الجريمة السيبرانية وآليات مكافحتها (دراسة مقارنة)

نورهان محمد الربيعي

كلية الحقوق , جامعة عجمان, الإمارات العربية المتحدة

alrubayeenorhan@gmail.com

الخلاصة:

جريمة السيبرانية، المعروفة أيضاً بجرائم التكنولوجيا الرقمية أو الجرائم الإلكترونية، تشير إلى الأنشطة الإجرامية التي تتم باستخدام التكنولوجيا الرقمية وشبكات الإنترنت. يشمل ذلك مجموعة واسعة من الأنشطة غير القانونية التي تستهدف الأفراد، الشركات، أو الحكومات، مع التركيز على سرقة المعلومات، التلاعب بالبيانات، والتلاعب الإلكتروني .البحث يتناول موضوع الجرائم السيبرانية في أربعة مباحث رئيسية. المبحث الأول يركز على فهم مفهوم الجريمة السيبرانية، حيث يتم تعريفها وتوضيح خصائصها وأنواعها. المبحث الثاني يستعرض الإطار القانوني لهذه الجرائم، من خلال تحديد أركانها والتطرق إلى الطبيعة القانونية لها. المبحث الثالث يركز على جوانب مكافحة الجرائم السيبرانية، حيث يتم استعراض مواقف التشريع العراقي والإماراتي تجاه هذا الموضوع. المبحث الرابع يتناول المكافحة الإجرائية للجرائم السيبرانية، مع التركيز على الآليات الإجرائية على مستوى الدولي والوطني. بشكل عام، يسلط البحث الضوء على أهمية فهم مفهوم وخصائص الجرائم السيبرانية، ويقدم نظرة شاملة على الإطار القانوني والجهود المبذولة في مكافحتها على مستوى التشريع والإجراءات.

كلمات مفتاحية: جرائم سيبرانية , مكافحة , قانون.

Cybercrime and Mechanisms to combat it

Nourhan Muhammad Al-Rubaie

College of Law, Ajman University, the United Arab Emirates.

Abstract:

The paragraph discusses cybercrime, also known as digital technology or electronic crimes, which refers to criminal activities carried out using digital technology and internet networks. This includes a wide range of unlawful activities targeting individuals, companies, or governments, focusing on information theft, data manipulation, and electronic manipulation. The research addresses the topic of cybercrime in four main sections. The first section focuses on understanding the concept of cybercrime, providing definitions, clarifying its characteristics, and detailing its types. The second section reviews the legal framework of these crimes by identifying their pillars and discussing their legal nature. The third section concentrates on aspects of combating cybercrime, reviewing the positions of Iraqi and Emirati legislation on this matter. The fourth section addresses the procedural combating of cybercrimes, emphasizing procedural mechanisms at both the international and national levels. Overall, the research highlights the importance of understanding the concept and characteristics of cybercrimes, offering a comprehensive view of the legal framework and efforts made to combat them legislatively and procedurally.

Keyword: Cybercrime, combat, law.

المقدمة:

في العصر الرقمي الحالي، تُعَدُّ الجرائم السيبرانية تحديات بارزة تُهدِّد أمان البيانات والخصوصية على الإنترنت. تتضمن هذه الجرائم مجموعة متنوعة من الأنشطة الضارة، مثل الاختراقات السيبرانية، وسرقة المعلومات، والتجسس الإلكتروني، والابتزاز الرقمي، والاحتيال عبر الإنترنت. التأثير السلبي الذي تفرضه الجرائم السيبرانية على الأفراد والمؤسسات يكون كبيرًا. ففقدان البيانات الشخصية والمالية يُعرّض الأفراد لمخاطر جسيمة، كما يُؤدي الاختراق إلى تعطيل الخدمات الحيوية ويُلحق ضررًا بسمعة المؤسسات. لمكافحة الجرائم السيبرانية بنجاح، يجب على الحكومات والقطاع الخاص التعاون بشكل شامل. يُنبغي تعزيز الوعي بأهمية الأمان السيبراني واتباع إجراءات الحماية للبيانات. تحقيق الأمان السيبراني يتطلب أيضًا تحديث التشريعات وتنفيذ عقوبات صارمة ضد المتورطين في الجرائم السيبرانية. التحدي الأساسي يتمثل في إيجاد توازن بين التطور التكنولوجي وتعزيز الأمان السيبراني. يتطلب هذا جهودًا مُستمرة لتحسين الحماية السيبرانية وتعزيز السياسات والتشريعات المرتبطة بالأمان الرقمي. مع التطور السريع للتكنولوجيا، تتغير أساليب الهجمات السيبرانية باستمرار. يبتكر القراصنة والمجرمون الإلكترونيين أساليب جديدة ومتطورة لاختراق الأنظمة وسرقة المعلومات. تؤثر الجرائم السيبرانية على مختلف القطاعات الاقتصادية والاجتماعية. تُكلِّف هذه الجرائم الشركات والحكومات مبالغ مالية هائلة سنويًا في تكاليف الإصلاح والتعويضات. بالإضافة إلى ذلك، يُعاني الأفراد الضحايا من آثار نفسية ومالية سلبية. بالنظر إلى طبيعة الجرائم السيبرانية التي لا تلتزم بالحدود الجغرافية، يتطلب مواجهتها التعاون الدولي الوثيق. يجب على الدول والمنظمات الدولية تبادل المعلومات وتعزيز التعاون لمواجهة هذه الجرائم بفعالية. لمواجهة التحديات المستقبلية، يجب الاستمرار في الابتكار والتطور في تقنيات الأمان. الاستثمار في أبحاث الأمان السيبراني وتطوير تقنيات متقدمة يُعدّ من الأمور الضرورية للدفاع ضد الهجمات الإلكترونية. بمعاونة تطور التكنولوجيا، من المُتوقع زيادة تعقيدات وتنوع الجرائم السيبرانية في المستقبل. يجب على الأفراد والجهات المعنية الاستعداد والتحضير لمواجهة التحديات الجديدة التي قد تنشأ. في الختام، تظل الجرائم السيبرانية تحديًا كبيرًا يتطلب استجابة شاملة لضمان الحماية الكافية للمستخدمين والبنية التحتية الرقمية.

أهمية البحث:

تتمثل أهمية بحث الموضوع المطروح تحت عنوان (الجرائم السيبرانية وآليات مكافحتها) في الآتي:

- استجلاء موقف المشرع العراقي والإماراتي حيال تلك النوعية من الجرائم المستجدة والتي تعد نتاج الثورة التكنولوجية والتقنية وتمثل أخطر إفرازاتها السلبية على المجتمع في نواح عدة.

- إلقاء الضوء على الإطار القانوني للجريمة السيبرانية.

- إيضاح الآليات الإجرائية لمكافحة الجرائم السيبرانية على مستوى الدولي والمستوى الوطني.

اهداف البحث:

تم إجراء هذا البحث لتوضيح الأسس العامة والأفكار التفصيلية المتعلقة بظاهرة الجريمة السيبرانية. يهدف البحث إلى فهم المفهوم العام للجريمة السيبرانية، وطبيعتها، ومكوناتها الفريدة، بالإضافة إلى الأسس الأساسية للمكافحة الجنائية لهذه الظاهرة وكيفية الوقاية منها. يتناول البحث دراسة البيئة التي يحدث فيها الجرم السيبراني وأشكاله وصوره في الساحة العملية. كما يسلط الضوء على المفاهيم الجديدة المرتبطة بهذه الظاهرة، مثل المجني السيبراني والمجني عليه السيبراني ، والبيئة السيبرانية (بيئة الجريمة السيبرانية)، والسلوك الجنائي التقني. يتناول البحث أيضًا التحليل الشامل للأنماط والأشكال التي تتبعها جرائم الإنترنت. فهذا البحث يسعى إلى تحقيق اهداف التالية:

- التعرف بواقع الجرائم السيبرانية وانماطها المرتكبة، ومن ثم التعرف على مخاطرها والآثار التي نجمت عنها.

- موقف المشرعين العراقي والإماراتي من جريمة السيبرانية.

- اقتراح الآليات المناسبة لرفع كفاءة الأجهزة المختصة وفاعليتها في مواجهة الجرائم السيبرانية.

منهجية البحث:

نظراً لطبيعة الدراسة ولغرض الوصول إلى تحقيق أهداف الدراسة فإن الباحثة سوف تستخدم المنهج الوصفي التحليلي وكذلك المنهج المقارن، وذلك من خلال العمل على تحليل مفاهيم الجرائم السيبرانية ، و بيان خصائصها وانواعها، وتوضيح الإطار القانوني للجريمة السيبرانية، ومن ثم بيان الآليات الإجرائية لمكافحة الجرائم السيبرانية على مستوى الدولي وعلى المستوى الوطني حيث يعد هذا المنهج من المناهج المناسب لهذه الدراسة من خلال تناول مشكلة الدراسة ووضع الحلول العلاجية لها، وستكون المقارنة بين واقع الجريمة السيبرانية ومدى آثرها على الامن السيبراني في التشريع جمهورية العراق، والتشريع دولة الإمارات العربية المتحدة، وتشريعات المقارنة.

خطة البحث:

انطلاقاً من أهداف البحث، ومشكلة البحث، فقد تم تقسيم البحث إلى اربع مباحث كما يلي :

المبحث الأول: ماهية الجريمة السيبرانية.

المطلب الأول: تعريف الجريمة السيبرانية.

المطلب الثاني: خصائص وأنواع الجريمة السيبرانية.

المبحث الثاني: الإطار القانوني للجريمة السيبرانية.

المطلب الأول: اركان الجريمة السيبرانية.

المطلب الثاني: الطبيعة القانونية للجريمة السيبرانية.

المبحث الثالث: مكافحة الجرائم السيبرانية.

المطلب الأول: موقف التشريع العراقي من مكافحة الموضوعية للجرائم السيبرانية.

المطلب الثاني: موقف التشريع الإماراتي من مكافحة الموضوعية للجرائم السيبرانية.

المبحث الرابع: المكافحة الإجرائية للجرائم السيبرانية.

المطلب الأول : الآليات الإجرائية لمكافحة الجرائم السيبرانية على مستوى الدولي.

المطلب الثاني: الآليات الإجرائية لمكافحة الجرائم السيبرانية على مستوى الوطني.

المبحث الأول

ماهية الجريمة السيبرانية

تطورت أساليب ارتكاب الجرائم بشكل كبير عن الوضع الذي كان معروفًا في السابق. لم تعد الاعتداءات تقتصر على المساس بالأفراد والممتلكات فحسب، بل اتجهت أيضًا نحو الاعتداء على المعلومات والبيانات الحساسة التي يتعامل معها مستخدمو البيئة الرقمية. حيث أصبح بإمكان المجرمين ارتكاب أبشع الجرائم بكل هدوء، دون اللجوء إلى أي أعمال عنفيه. ،وبناءً على ذلك سنخصص المبحث الأول لتعرف على هذه النوع الجديد من الجرائم من خلال التطرق إلى تعريفها وإلى خصائص التي تميزها عن الجرائم التقليدية وذلك في مطلبين التالين:

المطلب الأول: تعريف الجريمة السيبرانية.

المطلب الثاني: خصائص وأنواع الجريمة السيبرانية.

المطلب الأول

تعريف الجريمة السيبرانية

سوف أحاول خلال هذا المطلب التطرق الى تعريف الجريمة السيبرانية وإلى أهم الخصائص التي تميزها عن الجريمة التقليدية.

الفرع الأول

تعريف الجريمة السيبرانية

لم يعرف المشرع العراقي، شأنه شأن جل التشريعات المقارنة الجريمة السيبرانية، لعل سبب يرجع في كون أن وضع التعريفات للمفاهيم القانونية العامة هو عمل فقهي وليس من عمل المشرع. لذلك يعرف الفقه القانوني الجريمة بصفة عامة على انها " فعل غير مشروع صادر عن إرادة جرمية يقرر له القانون العقوبة أو التدبير احترازيا (روابح،٢٠١٨\٢٠١٩ ،ص٢٩).

كما يعرف الفقه القانوني الجريمة بصفة عامة " كل تصرف جرمه القانون سواء كان إيجابيا أو سلبيا كالامتناع ما لم نص على خلاف ذلك(المرجع السابق، ٢٩).

أما بالنسبة لمفهوم الجريمة السيبرانية فلم يتفق الفقهاء والباحثون على التعريف موحد لهذه الأخيرة، فمنهم من ينظر إلى موضوع الجريمة في حد ذاتها، وهناك من ينظر إلى الوسيلة المستعملة في ارتكابها، غرار أنهم لم يتفقوا على تسمية موحد لهذا النوع الجديد من الجرائم التي تباينت تسمياتها عبر مراحل زمنية ارتبطت بتقنية المعلومات، فهناك من يطلق عليها بتسمية الجرائم السيبرانية "cybre crime" وهناك من يطلق عليها بتسمية إساءة استخدام تكنولوجيا المعلومات والاتصال، كما يطلق عليها أيضاً بجرائم الكمبيوتر والأنترنيت. كما عرفها المشرع الإماراتي في المادة الأولى من مرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ في شأن مكافحة الشائعات والجرائم الإلكترونية حيث نصت على (كل استهداف متعمد ومخطط للأنظمة المعلوماتية أو البنية التحتية أو الشبكات الإلكترونية أو وسائل تقنية المعلومات يقلل من قدرات ووظائف أي منها، سواء كان ذلك لغرض شخصي أو لأغراض الاعتراض أو التسلل أو الاختراق أو التسريب أو بغرض تعريض البيانات أو المعلومات للخطر أو تعطيل العمليات وما في حكمها).

الفرع الثاني

خصائص الجريمة السيبرانية

الجرائم السيبرانية تتميز بخصائص فريدة تجعلها مختلفة عن الجرائم التقليدية. تلك الفروقات تعود إلى سماتها الفريدة والعناصر التي تشكلها، بالإضافة إلى الأدوات والوسائل التي يستخدمها الجرائم السيبرانية في تنفيذها، وتتمثل هذه الخصائص في:

- بأنها جرائم تتم عبر التقنيات التكنولوجية الحديثة، وعلى راسها شبكة الأنترنيت التي تعتبر كوسيلة لارتكابها.

- **من حيث الهدف:** تستهدف الجرائم السيبرانية الأنظمة المعلوماتية من خلال اختراقها بهدف تلاعب أو تشويه المعلومات والبيانات الخاصة بمستخدمي البيئة الرقمية، على غرار ما يحدث في الجرائم التقليدية.

- **الجريمة السيبرانية تعتبر جريمة ناعمة** بسبب خفتها وصعوبة اكتشافها، حيث قد لا يلاحظ الشخص المتضرر ارتكابها أثناء تواجده على الشبكة. الجاني يمتلك مهارات تقنية متقدمة تسمح له بالقيام بتلك الجرائم دون أن يتم الكشف عنها، مثل سرقة الأموال أو إرسال فيروسات ضارة إلى البرامج وأجهزة الكمبيوتر(الصغير، ٢٠١٢\٢٠١٣،صفحة١٤-صفحة١٥).

- **صعوبة اكتشافها:** تعتبر الجريمة السيبرانية من الجرائم التي يصعب اكتشافها ولذلك لعدم تركها لآثار مادية يمكن من خلالها كشف مرتكبها هذه الأخيرة. مما يجعل الأمور تزداد تعقيداً لدى سلطات الأمن وأجهزة التحقيق، فداخل هذه البيئة تكون البيانات والمعلومات عبارة عن نبضات إلكترونية غير مرئية، مما يجعل أمر طمس هذا الدليل الإلكتروني ومحوه كلياً من قبل الفاعل أمر في غاية السهولة(الصغير، ٢٠١٤، صفحة٠٨).

- **جريمة ذات بعد دولي تعد الجريمة السيبرانية** جرائم عابرة للحدود لا تعترف بعنصر الزمان والمكان، فهي تتميز بالتباعد الجغرافي واختلاف التواقيت بين الجاني والمجني عليه(قويدري،٢٠٢٢، ص٢٠١). وهذا راجع الى المجتمع الذي لا يعترف بالحدود الجغرافية، فهو مجتمع منفتح على الشبكات تخترق الزمان والمكان دون أن تخضع لحرس الحدود.

- **تعتبر جرائم** السيبرانية من بين الجرائم التي يتطلب إلمام مرتكبها بجوانب التقنية وكذلك الخبرة الفائقة في استخدام الحاسب الآلي.

- **صعوبة ضبط وتوصيف الجرائم السيبرانية** أن من بين الصعوبات التي تواجه ظباط الشرطة القضائية والمحققين وكذا القضاء خاصة فيما يتعلق بإجراءات ضبط الجرائم المعلوماتية وإضفاء الوصف القانوني المناسب لها، ولعل المراد ذلك إلى الطبيعة الخاصة التي تتميز بيها هذه الأخيرة (الصغير، مرجع سابق، ص٧٥).

المبحث الثاني

الإطار القانوني للجريمة السيبرانية

يتطلب الكشف عن الجريمة السيبرانية توفير أركان محددة، المتفق على ضرورة توافرها على أرض الواقع في أية جريمة أخرى، بدون هذه الأركان، يصعب تأكيد وجود هذه الجريمة. كما أن لهذه الجريمة محل تقع عليه، يتمثل في المعطيات والمصلحة التي تهدرها سنناقش هنا هاتين النقطتين لفهم هذا الموضوع بشكل أفضل وذلك في مطلبين التاليين:

المطلب الأول: اركان الجريمة السيبرانية.

المطلب الثاني: الطبيعة القانونية للجريمة السيبرانية.

المطلب الأول

اركان الجريمة السيبرانية

الجريمة السيبرانية لا تختلف عن الجرائم التقليدية التي ينص عليها قانون العقوبات. تتطلب الجرائم وجود عناصر محددة يجب توافرها في أي جريمة، وهذا يشمل الجرائم السيبرانية كجزء من القوانين الجنائية العامة. هذا النوع من الجرائم يتطلب وجود ركنين أساسيين: ركن مادي وركن معنوي. بدون وجود هاتين العنصرين، لا يمكن اعتبار وجود الجريمة. بالإضافة إلى العنصر المفترض الذي يفرضه المشرع مسبقًا في جرائم المعلوماتية، والذي يُعتبر جزءًا من جانب المادي للجريمة، وذلك على النحو التالي:

الفرع الأول

الركن المادي للجريمة السيبرانية

إنه في إطار الجريمة محل البحث، يتعين أن يأتي الركن المادي للجريمة السيبرانية على الشكل والهيئة التي يتطلبها المشرع، سواء من حيث اجتماع عناصره الثلاثة من نشاط أو سلوك مادي وعلاقة سببية ونتيجة إجرامية، أو أن يكتفي المشرع بعنصر وحيد وهو النشاط أو السلوك المادي فقط، وفى هذه الحالة تتوافر الجريمة دون حاجة للبحث عن النتيجة المتحققة وعلاقة السببية، حتى وإن توافرت على المستوى المادي، فإن هذا الوجود يعد من طبيعة مادية ليس له في القانون من أثر (جريمة شكلية)(إبراهيم ،٢٠٠٩،صفحة٩٨). أو كما يسميها بعض أصحاب الفقه الجنائي جريمة السلوك والنشاط (المري، ٢٠١٩، صفحة٣٣) .

فإن النشاط أو السلوك المادي يتمثل في الفعل الذي يأتيه الجاني بالمخالفة لإرادة المشرع ويتعين أن يكون له مظهر خارجي وسأوضح عناصر الركن المادي في الجريمة السيبرانية بشيء من التفصيل فيما يأتي:

أولا: الركن المادي للجريمة السيبرانية :

وهو يمثل عنصر جوهريًا لقيام الركن المادي في كافة أنواع الجرائم المادية والشكلية، إذ لابد لكل جريمة سلوك، والمراد بالسلوك النشاط الخارجي الذي يقوم به الجاني، ويبرز في العالم الخارجي مكونا لماديات الجريمة ومسببا لما قد يترتب عليها من ضرر أو خطر، وسواء قصد الجاني من هذا السلوك الإجرامي تحقيق نتيجة معينة أم تحققت النتيجة دون أن تنصرف إرادته إليها(الحجازي،٢٠٠٩، ص١١٩).

ويختلف النشاط أو السلوك المادي من جريمة لأخرى، كما يختلف في الجرائم السيبرانية عنه في الجرائم التقليدية، إذ يتطلب السلوك المادي في الجرائم السيبرانية وجود بيئة رقمية: المقصود بالبيئة الرقمية: هو مجموعة المواد (نصوص أو صور فيديوهات وغيرها) مخزنة بصيغة رقمية ويمكن الوصول إليها عبر عدة وسائط وأهم وسائل الوصول لمحتوى الرقمية على الكتب الرقمية فقط يتعداه إلى غيرها من الوسائط واتصال بالإنترنت من خلال الحاسب الآلي أو الهاتف الذكي. كما يتطلب السلوك المادي في جرائم السيبرانية أيضا معرفة بداية هذا النشاط والشروع فيه ونتيجته. فمثلا يقوم مرتكب الجريمة بتجهيز الحاسب لكي يحقق له حدوث الجريمة ، فيقوم بتحميل الحاسب ببرنامج اختراق، أو أن يقوم بإعداد هذا البرنامج بنفسه، وآنذاك قد يحتاج إلى تهيئة صفحات تحمل في طياتها مواد خليعة أو مخلة بالآداب العامة وتحميلها على الجهاز المضيف Hosting Server ، كما يمكن أن يقوم بجريمة إعداد برامج فيروسات تمهيدا لبثها(إبراهيم، مرجع سابق، صفحة٩٨). ولكن ليس كل جريمة تستلزم وجود أعمال تحضيرية، فالسلوك الإجرامي في الجريمة السيبرانية يرتبط دائما بالمعلومة المخزنة على الحاسب الآلي وتكمن صعوبة المشكلة في أن السلوك الإجرامي قد يتحقق بمجرد ضغطة زر في لوحة المفاتيح الملحقة بالحاسب فيتم - مثلا - تدمير نظام أرصدة العملاء في أحد البنوك، أو إساءة استعمال بطاقات الائتمان(المطلب، ٢٠٠٠،صفحة ٥٦).

وقد أصبح هذا السلوك محلا لتساؤلات عديدة خاصة فيما يتعلق ببدايته أو الشروع في ارتكاب الجريمة، فهو يختلف عما عليه الحال في العالم المادي. فقد عد المشرع الفرنسي الشروع كالجريمة التامة في نطاق الجرائم السيبرانية، إذ عد جريمة الدخول غير المشروع أو البقاء غدرا بالأنظمة الآلية لمعالجة المعلومات المنصوص عليها في المادة -١\٣٢٣ من قانون العقوبات الفرنسي لسنة ١٩٩٢ المعدل جريمة بحد ذاتها نصت هذه المادة على أن (" كل شخص قام بالدخول أو البقاء بطريقة كلية أو جزئية داخل نظام لمعالجة المعلومات سيعاقب بالحبس الذي لا يقل عن شهرين ولا يزيد عن سنة وبغرامة تتراوح بين ٣٠٠٠٠ إلى ٥٠٠٠٠ فرنك أو بإحدى هاتين العقوبتين كل من دخل بطريق الغش أو مكث غدرا في نظام للمعالجة الآلية للمعلومات أو في جزء منه...) ، أي أنها جريمة شكلية لا يتطلب لإتمامها نتيجة معينة، فهي من جرائم السلوك المجرد. بالنسبة للمشرع الإماراتي فقد نص على تجريم الشروع في مرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ في شأن مكافحة الشائعات والجرائم الإلكترونية الباب الأول: الجرائم والعقوبات في المادة ٣\١ نصت على (وتكون العقوبة الحبس مدة لا تقل عن سنة والغرامة التي لا تقل عن (٢٠٠,٠٠٠) مائتي ألف درهم ولا تزيد على (٥٠٠,٠٠٠) خمسمائة ألف درهم، أو بإحدى هاتين العقوبتين، إذا كان الاختراق بغرض الحصول على البيانات أو المعلومات **لتحقيق غرض غير مشروع** .

١ـ النتيجة الإجرامية :

بناءً على ما تم طرحه، نرى أن الجريمة السيبرانية تُعتبر من فئة الجرائم ذات السلوك المجرد، حيث لا تتطلب نتيجة محددة ليتم تحقيقها بل تحدث بمجرد وقوع السلوك ذاته. على سبيل المثال، يُمكن اعتبار الإبلاغ عن جريمة سيبرانية كفعل جرمي بمفرده دون الحاجة إلى انتظار النتيجة. مثلا: إنشاء موقع للتشهير بشخص معين دون طرح هذا الموقع على الشبكة إلا انه لا مناص من معاقبة الفاعل(حياة ، ٢٠١٨\٢٠١٩، صفحة١٣).

٢ـ علاقة السببية:

يراد بعلاقة السببية، الصلة التي تربط بين الفعل (السلوك الإجرامي) والنتيجة الإجرامية، إذ يثبت أن ارتكاب الفعل هو الذي أدى إلى حدوث النتيجة(حسني، ٢٠٠٧،صفحة٢٧٩) ، وللسببية هذه أهميتها فهي التي تربط بين عنصري الركن المادي فتقيم بذلك وحدته وكيانه، فإذا انتفت هذه العلاقة كانت مسئولية مرتكب الفعل تقتصر على الشروع إذا كانت الجريمة عمدية وتوافرت عناصر هذا الشروع أما إذا كانت الجريمة غير عمدية فلا يسأل مرتكب الفعل لأنه لا شروع في الجرائم غير العمدية.

وعلاقة السببية تبحث بشكل عام بالنسبة للجرائم المادية وليس الشكلية، وذلك لحصول النتيجة في الجرائم الشكلية بمجرد وقوع السلوك الإجرامي في هذه الجرائم(الاطرقجي،٢٠٠٠، صفحة١٠١).

نظرًا لأن الجريمة السيبرانية تندرج ضمن فئة الجرائم ذات السلوك المجرد، حيث يفرض المشرع عقوبة بمجرد وقوع الفعل، ويأتي ذلك نتيجة لتكامل النتيجة والعلاقة السببية في هذا النوع من الجرائم. وبمعنى آخر، لا يتوجب وجود العناصر الأخرى للجانب المادي كالنتيجة الجنائية والعلاقة السببية لتحقيق هذا النوع من الجرائم.وتتطلب النتيجة دائما إسنادا ماديا ومعنويا . فالإسناد المادي يقتضي نسبة الجريمة لفاعل معين ونسبتها إلى الفعل، بالإضافة لنسبة الفعل إلى فاعل(رؤوف، ١٩٩٦، صفحة٣).

أما الإسناد المعنوي، فهو نسبة الجريمة إلى شخص متمتع بالأهلية اللازمة لتحمله المسئولية الجنائية، ويقتضى ذلك أن يتوافر لدي الفاعل الإدراك وحرية الاختيار، ويلاحظ أن الإسناد المادي والمعنوي من عناصر المسئولية الجنائية، إذ بغيرهما لا تقوم لها قائمة(المرجع السابق، ص٣). ولا يختلف مفهوم علاقة السببية في الجرائم السيبرانية عن الجرائم العادية، لأن رابطة السببية - كما هو معلوم - ارتباط الفعل التقني غير المشروع بالنتيجة المجرمة ارتباط السبب بالمسبب ومن ثم فهي مرتبطة بالواقع الافتراضي الذي يتم عبر شبكة الإنترنت وترتب آثارها في الواقع المادي. فتقوم الجريمة إذا رتب السلوك التقني نتيجة مؤثمة(يونس،٢٠٠٣، صفحة٣٢١).

٣- العنصر المفترض:

وهو يعرف بأنه المركز القانوني أو الواقعي الذي يلزم توافره قبل ارتكاب الجريمة، أو هو كل أمر يشترط القانون تقدمه على أركانها، فلا يصح الحديث عنها إلا إذا وجد ويترتب على انعدامه العلم، وقد يتعلق هذا الشرط بالجاني أو المجني عليه أو يتصل بمحل الجريمة المجيد(٢٠٢٣، صفحة ٢٠١). وإذ أضحت المعلومات والبيانات محلا لمصلحة جديرة بأن تشملها التشريعات الجنائية بالحماية الخاصة، مما يجعل هذا المحل عنصرا مفترضا في الجريمة محل البحث، يشترط القانون وجوده لوجودها. فعلى سبيل المثال في جريمة خيانة الأمانة السيبرانية وهى من الجرائم العمدية التي تستلزم توافر القصد الجنائي.

ترى الباحثة؛ إن الجريمة المفترضة في حالة خيانة الأمانة السيبرانية تتجلى عندما يقوم الجاني بتسليم الأسطوانات التي تحتوي على برامج ومعلومات للغير، ثم يقوم بنسخها وإعادتها مع الاحتفاظ بها لنفسه. يتحول بذلك من حيازة مؤقتة إلى حيازة كاملة. يتم تسليم هذه الأشياء إلى الجاني بهدف ممارسة نشاط محدد على حساب صاحب الحق فيها.

وكذلك يتحقق العنصر المفترض في حق الجاني الذي يعلم بالضرر الذي ينجم عن تلاعبه في البرامج أو المعلومات التي يكون له حق الدخول إليها والتعامل معها بحكم عمله خاصة فيما يتعلق بإفشاء المعلومات السرية أو في حالة الاستيلاء على أموال الغير(الصغير،١٩٩٢، صفحة١١٧). باعتبار أن الفعل انصب على المعلومات في ذاتها بمعزل عن الوسيط المادي الحامل لها.

ثانياً: الركن المعنوي للجريمة السيبرانية:

الركن المعنوي هو الحالة النفسية للجاني، والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني، وبالنظر لما للركن المعنوي من أهمية أساسية في النظرية العامة للجريمة، إذ الأصل أنه لا جريمة بدون ركن معنوي، فهذا الركن هو سبيل المشرع إلى تحديد المسئولية عن الجريمة. فإنه يتعين توافر الركن المعنوي في الجريمة السيبرانية بالرغم من أنها لا ترتكب في عالم مادي وإنما في عالم افتراضي، فيجب أن يكون الجاني عالما بأن الفعل الذي يأتيه أو سلوكه المادي يجرمه القانون، وعلى الرغم من توافر هذا العلم لديه تتجه إرادته إلى إتيان هذا الفعل قاصدا تحقيق نتيجته(المري، مرجع سابق، صفحة٣٨). وقوام الركن المعنوي، هو الأصول النفسية لماديات الجريمة والسيطرة النفسية عليها، ومن ثم كان الركن المعنوي في جوهره قوة نفسية، وهذه القوة هي الإرادة. إلا أن هذا الركن لا يتحقق بهذه الإرادة وحدها ما لم تتجه إلى إتيان فعل جرمه القانون إذن الإرادة هي جوهر الركن المعنوي، كما أنها دليل على خطورة شخصية الجاني، وهى مظهر لهذه الشخصية، فإذا اتخذت هذه الإرادة صورة القصد الجنائي؛ وصفت الجريمة بأنها عمدية، أما إذا اتخذت صورة القصد غير العمدي؛ فإن الجريمة توصف بأنها غير عمدية (عسل، الظروف ،١٩٩٠،صفحة٧١). ويعتمد هذا التقسيم على أن الفاعل في الجريمة العمدية قد قام باقتراف فعله قاصدا ارتكاب السلوك المجرم الذي أتاه، كما أراد النتيجة الإجرامية التي حصلت منه أو أية نتيجة أخرى، بينما أن الفاعل في الجريمة غير العمدية لم يقصد سوى ارتكاب السلوك دون إرادة تحقيق النتيجة الإجرامية. وعلى هذا الأساس يتبين أن الركن المعنوي في ضوء القواعد العامة يتخذ صورتين: «القصد الجنائي» و «الخطأ غير العمدي»، وسنحاول تطبيق هاتين الصورتين على عناصر الركن المعنوي في الجريمة السيبرانية، وذلك على النحو الاتي:

١- الجريمة سيبرانية كجريمة عمدية:

بناءً على ما تم ذكره سابقًا، يتضح أن القصد الجنائي يشير إلى معرفة عناصر الجريمة، ووجود إرادة موجهة نحو تحقيق تلك العناصر والموافقة عليها. يمكن تطبيق هذا التعريف على القصد الجنائي بجميع أشكاله، سواء كان القصد مباشرًا أو احتماليًا. ويوضح هذا التعريف، أن القصد الجنائي يقوم على عنصرين، وهما «العلم» و «الإرادة»، غير أن لعنصر الإرادة أهمية تفوق أهمية عنصر العلم لكون الإرادة هي جوهر القصد وليس العلم متطلبا لذاته وإنما باعتباره مرحلة في تكوين الإرادة وشرطا لتطورها. ويتوافر القصد الجنائي بتوافر هذين العنصرين معا، فالعنصر الأول يمثل إرادة النشاط الذي ينتهي إلى وضع إجرامي معين في القانون، والعنصر الثاني هو العلم والإحاطة بحقيقة هذا الوضع الإجرامي من حيث الوقائع وماهيته من حيث القانون وذلك في معنى الإدراك(المجيد، مرجع سابق، ص٢٠٦).

هذا ويعد القصد الجنائي هو أخطر صور الركن المعنوي، إذ تنصرف إرادة الجاني إلى السلوك الإجرامي وإلى ما يترتب عليه من نتيجة إجرامية . الفرق بين الجريمة العمدية وغير العمدية يتمحور، بشكل عام، حول النتيجة الجنائية الناتجة. إذ كلما كانت النية للوصول إلى تلك النتيجة وكان الجاني قد وجه جهوده نحو تحقيقها، تُعتبر الجريمة عمدية. أما إذا لم يكن الجاني يقصد بفعلها ولم يتوقعها، أو قد قام بتقدير خاطئ بشأنها دون التصرف لتجنبها، فإن الجريمة تُصنف عادة كغير عمدية. وفي إطار الجريمة محل البحث، قد يأخذ الاعتداء على الحاسب الآلي صورة العمد، ويتمثل ذلك في أفعال السرقة والنصب وخيانة الأمانة والتزوير السيبرانيين واتلاف المكونات المادية للحاسب الآلي (الشاشات والكابلات ولوحة المفاتيح والسماعات والدعامات المغناطيسية من الأسطوانات والأقراص والبطاقات الممغنطة أو اتلاف مكوناته المعنوية من البرامج والنظم التطبيقية .... الأمر الذي يترتب عليه خسائر جسيمة. ومثال ذلك، ما حدث لأحد البنوك الفرنسية حيث أدى اتلاف نظام الشبكات الخاص به إلى تأخير البيانات آليا ما ترتب عليه خسائر قدرت بمليوني فرنك فرنسي(الدين، ٢٠٠٨،صفحة ٣١).

من المرجح أن تكون الجريمة السيبرانية نتيجة لتصرف عمد، حيث يتم التفكير المسبق في الحصول على معلومات من خلال اختراق شبكة حاسوب أخرى بهدف تحقيق فوائد شخصية أو تنفيذ هدف محدد. يمكن أن يكون مثالاً على ذلك قيام قراصنة بنسخ برامج حاسوب من مواقع على الإنترنت، وفك شفرات هذه المواقع وتعطيلها للحصول على البرمجيات ولتسبب الأذى للشركة.

٢. الجريمة السيبرانية كجريمة غير عمدية:

سبق لنا الإشارة إلى أن الجريمة تكون غير عمدية إذا كان الجاني له وجه إرادته إلى ارتكاب السلوك الإجرامي فقط دون إرادة تحقيق النتيجة الإجرامية عن طريق النص القانوني، فالجريمة غير العمدية هي الجريمة الناشئة أو الناتجة عن خطأ غير صدي، شريط أن ينص عليه القانون وقد أغفل قانون العقوبات المصري إيراد تعريف الخطأ غير صدي، واكتفى بذكر صوره في القسم الخاص في معرض بيانه للجرائم غير العمدية لاسيما جرائم القتل والإصابة الخطأ، ولعل السبب في ذلك يرجع إلى الصعوبة التي يجدها المشرع الجنائي، إذا وضع تعريف عام للخطأ في الإحاطة بكل الحالات الموجودة والتي ستوجد في المستقبل، ناهيك من أن ذلك سيكون قيدا على حرية القاضي في التعامل مع الوقائع المتغيرة والمعقدة التي تعرض عليه(المجيد، مرجع سابق، صفحة٢١٥). إذا أردنا تقييم إمكانية تطبيق هذا المعيار الشخصي على الأفراد في جرائم السيبرانية، يمكننا تصوّر أن الجرائم الجديدة قد تظهر كأخطاء غير متعمدة. على سبيل المثال، يمكن للموظف المسؤول (الفاعل) تدمير أجهزة المؤسسة بناءً على فرضيات شخصية، مثل استخدام جهاز الحاسوب الخاص به في إجراءات غير مشروعة بناءً على مهاراته في إنشاء فيروسات، أو استخدام قرص مرن في جهاز الحاسوب الخاص بالمؤسسة لنقل فيروسات، مما يؤدي إلى تدميرها جزئيًا أو كليًا. يظل هذا السيناريو ممكنًا طالما يشارك الإنسان في عمليات معالجة البيانات.

- محل الجريمة السيبرانية :

الحاسوب الآلي يشكل عنصرًا حيويًا في حياة الإنسان، إذ ساهمت فوائده الكبيرة في تحسين الحياة اليومية، ولكن في الوقت نفسه، أحدث تحديات خطيرة. يُصنع الحاسوب بواسطة الإنسان، ويترتب ارتباط استخدامه بين الأغراض الشرعية والمفيدة وبين الأغراض غير الشرعية والمؤذية. يفتقر الحاسوب إلى القدرة على التمييز بين هذه الأغراض، حيث يُبرمج لاستقبال الأوامر دون القدرة على فهم الأهداف التي يسعى المستخدم لتحقيقها. وفي سياق متصل، يظهر أن الاتصال بشبكة الإنترنت يزيد من احتمالية استخدام الحاسوب في أغراض إجرامية. يؤدي الحاسوب وظيفته وفقًا للتعليمات التي يتلقاها، وبالتالي يكون تحت تأثير وسيطرة المستخدم، سواء كانت نياته صافية أم أنه يقوم بأفعال جريمة سيبرانية. تُشير "الجريمة السيبرانية" إلى الجرائم التي ترتكب

باستخدام الحاسوب، وتمثل نوعًا جديدًا من التصرفات الهادفة إلى الإلحاد بسلوكيات الحاسوب ومكوناته. يمكن أن تتورط في هذه الجرائم الأفراد الذين يتمتعون بالخبرة العلمية والعملية في مجال التعامل مع الحواسيب. يصبح النظام المعلوماتي هدفًا للجريمة السيبرانية، حيث يمكن أن تستهدف المكونات المادية وغير المادية للنظام. بالإضافة إلى ذلك، تظهر تفاصيل الجريمة بشكل مزدوج، حيث يمكن أن تكون لها جوانب مادية وأخرى غير مادية. على سبيل المثال، يمكن أن تكون المعلومات جزءًا من النظام غير المادي، بينما يمكن أن تتجسد في صورة مادية على وسائط تخزين، مما يجعلها تخضع للقوانين بحسب طبيعتها. إذن، فإن موضوع الجريمة السيبرانية أي محلها، يتمثل في المعطيات والمصلحة التي تهدرها، والحق الذي تعتدي عليه هو الحق في المعلومات بذاتها، وبما تمثله من أموال أو أصول أو أسرار أو بيانات شخصية أولها قيمة بذاتها كالبرامج (عزيزة،٢٠١٨،صفحة ١٨٤). فالمعلومات الإلكترونية جديرة بالحماية حتى عن المعلومات الورقية فتظهر جدارة المعلومات المبرمجة آليا بالحماية الجنائية عن المعلومات التي تحتويها الملفات الورقية من ضعف النوع الأول من المعلومات ومن أهميته في آن واحد، فالمعلومات المعالجة آليا ضعيفة داخل النظام عنها داخل الملفات الورقية. فهذه الأخيرة يمكن إخفاؤها بسهولة عن المعلومات داخل النظام، كما أن المعلومات المعالجة آليا تتميز بالضخامة والتنوع، ومنها ما يتعلق بالحياة الخاصة للأفراد وهذا ما دعي مشرعي كثير من البلاد إلى استحداث صور من التجريم لحماية المعلومات داخل الحاسب الآلي من الاطلاع عليها، بينما لا يوجد مثيل لتلك النصوص بالنسبة للمعلومات المسجلة داخل الملفات الورقية(عطا الله،٢٠٠٧، صفحة ٩٤).

المطلب الثاني

الطبيعة القانونية للجريمة السيبرانية

الحديث حول الطبيعة القانونية للجريمة السيبرانية يركز على الوضع القانوني للبرامج والمعلومات وما إذا كانت لها قيمة في ذاتها أم تعتبر مستحدثة من القيم القابلة للاستئثار. يشير الى أن الجرائم السيبرانية تختلف عن الجرائم العادية بسبب ارتباطها بالقانون الجنائي السيبراني، حيث تتم داخل نطاق المعالجة الإلكترونية للبيانات. يذكر أن هذه الجرائم تشمل تجميع وتجهيز وإدخال البيانات للحصول على معلومات، وتحدث في مجالات مثل معالجة الكلمات والنصوص. ويشير إلى أن الجاني يتعامل مع برامج وبيانات جديدة كمحل للاعتداء أو وسيلة له. يؤكد على أهمية تحديد الطبيعة القانونية للجريمة السيبرانية بسبب المال المعلوماتي وتقسيمه إلى نوعين: معلوماتية ذات طبيعة معنوية ومعلوماتية ذات طبيعة مادية. يشير إلى أن شبكة المعلومات الإنترنت تطرح تساؤلات حول نظام المسؤولية والتشريع لخدمات نشر المواقع وتبادل المعلومات فيها. ويشدد على أن القانون الملائم للجرائم السيبرانية يهدف إلى معرفة النصوص القانونية التي يجب تطبيقها على خدمات نشر المواقع والمعلومات، ويشير إلى تحديات مثل مسألة الإثبات وصعوبة محاكمة المتجاوزين في حالة وجود تشفير للبيانات. يختتم بالتأكيد على ضرورة تحديد الطبيعة القانونية للجرائم السيبرانية بناءً على المجال الذي يمكن أن تحدث فيه أو المحل الذي يقع عليه الاعتداء.

المبحث الثالث

مكافحة الجرائم السيبرانية

يتزايد القلق إزاء الزيادة المستمرة في ظاهرة الإجرام السيبراني، حيث تتطور هذه الجرائم بتزايد الذكاء الإلكتروني. يرتبط ظهور هذا النمط الجديد من الجرائم بتقدم أنظمة المعلومات، ويعتبر ذلك طبيعيًا نتيجة لتقدم المجتمع التكنولوجي. يظهر تطور الجرائم السيبرانية في ظل التقنيات والتكنولوجيا، التي سهلت التواصل وانتقال المعلومات بشكل مدهش. ورغم الفوائد الكبيرة لهذا التقدم، إلا أنه يُستغل أيضًا من قِبَل الجريمة، حيث يستخدم الجاني هذه التكنولوجيا لتطوير قدراته الإجرامية باستخدام شبكة المعلومات كوسيلة سهلة لتنفيذ أعمال جرمية، مما يسفر عن آثار وتداعيات تتجاوز حدود الدول. يواجه العالم بأسره تحديات حقيقية في مكافحة هذه الأشكال الحديثة للإجرام. بناءً على ذلك تم تقسيم هذا المبحث الى مطلبين:

المطلب الأول: موقف التشريع العراقي من مكافحة الموضوعية للجرائم السيبرانية.

المطلب الثاني: موقف التشريع الإماراتي من مكافحة الموضوعية للجرائم السيبرانية.

المطلب الأول

موقف التشريع العراقي من مكافحة الموضوعية للجرائم السيبرانية

ما زال المشرع العراقي يواصل التأجيل في إصدار قانون مخصص لتنظيم الجرائم المعلوماتية بسبب الظروف الراهنة في البلاد. وقد تم تقديم مشروع قانون يحتوي على ٣٣ مادة إلى مجلس النواب، إلا أنه تم إلغاؤه بسبب الضغوط التي مارستها نقابات حزبية، يمكن أن يكون سبب تأجيل هذا القانون هو عدم مراعاة المعايير والمبادئ اللازمة للتشريع. لكن هذا لا يعني عدم خضوع الجريمة الالكترونية للقانون بل يطبق عليها القوانين الاتية:

١- قانون العقوبات العراقي رقم(١١١) لسنة١٩٦٩ المعدل.

٢- قانون اصول المحاكمات الجزائية رقم (٢٣) لسنة ١٩٧١.

٣- قانون الاثبات العراقي (١٠٧) لسنة ١٩٧٩ نصت المادة ٢٧ منه (يكون للبرقيات حجية السندات العادية اذا كان احلها المودع في مكتب الإصدار موقعاً من مرسلها).

٤- قانون المطبوعات رقم (٢٠٦) لسنة ١٩٦٨ الذي يخص الصحف والمجلات وتستند عليه فيما ينشر على موقع الانترنت بما فيها التواصل الاجتماعي.

٥- قانون مكافحة الإرهاب رقم (١٣) لسنة ٢٠٠٥ فيما يخص جرائم الإرهاب الالكتروني فقد جرمت المادة الأول منه (كل فعل إجرامي أوقع بالممتلكات العامة او الخاصة او اثارة الرعب والخوف بأي وسيلة كانت).

❖ من ملاحظة على القانون الإرهاب رقم (١٣) لسنة ٢٠٠٥ بمادته الأولى انه عرف الإرهاب بشكل غير كامل وكان والاجدر به الاستعانة بتعريف الاتفاقية العربية لمكافحة الإرهاب والذي أنظم اليها وصادق عليها فقد شملت بالتعريف كل طبع أو نشر ممرات او تسجيلات مهما كان نوعها.

المطلب الثاني

موقف التشريع الإماراتي من مكافحة الموضوعية للجرائم السيبرانية

أما دولة الإمارات، فقد أصدرت المرسوم بقانون اتحادي رقم (٣٤) لعام ٢٠٢١ فيما يتعلق بمكافحة الشائعات والجرائم الإلكترونية، وبدأ تنفيذه في الثاني من يناير ٢٠٢٢. يُعوِّل هذا القانون على استبدال القانون الاتحادي السابق الصادر بمرسوم اتحادي رقم ٥ لعام ٢٠١٢ المتعلق بمكافحة جرائم التقنيات المعلوماتية. هدف هذا القانون هو توفير إطار قانوني شامل لتعزيز حماية المجتمع من الجرائم الإلكترونية التي تتم من خلال شبكات الإنترنت والتقنيات ذات الصلة. بالإضافة إلى ذلك، يهدف إلى حماية المواقع الإلكترونية وقواعد البيانات الحكومية في دولة الإمارات، ومكافحة انتشار الشائعات والأخبار المزيفة، ومكافحة الاحتيال الإلكتروني، وضمان حفظ الخصوصية والحقوق الشخصية. يوضح القانون الأفعال الممنوعة والعقوبات المترتبة على أي فرد يقوم بإنشاء أو استخدام موقع إلكتروني أو وسائل تقنية معلوماتية لاختراق أو هجوم على نظم المعلومات والبيانات الحكومية أو إتلافها، وكذلك نشر المعلومات الزائفة أو المعلومات التي تضر بمصلحة وأمن دولة الإمارات. يتناول القانون أيضًا مجموعة متنوعة من الجرائم الإلكترونية الأخرى.

المبحث الرابع

المكافحة الإجرائية للجرائم السيبرانية

المكافحة الإجرائية للجرائم السيبرانية تتطلب تبني استراتيجيات شاملة للحد من الأنشطة الإلكترونية غير القانونية. تشمل هذه الاستراتيجيات وضع تشريعات صارمة تجرم الأنشطة السيبرانية، وتعزيز التعاون الدولي لتبادل المعلومات ومكافحة الجريمة عبر الحدود. كما يجب تطوير التقنيات الرقمية لتمكين التحقيق الفعّال في حالات الجرائم السيبرانية، بما في ذلك استخدام تقنيات التحليل الرقمي والاسترجاع الإلكتروني. تعزيز الأمان التقني يأتي عبر تحسين تقنيات الحماية والتشفير، وتحديث الأنظمة بشكل

دوري. يتضمن الجانب التدريبي تأهيل القضاة ورجال الشرطة لفهم أحدث التقنيات وتقنيات التحقيق الرقمي. هذا يساعد في تعزيز فهم المجتمع لمخاطر الأمان السيبراني وكيفية الوقاية منها. التعاون مع القطاع الخاص يلعب دورًا مهمًا في تحقيق هذه الأهداف، حيث يتيح التبادل المستمر للمعلومات بين الحكومة والشركات تحديد ومواجهة التهديدات بشكل أفضل. إضافة إلى ذلك، يجب أن تكون هناك عقوبات قوية للجرائم السيبرانية لتردع المرتكبين وتحد من انتشار هذه الأنشطة غير القانونية.

من هذا المنطلق، فأنني سأتناول في هذا المبحث المكافحة الإجرائية للجرائم السيبرانية وذلك في مطلبين التاليين:

المطلب الأول: الآليات الإجرائية لمكافحة الجرائم السيبرانية على مستوى الدولي.

المطلب الثاني : الآليات الإجرائية لمكافحة الجرائم السيبرانية على مستوى الوطني.

المطلب الأول

الآليات الإجرائية لمكافحة الجرائم السيبرانية على مستوى الدولي

في سياق تحليل الآليات الإجرائية لمكافحة الجرائم السيبرانية في الاتفاقيات الدولية، سأتناول الجهود الدولية المبذولة لمكافحة هذا النوع من الجرائم، بالإضافة إلى التدابير الجديدة المُعتمدة لاحتوائها على مستوى هذه الاتفاقيات. وأستعرض هذا الموضوع في عدة اتفاقيات دولية، منها اتفاقية مجلس أوروبا - بودابست لسنة ٢٠٠١ واتفاقية مجلس أوروبا لسنة ٢٠٠٤، ونلقي الضوء على التطورات والتحديات التي تعتبرها هذه الاتفاقيات لتعزيز الآليات القانونية والإجرائية في مجال مكافحة الجرائم السيبرانية. في إطار اتفاقية مجلس أوروبا - بودابست لعام ٢٠٠١، يتم التركيز على الاعتراف بأن النشاط التقني يشكل جزءًا لا يتجزأ من النشاط المادي، وهو خطوة أولى هامة في مسار مكافحة الجرائم السيبرانية.

الفرع الأول

في اتفاقية مجلس أوربا ـ بودابست لسنة ٢٠٠١

أشرنا سابقًا إلى عقد اتفاقية مجلس أوروبا - بودابست في ٢٣ نوفمبر ٢٠٠١، والتي أطلق عليها اسم "اتفاقية الجريمة عبر العالم السيبراني (الإنترنت)"، بهدف تقديم إطار قانوني يساعد الدول في مواجهة الجريمة السيبرانية. وقعت عليها ٤٣ دولة أوروبية عضوة في المجلس الأوروبي. هذه الاتفاقية ألقت الضوء على أهمية النشاط التقني كجزء لا يتجزأ من النشاط المادي في جرائم السيبرانية، وذلك في مادتها الثالثة التي تشير إلى "استخدام التقنية"، حيث يُفهم بأنه استخدام الحواسب الآلية بكل تقنياتها وتكنولوجيا الاتصالات. تعد هذه الاتفاقية خطوة رئيسية في مجال مكافحة الجريمة السيبرانية، حيث لا تقتصر على وضع قواعد مكافحة موضوعية بل تعالج أيضًا المشكلات الإجرائية التي تواجه جهود مكافحة هذه الجريمة. بفهم الدول الموقعة على الاتفاقية أن مواجهة هذا النوع من الجرائم تتطلب تعاونًا دوليًا، تنص الاتفاقية على مبادئ وإجراءات جديدة لتوجيه جهود مكافحة الجرائم السيبرانية بشكل فعّال، سأوضح ذلك فيما يلي:

١ـ المبادئ الإجرائية العامة:

تشير الاتفاقية في مجال المكافحة الإجرائية إلى بعض المبادئ الإجرائية العامة، والتي تتلخص في الاتي :

- توفير تنسيق بين عناصر الجرائم السيبرانية والقانون الجنائي الوطني، مع تأمين سلطات التحقيق والملاحقة اللازمة لمكافحة جرائم الحواسب.

- إنشاء نظام فعّال للتعاون الدولي يشمل الإجراءات المحلية والتحقيقات الجنائية لمكافحة الجرائم التي تتعلق بتقنية المعلومات وتوثيق الأدلة الإلكترونية.

- إلزام الدول الموقعة على الاتفاقية بتضمين معلومات رقمية أو إلكترونية في قوانينها الداخلية واستخدامها كأدلة قانونية أمام القضاء، مع التركيز على جرائم الحواسب.

- فرض التفعيل الداخلي للإجراءات المشتقة من القوانين الوطنية، مع ترك مسألة تنفيذ وسريان هذه الصلاحيات في إطار النظام القضائي لكل دولة.

- التأكيد على وجوب قبول الدول للأدلة الرقمية والإلكترونية كجزء من الإجراءات الجنائية والقضائية في مواجهة مختلف أشكال الجرائم السيبرانية.

- **الإجراءات الجنائية الجديدة في اتفاقية بودابست :**

نصت هذه الاتفاقية على بعض الإجراءات الجنائية الجديدة لمكافحة الجريمة السيبرانية، وهي كالاتي:

أ. الحفظ السريع للمعطيات المخزنة:

الاتفاقية تنص في المادتين ١٦ و١٧ على إجراء الحفظ السريع للمعلومات المخزنة، بهدف الاحتفاظ بها بسرعة وتأمينها من التلف. يهدف هذا الإجراء إلى تفادي فقدان الأدلة في جرائم الحواسب نتيجة لتغير سريع في البيانات.

ب. تجميع المعلومات الخاصة بالمشتركين:

تحديد أهمية جمع المعلومات حول المشتركين في جرائم الحواسب لتحديد هوية الجاني. تشمل هذه المعلومات معلومات الاستخدام وفترة الاشتراك، مما يسهم في تحقيق العدالة في جرائم الحواسب.

ج. التفتيش المعلوماتي:

تأكيد الحاجة إلى الحصول على إذن رسمي لتفتيش البيانات الإلكترونية، بعد اعتقاد بوجود بيانات تساعد في إثبات جريمة سيبرانية. يجب توفير شروط الحصول على الإذن وضمان فعالية التفتيش وحجز الأدلة.

د. دخول على المعطيات المعلوماتية:

إلزام الدول بتخويل سلطاتها بالتحقيق والدخول على المعلومات المخزنة في نظم المعلومات. يتضمن ذلك التفاعل في الوقت الفعلي لجمع الأدلة الإلكترونية.

ه. اجراء التنصت:

فرض إجراء التنصت كخطوة جديدة في مكافحة الجريمة السيبرانية، مع التأكيد على أن يُجرى بموافقة قضائية. يستخدم لاعتراض المراسلات عبر وسائل الاتصال السلكية واللاسلكية لتحصيل أدلة تثبت وقوع جريمة سيبرانية.

و. لتعاون الدولي:

تشدد الاتفاقية على ضرورة التعاون الدولي لتبادل المعلومات والأدلة بشكل سريع. تنص على ضرورة وجود إجراءات قانونية إضافية لتأمين البيانات التي تستخدم كدليل في الجرائم السيبرانية.

ي. الالتزام والتنفيذ:

تلتزم الدول الأطراف بإصدار التشريعات واتخاذ الإجراءات الضرورية لتنظيم الجريمة السيبرانية وتحديد المسؤوليات الجنائية. يلزم التعاون الدولي بمواجهة التحديات المتعلقة بتحقيق العدالة في جرائم الحواسب وتقديم المجرمين للمحاكمة .هذا وقد طرحت اتفاقية بودابست مسألة مدى إمكانية أن تفرض على مقدمي الخدمات الالتزام بالتجميع والاحتفاظ ببيانات المرور خلال دورة محددة الزمن ؟ . كما ناقشت مشكلة تحديد المصطلحات القانونية التي تستعمل في مجال المكافحة الإجرائية للجريمة السيبرانية هل نبقي على المصطلحات التقليدية المستعملة في الجرائم التقليدية كمصطلح التفتيش والضبط... إلخ (http://conventions.coe.int/Treaty/fr/Reports/Html/185.htm).

أم تستخدم مصطلحات جديدة أقرب إلى مجال التكنولوجيا مع مناقشة مسألة تطور المفاهيم في المجال السيبراني، وهل نحتفظ للتحري والوصول إلى أدلة تثبت قيام جريمة سيبرانية بالمفاهيم التقليدية كالتفتيش والضبط... إلخ أو المفاهيم الجديدة كالولوج النسخ... البقاء غير المشروع.

الفرع الثاني

اتفاقية مجلس أوربا لسنة ٢٠٠٤

اتفاقية مجلس أوروبا تُعد واحدة من أحدث الاتفاقيات الدولية المخصصة لمكافحة الجريمة السيبرانية. أُصدرت هذه الاتفاقية بواسطة المجلس الأوروبي وحظيت بتوقيع اثنين وثلاثين دولة، ودخلت حيز التنفيذ في يوليو ٢٠٠٤. تركز هذه الاتفاقية على تحديد مجموعة من الجرائم التي تؤثر على النظام المعلوماتي وتكشف عن الأساليب التحقيقية المطبقة في هذا السياق. تتضمن هذه الجرائم المختلفة الهجمات على سرية وتكامل وتوافر البيانات أو نظم الحاسوب، مثل جرائم التدخل والاختراق على أجهزة الحاسوب الآلية. كما تشمل الاتفاقية الجرائم ذات الصلة بالمحتوى، مثل الإنتاج أو النشر غير المشروع لمواد إباحية للأطفال عبر النظم المعلوماتية. بالإضافة إلى ذلك، تتعامل مع الجرائم التي تنطوي على انتهاك حقوق الملكية الفكرية، وتحدد الأساليب الإجرائية التي يجب اتباعها في هذا السياق:

١- إرساء كل من إجراء تفتيش وضبط أنظمة الحاسبات الآلية.

٢- إجراء الحفظ السريع لبيانات الحاسب المخزونة التي تم جمعها وحفظها فعليا بمعرفة حائز البيانات وهذا الإجراء هو إجراء تحقيقي جديد وهام خاصة فيما يتعلق بالجرائم التي ترتكب على شبكة الإنترنت.

٣- إجراء الأمر بإصدار نسخة من البيانات يسمح للسلطات المختصة بفرض تقديم المعلومات المخزنة أو المتعلقة بمزود خدمة الإنترنت، مما يُسهم في الحصول على تفاصيل حول المشترك. تركز الاتفاقية بشكل خاص على إجراءات التفتيش والضبط في البيئة المعلوماتية حيث تكون البيانات قابلة للتحليل بشكل ملموس. يعتمد الإجراء على جمع فوري لبيانات الحاسوب، مستندًا إلى جمع فوري لبيانات النقل المرتبطة بوسيلة اتصال في نظام الحاسوب.

٤- إجراء اعتراض بيانات المحتوى في سياق مكافحة الجريمة السيبرانية، حيث يُمكن هذا الإجراء السلطات من الاعتراض على محتوى الاتصال، سواء كانت رسالة أو معلومة منقولة. تأخذ الاتفاقية في اعتبارها خطوات وتدابير متبعة على المستوى الدولي بهدف زيادة فعالية هذا الإجراء، استنادًا إلى توصيات اجتماعات مثل اجتماع إبيك في بانكوك عام ٢٠٠٢، وتوصيات منظمة الدول الأمريكية في نيويورك عام ٢٠٠٤، ومؤتمر الجريمة السيبرانية في ستراسبورغ عام ٢٠٠٤، وقمة رؤساء الدول والحكومات في وارسو عام ٢٠٠٥.

الهدف هو تعزيز كفاءة الاعتراض على محتوى الاتصال على الصعيدين الوطني والدولي. ذلك، وفي إطار المكافحة الإجرائية في اتفاقية المجلس الأوربي يجب التنويه إلى دور هذه الاتفاقية في إنشائها لوحدة Eurojust التي مهمتها التعاون بين دول الإتحاد الأوربي في مجال مكافحة الجريمة السيبرانية بتعاون السلطات القضائية للدول الأعضاء في هذا الإتحاد بمكافحة الجريمة السيبرانية، وذلك بإصدار إجراء جديد جماعي هو أمر القبض الأوربي الذي يسمح بتسليم مجرم سيبراني بسرعة في أي دولة من دول الاتحاد الأوربي.

المطلب الثاني

الآليات الإجرائية لمكافحة الجرائم السيبرانية على مستوى الوطني

بسبب التقدم السريع في التكنولوجيا ووسائل الاتصال، والتطور الملحوظ في مجال تكنولوجيا المعلومات، وظهور الفضاء السيبراني ووسائل الاتصال الحديثة مثل الفاكس والإنترنت، أصبحت الجرائم السيبرانية من بين أخطر الجرائم التي يتم ارتكابها على أنظمة المعلومات وبواسطتها. في هذا السياق، سأتناول الإجراءات التقليدية لمكافحة الجريمة السيبرانية (الفرع الأول)، ثم سأقدم تفصيلاً حول الآليات الحديثة المستخدمة لمواجهة هذه الجرائم الناشئة (الفرع الثاني).

الفرع الاول

الإجراءات التقليدية لمكافحة الجريمة السيبرانية

لقد أثارت الإجراءات التقليدية المعتمدة جدلا فقهيا كبيرا من ناحية صلاحيتها في البيئة الرقمية، وسنكتفي بدراسة الإجراءات التقليدية المتمثلة في التفتيش والمعاينة والخبرة، وذلك لعلاقتها المباشرة بالوسط الرقمي وقابلية تطبيق قواعدها من جهة، ومن جهة أخرى استبعاد الاعتراف والشهادة والاستجواب، كونها لا تثير أي صعوبات ونظرا لخضوعها للقواعد العامة المقررة قانونا ولنرى ذلك بإيجاز فيما يلي:

أولا: التفتيش في البيئة الرقمية:

الرقمية، الإجراء الذي يسمح بجمع الأدلة المخزنة أو المسجلة بشكل إلكتروني، والبحث عن معطيات الحاسب الآلي غير المادية المخزنة في الجهاز أو في الأقراص المضغوطة(الحلبي، ٢٠١١، صفحة١٥٧). ، بهدف إثبات الجريمة السيبرانية ونسبتها إلى مرتكبها. مرتبطة بسبب وقوع الجريمة، ويتطلب توجيه الاتهام نحو الفرد المستهدف للتفتيش، بهدف تنظيم ما يمكن أن يسهم في اكتشاف الحقائق. هناك أيضًا متطلبات شكلية، حيث يجب أن يكون أمر التفتيش مبررًا، ويُفضل حضور المتهم أو وكيله إذا كان ذلك ممكنًا. ويتعين أيضًا توثيق محضر التفتيش. في سياق الجرائم السيبرانية، يشمل موقع التفتيش جميع مكونات الحاسوب، سواء الفعلية أو الافتراضية، بالإضافة إلى الشبكات الاتصال المتصلة بها. سيتم توضيح قابلية فحص هذه المكونات والأفراد الذين يستخدمونها استنادًا إلى القوانين والضوابط النافذة.

١ـ خضوع أنظمة الحاسب الآلي للتفتيش:

بناءً على ما تم ذكره سابقًا، يُمكن القول إن تفتيش أنظمة الحاسوب يتم بإحدى الطريقتين التاليتين:

أـ تفتيش المكونات المادية للحاسب:

تتمثل المكونات المادية لجهاز الحاسب الآلي، في مجموعة من الوحدات المتصلة فيما بينها بشكل يجعلها تعمل كنظام متكامل(الحلبي، مرجع سابق، ٦٧)، وهي: وحدات الإدخال مثل الفارة ولوحة المفاتيح ووحدات الإخراج مثل شاشة الحاسب الآلي والطابعة، وأخيرا الذاكرة (الطوالبة،٢٠٠٤، صفحة ١٩) . يسهل معاينة القائمين بالتفتيش للمكونات المادية للحاسوب، حيث لا توجد صعوبة بسبب عدم تعارض هذا التفتيش مع المفهوم التقليدي. يعد التفتيش في هذه الحالة بحثًا عن الأدلة المادية، ويجب أن يتم وفقًا للقواعد القانونية والإجراءات المحددة في قانون الإجراءات الجنائية.

ب – تفتيش المكونات غير المادية للحاسب:

وهي تسمى أيضا بالمكونات المعنوية لجهاز الحاسب الآلي، وهي عبارة عن مجموعة من البرامج والملفات المتعلقة بتشغيل وحدة معالجة البيانات، وتنقسم إلى كيانات أساسية تضم البرامج الضرورية التي يتم من خلالها تشغيل واستخدام جهاز الحاسب الآلي، وكيانات تطبيقية تضم برامج تمكن المستخدم من أن ينفذ بواسطتها عملا معينا بإستخدام جهاز الحاسب . وعلى هذا الأساس، فإن المكونات غير المادية للحاسب، وهي البرامج أو الكيانات المنطقية، تشمل ما يأتي(بكري، ٢٠١١،ص٦٨):

- البيانات المسجلة في ذاكرة الحاسب أو في مخرجاته.

- السجلات المثبتة لاستخدام نظام المعالجة الآلية للبيانات.

- دفتر يومية التشغيل وسجل المعاملات.

- السجلات الخاصة بعمليات الدخول إلى نظام المعالجة الآلية للبيانات وما يتعلق بعا من سجلات كلمات السر، ومفاتيح الدخول، ومفاتيح فك الشفرة.

٢- خضوع شبكات الاتصال الخاصة بالحاسب الآلي للتفتيش:

مما لا شك فيه أن طبيعة الجريمة السيبرانية تزيد من صعوبة القيام بهذا الإجراء، فالبيانات التي تتضمن أدلة قد تتوزع عبر شبكات الحاسب الآلي في أماكن قد تكون على مسافات بعيدة عن الموقع المادي الذي يتم فيه التفتيش هذا من جهة، ومن جهة ثانية قد يكون الموقع الفعلي للبيانات خارج اقليم الدولة التي صدر فيها الإذن بالتفتيش، وهو ما يصعب تنفيذ هذه العملية حيث تواجه سلطات التحقيق مشكلة كبيرة تتمثل في مدى امكانية تنفيذ اجراءات البحث والتفتيش في اقليم دولة أخرى، وهو ما يسمى بالتفتيش العابر للحدود(الغافري، ٢٠٠٩،صفحة٣٧٦) والحقيقة، أن المسلم به في الفقه الجنائي، هو أنه لا يجوز السلطات التحقيق التابعة لدولة ما اللجوء إلى التفتيش العابر للحدود لاسترجاع بيانات مخزنة في الخارج إلا في اطار اتفاقات تعاون خاصة ثنائية أو جماعية تجيز وتنظم هذا الامتداد أو اطار الإنابة القضائية المتبادلة، أو على الأقل بعد الحصول على الإذن الصريح من الدولة الأجنبية، وفي ظل غياب هذه الاتفاقات والإذن بعد الاختراق المباشر انتهاكا فعليا لسيادة الدولة. ولكن تحسبا لطابع السرعة الفائقة الذي يجري عليه نقل المعلومات الإجرامية وتهريبها للخارج بقصد تخزينها واخفائها، وما يستدعيه من الاستعجال في تعقب آثارها وضبطها لاستعمالها كدليل إثبات، وسعت بعض التشريعات المقارنة من صلاحيات سلطات التحقيق للقيام بتفتيش الأنظمة المتصلة حتى لو كانت متواجدة خارج اقليمها الوطني، وقرنت ذلك بحالة الضرورة. وجدير بالذكر أن اتفاقية بودابست لعام ٢٠٠١ قد حسمت هذه المسألة، بالنص صراحة في المادة ٣٢منها على امكانية الدخول بغرض التفتيش والضبط في أجهزة أو منظومة معلوماتية تابعة لدولة أخرى بدون الحصول على إذن مسبق من هذه الأخيرة، في حالتين، وهما :

١. إذا تعلق التفتيش بمعلومات أو بيانات متاحة للجمهور.

٢. إذا رضي صاحب أو حائز هذه المعلومات بهذا التفتيش. وقد اقترحت لجنة الدول أطراف هذه الاتفاقية على اثر المناقشات التي أجرتها في عام ٢٠٠٩اضافة حالات أخرى إلى الحالتين المشار إليهما في المادة٣٢من الاتفاقية. (تم وضع هذا المرشد عام ١٩٩٤ في عهد وزارة النائب العام السير Jenat Reno وهو من اعداد قسم جرائم الحاسب والملكية الفكرية بوزارة العدل الأمريكية، وقد صدر له ملحان في عامي ١٩٩٧\١٩٩٩، ولقد قام بإعداده مجموعة عمل في قسم جرائم الحاسب الآلي والملكية الفكرية بإشراف أستاذ القانون الجنائي Orin Kerr، ليكون معينا للسلطات في ضبط جرائم الحاسب والإنترنت، ولقد ادخلت عليه تعديلات منها تعديل عام ٢٠٠٢ بعد احداث ١١ سبتمبر ٢٠٠١ الذي تضمن تطبيقا للقانون الوطني الأمريكي الصادر في ٢٠٠١\١٠\٢٦، وآخرها تعديل عام ٢٠٠٥، وجاء في مقدمة هذا المرشد أن التزايد المستمر في الجرائم المرتبطة بالحاسب يتطلب من جهات التحقيق والمسئولين عن تنفيذ القانون ادراك كيفية الحصول على دليل إلكتروني مخزن في الحواسب، وجاء أيضا أن الغرض من هذا المرشد هو تزويد المسئولين عن تنفيذ القانون وجهات التحقيق بكتاب منظم يمكن أن يساهم في فهم القضايا القانونية التي تظهر عند القيام بالبحث عن دليل إلكتروني في التحقيقات الجنائية، الصغير، مرجع سابق، صفحة ١٩٧) هي:

١- حالة التفتيش عن بعد بحسن نية.

٢- حالات الاستعجال القصوى أو الحالات الاستثنائية.

٣- حالة التفتيش عن بعد وفقا لمعيار مشروعية التفتيش سلطة الاستعمال.

٤- وتفتيش نظم الحاسب الآلي يمكن أن يتم بعدة طرق، وفي هذا الصدد جاء المرشد الفيدرالي الأمريكي لتفتيش وضبط الحواسب وصولا إلى لدليل الإلكتروني في التحقيقات الجنائية.

الفرع الثاني

مكافحة الجريمة السيبرانية بالوسائل الإجرائية المستحدثة

تم تبني عدة إجراءات جديدة لمكافحة الجريمة السيبرانية، وتستهدف هذه الإجراءات تقديم دلائل قاطعة حول وقوع الجريمة، والكشف عن هوية الفاعل من خلال الاستفادة من برامج وتقنيات إلكترونية متنوعة، وذلك استنادًا إلى توجيهات المشرع لمكافحة هذا النوع من الجرائم. يتمثل ذلك في تبني تقنيات مثل اعتراض المراسلات ونظام التسريب، ونظام المراقبة الإلكترونية، بالإضافة إلى الاستفادة من التعاون الدولي في المجال القضائي لمكافحة الجريمة السيبرانية. سأوضح هذه الوسائل بالتفصيل فيما يلي:

أولا: اعتراض المراسلات الإلكترونية:

ويمكن القول أن هذه العملية تنصب عادة على رسائل البريد الإلكتروني، حيث يعتبر هذا الأخير من أهم الوسائل الحديثة للاتصال في مجال الإنترنت، وهو بمثابة نظام للتراسل عن طريق شبكة الإنترنت، إذ يحتوي على العديد من المعلومات كتاريخ إنشاء الرسالة وتاريخ إرسالها أو تلقيها، وكذا عنوان المرسل وعنوان المرسل إليه، ولكن تبقى المعلومات التي تحتويها حاشية رسالة البريد الإلكتروني هي الأهم، بحيث تتضمن على عنوان التعريف لمرسل الرسالة، بحيث يتكون هذا العنوان من أربعة أجزاء يشير الجزء الأول من اليسار إلى المنطقة الجغرافية، والجزء الثاني المزود الخدمة ، لمجموعة الحاسبات الالية المترابطة، وأما الجزء الرابع فيحدد الحاسب الآلي الذي تم الاتصال بواسطته (زيبحه ،٢٠١١، صفحة ١٥٩) .

ثانيا التسرب الإلكتروني:

التسرب الإلكتروني يشير إلى الكشف غير المصرح به عن معلومات أو بيانات إلكترونية، سواء كان ذلك ناتجًا عن هجوم إلكتروني أو خرق أمان أو إهمال في التعامل مع المعلومات الرقمية. يمكن أن يشمل التسرب الإلكتروني سرقة البيانات، والتجسس الإلكتروني، وفقدان السيطرة على البيانات، والتسريب العرضي للمعلومات، والهجمات السيبرانية الأخرى. تكون المعلومات التي قد تتسرب متنوعة، بما في ذلك المعلومات الشخصية، والمعلومات الحساسة للشركات، والبيانات الحكومية. يمكن أن يكون للتسرب الإلكتروني تأثير كبير على الأفراد والشركات، بما في ذلك فقدان الخصوصية، والسرقة الهوية، والتأثير الاقتصادي الضار. لحماية أنفسهم من التسرب الإلكتروني، يجب على الأفراد والمؤسسات اتخاذ إجراءات أمان رقمي فعالة، مثل تحديث البرامج والأنظمة بانتظام، واستخدام كلمات مرور قوية، وتفعيل التحقق الثنائي للدخول إلى الحسابات الرقمية، وتوعية المستخدمين حول مخاطر الهجمات السيبرانية.

ثالثا: المراقبة الإلكترونية:

تعتبر المراقبة من أهم مصادر التحري التي غالبا ما يستعان بها في البحث والتقصي عن الجرائم، سواء تلك التقليدية أو المستحدثة كجرائم الإنترنت، وهي ما يعرف بـ المراقبة الإلكترونية(هروال،٢٠١٩،صفحة١٩٧. الرقابة الإلكترونية هي عملية استخدام التقنيات الرقمية لرصد ومراقبة الأنشطة الإلكترونية، سواء على مستوى الأفراد أو الكيانات الحكومية أو الشركات. يشمل ذلك تحليل وتتبع البيانات الرقمية، مثل استخدام الإنترنت، والاتصالات الإلكترونية، وسجلات النشاط على الأجهزة الرقمية. يمكن تنفيذ هذه الرقابة لأغراض متنوعة، من الأمان الوطني إلى مراقبة أنشطة الموظفين في بيئة العمل، وقد تثير قضايا حول حقوق الخصوصية والحريات الفردية.

رابعاً: المساعدة القضائية في مجال مكافحة الجرائم السيبرانية :

تعد المساعدة القضائية المتبادلة في المسائل الجنائية من الآليات الفعالة لمواجهة جرائم السيبرانية خصوصا لما للتعاون في مجال الإجراءات الجنائية من دور مهم في التوفيق بين حق الدولة في ممارسة اختصاصها الجنائي داخل حدودها الإقليمية وحقها في توقيع العقاب (سرور، ١٩٩٦، صفحة٩١). وتعرف المساعدة القضائية الدولية، بأنها كل إجراء قضائي تقوم به دولة من شأنه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم وتتخذ المساعدة القضائية في المجال الجنائي صور عدة، كما أنه قد تكون هذه المساعدة رسمية أو غير رسمية.

الخاتمة:

في ختام بحثي، يظهر أن الجريمة السيبرانية أصبحت ظاهرة بارزة في العالم الحديث، وقد شهدت زيادة في تكرارها خلال الفترة الأخيرة. تعتبر هذه الجرائم من الأنواع الخطيرة التي لا تقتصر تأثيراتها على الأفراد فقط، بل تتعدى ذلك لتطال سلامة وأمان واستقرار الدول. تنوعت آفاق الجريمة السيبرانية لتشمل مختلف القطاعات والجوانب الحيوية في المجتمع، من القضايا الشخصية إلى التأثير الكبير على الهياكل الوطنية. **قد توصلت الباحثة خلال بحثها هذا إلى النتائج التالية:**

١- يبرز أن الجريمة السيبرانية تشكل تحديًا حقيقيًا يتطلب تعاونًا دوليًا لمواجهتها بفعالية.

٢- يتضح أن هذه الجرائم تفرض ضغوطًا كبيرة على الأنظمة الأمنية والقانونية، مما يستلزم التطور المستمر للسياسات والتشريعات لمكافحتها.

٣- يتضح أنه يجب توعية الأفراد والمؤسسات بأهمية الأمان السيبراني وتبني إجراءات وقائية للحد من تأثيرات هذه الجرائم المتزايدة.

٤- تعتبر الجريمة السيبرانية من الآثار السلبية التي خلفتها الثورة التكنولوجية الهائلة التي يشهدها العالم.

٥- التفاوت في تسميات وتصنيفات الجرائم السيبرانية يظهر عدم الاستقرار في الفهم القانوني، حيث يُطلق عليها ببساطة "الجريمة الإلكترونية" أو "الجريمة التي تحدث عبر الإنترنت". هذا الاختلاف ينتج عن ظهور جرائم جديدة متأثرة بتقنيات حديثة.

٦- تتميز الجريمة السيبرانية في أنها من جرائم التي يصعب اكتشافها وإثباتها أمام القضاء ، كما تعد من الجرائم عابرة للحدود لا تعترف بالحدود الزمانية والمكانية.

ومن خلال النتائج التي تم التوصل إليها نقترح مجموعة من التوصيات التي تتجسد فيما يلي:

١- يتعين بشكل حاسم إيجاد وسائل فعّالة لتعزيز التعاون الدولي في مواجهة الجريمة الإلكترونية، وذلك من خلال تحقيق توافق بين التشريعات المتعلقة بها من خلال الاتفاقيات الدولية. يكمن أهمية ذلك في الاستفادة من مصادر المواقع العلمية التي تُعتبر ذات قيمة في فهم أوجه التواصل الاجتماعي وتحليلها.

٢- تحديث وتعديل وسائل البحث والتحقيق يصبح ضروريًا، خاصة في مجال الجرائم الإلكترونية حيث لا تترك آثارًا واضحة. يُشدد على أهمية تقليص أو تجاوز الإجراءات الروتينية الطويلة التي تستهلك وقتًا كبيرًا.

٣- على المشرع العراقي أن يسارع في إصدار قوانين خاصة تتناسب مع طبيعة الجرائم الإلكترونية المتطورة، أو يقوم بتعديل القوانين الجنائية ليتم تضمين هذه الجرائم في إطار قانوني.

٤- يتعين إعادة النظر في قانون أصول المحاكمات الجزائية العراقي وقانون الإثبات، خاصة فيما يتعلق بوسائل إثبات الجرائم الإلكترونية والتفريق بينها وبين الجرائم العادية.

٥- تهيئه رقابة على شبكات الانترنت لحذف الافكار التي لا تتفق مع المفاهيم اللا أخلاقية للدول.

المراجع:

الكتب العامة:

١. أحمد فتحي سرور ،الوسيط في قانون العقوبات ،القسم العام ،دار النهضة العربية ، ١٩٩٦.

٢. بكري يوسف بكري، التفتيش عن المعلومات في وسائل التقنية الحديثة، دار الفكر الجامعي، ٢٠١١.

٣. بهاء المري، شرح جرائم تقنية المعلومات، منشاة المعارف، ٢٠١٩.

٤. جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، دار النهضة العربية،١٩٩٢.

٥. رؤوف عبيد، السببية في القانون الجنائي ، مطبعة الاستقلال، ١٩٩٦.

٦. شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية ، دار الجامعة الجديدة،٢٠٠٧.

٧. عبد الفتاح بيومي الحجازي ، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنيت، بهجان للطباعة والتجليد،٢٠٠٩.

٨. علي حسن محمد الطوالبة ، التفتيش الجنائي على نظم الحاسوب والإنترنت، عالم الكتب الحديث، الأردن ،٢٠٠٤.

٩. فريد روابح، محاضرات في القانون الجنائي العام ، مطبوعة الدروس لسنة الثانية ليسانس، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد لمين دباغين، سطيف ، ٢٠١٨\٢٠١٩.

١٠.محمود نجيب حسني، الفقه الجنائي الإسلامي، دار النهضة العربية، ٢٠٠٧.

الكتب الخاصة:

١. بلال أمين زين الدين، جرائم نظم المعالجة الآلية للبيانات، دار الفكر الجامعي، ٢٠٠٨.

٢. خالد عياد الحلبي، إجراءات التحقيق في جرائم الحاسوب والانترنت، دار الثقافة للنشر والتوزيع، عمان،٢٠١١.

٣. خالد ممدوح إبراهيم، جرائم المعلوماتية على شبكة الإنترنيت، دار الفكر الجامعي ، ٢٠٠٩.

٤. زيدان زيبحه ،الجريمة المعلوماتية في التشريع الجزائري والدولي ، دار الهدى للطباعة والنشر والتوزيع، عين مليلة، الجزائر ،٢٠١١ ، ص ١٥٩.

٥. ممدوح عبد الحميد عبد المطلب، جرائم استخدام الكمبيوتر وشبكة المعلومات العالمية ، دار الفتح للطباعة والنشر ، الامارات (الشارقة)، ٢٠٠٠.

٦. محمود سعد عبد المجيد، الجرائم السيبرانية وانعكاسات ثورة تكنولوجيا المعلومات والاتصال على النظرية العامة للجريمة من حيث أسباب التكوين والأركان والعناصر وأساسيات المكافحة الجنائية ، دار المطبوعات الجامعية، الإسكندرية ، ٢٠٢٣.

٧. عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن الإنترنيت، بدون ذكر دار النشر،٢٠٠٣.

٨. نبلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنيت، دار الفكر الجامعي، الاسكندرية ، ٢٠١٩.

الرسائل الجامعية والمقالات:

١. حسين بن سعيد بن سيف الغافري، السياسية الجنائية، السياسة الجنائية في مواجهة جرائم الانترنت، السياسة الجنائية في مواجهة جرائم الانترنت، رسالة لنيل درجة الدكتوراه ،كلية الحقوق، جامعة عين شمس، دار النهضة العربية،٢٠٠٩.

٢. رابحي عزيزة، الأسرار المعلوماتية وحمايتها الجزائية، رسالة لنيل درجة دكتوراه في العلوم القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد – تلمسان،٢٠١٨.

٣. علي حمزة عسل، الظروف القضائية المخففة في القانون العراقي، رسالة لنيل درجة ماجستير في القانون ،كلية القانون، جامعة بغداد،١٩٩٠.

٤. عبد المؤمن الصغير، الطبيعة الخاصة للجريمة الإلكترونية المرتكبة عبر الأنترنيت في التشريع الجزائري والتشريع المقارن، مجلة الحقوق و الحريات، جامعة محمد خيضر، بسكرة، المجلد٠٢، ٢٠١٤.

٥. مرابطن حياة ، الجريمة الإلكترونية في التشريع الجزائري، رسالة لنيل درجة ماجستير، كلية الحقوق والعلوم السياسية - جامعة عبد الحميد بن باديس مستغانم – الجزائر،٢٠١٨\٢٠١٩.

٦. هدى سالم محمد الاطرقجي، التكيف القانون للجرائم في القانون العقوبات العراقي، رسالة لنيل درجة دكتوراه كلية القانون جامعة الموصل،٢٠٠٠.

٧. يوسف الصغير، الجريم المرتكبة عبر الأنترنيت، رسالة مقدمة لنيل درجة ماجستير في كلية الحقوق والعلوم السياسة، جامعة مولد معمر، تيزي وزي ، ٢٠١٢\٢٠١٣.

٨. http://conventions.coe.int/Treaty/fr/Reports/Html/185.htm

٩. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri= CELE X