الحق ضمنا عندما تناول الحق في الخصوصية بموجب المادة ١٧ (أن لكل فرد كفالة الحق في الخصوصية الشخصية، بما لا يتنافى مع حقوق الآخرين والآداب العامة)، كما نجد أن الحق ورد ضمنا عندما نضم الدستور في المادة (٤٠) حرية الإفراد في الاتصالات والمراسلات البريدية والبرقية والهاتفية والالكترونية وغيرها، كما نص لا يجوز مراقبتها أو التصنت عليها، الا لضرورة امنية وبقرار قضائي. نجد من النصوص السابقة أن المشرع الدستوري تناول حق الخصوصية بنص صريح وهذا النص تضمن الاعتراف بصورة ضمنية بالحق بحماية البيانات الشخصية باعتبار أن حق حماية البيانات الشخصية أحد صور الحق في الخصوصية، كما كفل الدستور حرية

[١] – د. هبه رمضان رجب: الحماية القانونية للبيانات الشخصية في عصر التكنلوجيا الرقمية، مج ٦٦، ع٣، مجلة العلوم القانونية والاقتصادية، كلية الحقوق جامعة عين شمس، ٢٠٢٤، ص٤٢٣.

المراسلات البريدية والبرقية والهاتفية والالكترونية بصورة صريحة بالنص الدستوري، وتعتبر المراسلات البرقية والهاتفية والالكترونية من البيانات الشخصية، وهنا نجد على المشرع الدستوري العراقي إضافة نص يخص حق حماية البيانات الشخصية أسوة بحقوق الإنسان الأخرى وذلك لإضفاء الحماية الدستورية على البيانات الشخصية، إذ يكون النص الدستوري يكون أساسا قانونيا لحماية الحق وهنا يقع على المشرع الدستوري التنظيم القانوني للحق؛ وذلك لمعالجة الانتهاكات التي تقع على البيانات الشخصية[١]. تعد تكنولوجيا تقنية المعلومات الحديثة نظاماً نشأ من اندماج نظم المعلومات بنظم الاتصال وما نتج عنها من شبكات، واصبحت حماية البيانات الشخصية على الانترنت من أهم الحقوق الفردية للمستخدمين، للحفاظ على الخصوصية، والبيانات الشخصية: هي جميع المعلومات المتعلقة بالشخص، سواء كانت متعلقة بالحياة الخاصة، او المهنية ضمن بيئة الإنترنت، وان الحماية القانونية لحرمة الحياة الخاصة، في عصر تقنية المعلومات الحديثة شهدت تطوراً كبيراً في نطاقها[٢]. ومما يتبين للباحث ان الهجمات السيبرانية قد تؤدي إلى سرقة الملكية الفكرية والأسرار التجارية، مما يؤثر سلبًا على الشركات وقدرتها على حماية ابتكاراتها. هذا يشكل تحديًا قانونيًا كبيرًا فيما يتعلق بحماية الحقوق والابتكارات. كما يمكن ان تؤدي الهجمات السيبرانية التي تستهدف البيانات الشخصية إلى انتهاكات خطيرة لخصوصية الأفراد وحقوقهم الرقمية. هذا يثير قضايا قانونية معقدة حول حماية البيانات وحقوق الخصوصية.

أن البيانات الشخصية تكون عرضة لمخاطر حتمية في ظل غياب قانون يحميهم ويحمي خصوصيتهم ولاسيما في غياب تشريع ينظم حماية حق بيانات الافراد، وبالتالي مراعاة خصوصيتهم ويمنع إساءة استخدامها أو استغلالها؛ اذ ينظم القانون عمليات جمع وحفظ المعلومات الشخصية باستخدام الحاسوب وغيره من الوسائل، سواء اكانت تجربها السلطات

[١] – شميم مزهر راضي: الحق في حماية البيانات الشخصية في ظل دستور جمهورية العراق لسنة ٢٠٠٥، ع٤، كانون الأول، مجلة جامعة الامام جعفر الصادق (ع) للدراسات القانونية، ٢٠٢٢، ص١٦٣.

[٢] – القاضي كاظم عبد جاسم الزيدي: الحماية القانونية للبيانات الشخصية في القانون العراقي، مقالة منشورة على الرابط التالي: https://dcc-iq.com/?p=41826 (٢٠٢٤/٦/٣).

العامة أو الافراد في أيدي الأشخاص الذين لا يجيز لهم القانون الحصول عليها أو تجهيزها أو استخدامها، أن الحياة الرقمية يترتب عليها العديد من المشكلات فمشكلة استغلال البيانات الشخصية من قبل الغير وانتشار الجرائم الالكترونية تتطلب تنظيم قانوني لحماية الحق، حيث يضع الحق في حماية البيانات الشخصية التزامات أساسية على الإفراد والجهات التي تحوز البيانات سواء أكانت خاصة أم عامة من ناحية الحيازة والتحكم طبقا للغرض المحدد لها، ولضمان الحق لابد من إجراءات تشريعية تحدد ما يجب من إجراءات في حال انتهاك حقوقهم كما تحدد التزامات الأطراف الحائزة للبيانات[١]. يظهر للباحث هنا انه مع تزايد حجم البيانات المتبادلة والمخزنة في الفضاء السيبراني، أصبح الحفاظ على الخصوصية وحماية البيانات الشخصية تحديًا كبيرًا. القوانين المتعلقة بالخصوصية تختلف من دولة لأخرى، مما يخلق تعقيدات في حماية حقوق المستخدمين على مستوى عالمي. هناك حاجة ماسة لتطوير أطر قانونية موحدة أو متناسقة تضمن حماية فعالة للبيانات الشخصية وتعزز الثقة في الاستخدام الآمن للفضاء السيبراني.

الخاتمة: لقد تناول هذا البحث تأثير الفضاء السيبراني على مبدأ سيادة أحكام القانون في إطار القانون الدستوري، وذلك من خلال تحليل التحديات القانونية التي تفرضها الطبيعة العالمية والمعقدة لهذا الفضاء. استعرضنا من خلال البحث الأطر القانونية الحالية وكيفية تعاملها مع قضايا حماية البيانات والخصوصية، بالإضافة إلى الاختصاص القضائي في النزاعات العابرة للحدود. ولقد توصلنا في ختام هذا البحث الى مجموعة من الاستنتاجات والتوصيات وهي التالية:

الاستنتاجات:

١. يشكل الفضاء السيبراني تحديًا جوهريًا لمبدأ سيادة القانون بسبب عدم وجود حدود جغرافية واضحة، مما يؤدي إلى صعوبات في تطبيق القوانين الوطنية.

[١] – شميم مزهر راضي، مصدر سابق، ص١٦٤.

٢. يوجد تباين كبير بين الدول في كيفية تعاملها مع الجرائم السيبرانية وحماية البيانات، مما يزيد من تعقيد النزاعات القانونية عبر الحدود.

٣. تظهر الحاجة الملحة للتعاون الدولي في مجال التشريعات السيبرانية لضمان تطبيق فعال للقانون وحماية حقوق الأفراد والدول.

٤. يتطلب التطور السريع في التكنولوجيا تحديثًا مستمرًا للأطر القانونية لضمان ملاءمتها للتحديات الجديدة.

٥. يلعب المجتمع المدني دورًا هامًا في تعزيز السياسات القانونية والسيبرانية من خلال المشاركة في الحوار والمناصرة.

التوصيات:

١. العمل على تحديث القوانين بشكل دوري لمواكبة التطورات التكنولوجية والهجمات السيبرانية الجديدة.

٢. تأمين البنية التحتية الحيوية من خلال تعزيز نظم الأمان واعتماد تقنيات المراقبة والتقييم المستمر.

٣. يجب على السلطات تحسين قدراتها في التحقيقات السيبرانية من خلال تدريب متخصصين واستخدام أدوات وتقنيات متقدمة لتتبع الجناة.

٤. إطلاق حملات توعية للجمهور حول أهمية الأمن السيبراني وكيفية حماية بياناتهم الشخصية.

المصادر

أولا: الكتب: –

١- عباس بدران: الحرب الإلكترونية الاشتباك في عالم المعلومات، مركز دراسات الحكومة الإلكترونية بيروت، لبنان، ٢٠١٠.

٢- حسن الهداوي: القانون الدولي الخاص: تنازع القوانين، المبادئ العامة والحلول الوضعية في القانون الأردني، دار الثقافة للنشر والتوزيع، عمان، ١٩٩٥.

ثانيا: البحوث المنشورة: -

١- شريفة كلاع، الأمن السيبراني وتحديات الجوسسة والاختراقات الإلكترونية للدول عبر الفضاء السيبراني، مج١٥، ع١، مجلة الحقوق والعلوم الإنسانية، جامعة زيان عشور الجلفة، الجزائر، ٢٠٢٢.

٢- - د. راجي يوسف محمود البياتي، الارهاب السيبراني(نماذج من الجهود الدولية للحد منه)، مجلة تكريت للعلوم السياسية، المجلد (٢)، العدد(٢٨)، ٢٠٢٢.

٣- د. دلالي جيلالي و د. بلبشير يعقوب: رهانات الأمن السيبراني الوطني في ظل التحول الرقمي، مجلة كلية القانون الكويتية العالمية-السنة العاشرة-العدد١-العدد التسلسلي ٣٧-ربيع الثاني/جمادى الأولى١٤٤٣هـ-ديسمبر ٢٠٢١.

٤- د. صدام مرير حمد الجميلي، الحروب الهجينة واثرها في مستقبل الصراع العالمي، مجلة تكريت للعلوم السياسية،المجلد(١)، العدد(٣٤)، ٢٠٢٤.

٥- اسراء شريف جيجان وصفا عباس فاضل: تأثير الفضاء السيبراني على الحروب الحديثة، ع٦٥، مجلة دراسات تربوية، وزارة التربية العراقية، ٢٠٢٤.

٦- محمد اكرم محسن ود. مروان سالم علي: السيبرانية "الماهية-الخصائص-الفواعل-الابعاد الاستراتيجية"، ع٤٣، س١١، مجلة حمورابي للدراسات، ٢٠٢٢.

٧- إسلام رمضان هديب: مفهوم الحرب السيبرانية في ظل القانون الدولي وتحديد خصائصها والنتائج المترتبة عليها، مج٣٦، ع١، مجلة البحوث القانونية والاقتصادية، كلية الحقوق جامعة بنى سويف، ٢٠٢٤.

٨- علاء الدين فرحات وعمارة عمروس: الفضاء السيبراني وتأكل مفهوم السيادة الوطنية، مج٨، ع٢، المجلة الجزائرية للدراسات السياسية، الجزائر، ٢٠٢١.

٩- د. هبه رمضان رجب: الحماية القانونية للبيانات الشخصية في عصر التكنلوجيا الرقمية، مج ٦٦، ع٣، مجلة العلوم القانونية والاقتصادية، كلية الحقوق جامعة عين شمس، ٢٠٢٤.

١٠- شميم مزهر راضي: الحق في حماية البيانات الشخصية في ظل دستور جمهورية العراق لسنة ٢٠٠٥، ع٤، كانون الأول، مجلة جامعة الامام جعفر الصادق (ع) للدراسات القانونية، ٢٠٢٢.

ثالثا: صفحات الانترنت: -

١- د. رغدة البهي: الردع السيبراني: المفهوم والاشكاليات، المركز المصري للفكر والدراسات الاستراتيجية، مقال منشور على الرابط التالي: https://ecss.com.eg/6203/ (٢٠٢٤/٦/٣).

٢- د. شادي عبد الوهاب: السيناريو الكارثي: متى تتحول الحرب السيبرانية إلى حرب شاملة؟، المستقبل للأبحاث والدراسات المتقدمة، مقال متاح على الرابط التالي: https://futureuae.com/ar-AE/Mainpage/Item/6992 (٢٠٢٤/٦/٣).

٣- القاضي كاظم عبد جاسم الزيدي: الحماية القانونية للبيانات الشخصية في القانون العراقي، مقالة منشورة على الرابط التالي: https://dcc-iq.com/?p=41826 (٢٠٢٤/٦/٣).

٤- باقر كريم سالم: التحديات الأخلاقية والقانونية في مجال الأمن السيبراني، مقالة علمية، متاح على الرابط التالي: https://uomus.edu.iq/NewCol.aspx?newid=24796 (٢٠٢٤/٧/٣).