وزارة التعليم العالي والبحث العلمي

جامعة اكلي محند أولحاج – البويرة

كلية الحقوق والعلوم السياسية

تأثير خصوصية الجريمة الإلكترونية على آليات مكافحتها

مذكرة مقدمة ضمن متطلبات نيل شهادة ماستر تخصص قانون جنائي

إعداد الطلبة:

- مازوز ليلى
- جوهري نصيرة

تحت إشراف :

- د. صغير يوسف

الأستاذ(ة): .....رئيسا

الأستاذ(ة): .....مشرفا

الأستاذ(ة): .....مناقشا

السنة الجامعية: 2023-2024


بسم الله الرحمن الرحيم

كلمة شكر وعرفان

يسرني أن أتقدم بجزيل الشكر والعرفان

إلى اللجنة الموقرة التي قبلت مناقشة هذه المذكرة المتواضعة

كما أتقدم بجزيل الشكر

إلى الذي شجعني ووقف وراء هذا العمل المتواضع

بمجهوداته ونصائحه القيمة التي أنارت طريقي

أستاذي المشرف "الدكتور صغير يوسف"

إهداء

أهدي ثمرة جهدي

إلى روح أبي الطاهرة

راجيا من الله عز وجل أن يسكنه جنة الفردوس

وإلى من تنحني هامتي لها

وأشد أزري بها إلى أمي العزيزة حفظها الله

وإلى كل إخوتي وأخواتي والعائلة الكريمة

إلى أستاذي الكريم صغير يوسف

وكل أساتذتي والموظفين في كلية الحقوق والعلوم السياسية

الذين أكرموني وساعدوني كثيرا

إلى جميع الأصدقاء والأحباب

ليلى

إهداء

أهدي ثمرة جهدي

إلى أبي الغالي و أمي العزيزة

حفظهما الله ورعاهما

إلى زوجي العزيز الذي كان سندا لي و إلى أولادي

وإلى كل إخوتي وأخواتي والعائلة الكريمة

إلى أستاذي الكريم صغير يوسف

وكل أساتذتي والموظفين في كلية الحقوق والعلوم السياسية

الذين أكرموني وساعدوني كثيرا

إلى جميع الأصدقاء والأحباب

نصيرة

مقدمة

خلق الله الإنسان في أحسن تقويم وفضله على سائر المخلوقات بصفة العقل الذي طور به نفسه والمجتمع وعلى مر العصور وبعد الأكتشافات عديدة واختراعات في شتى المجالات اقتصادية، صناعية، وإلكترونية وغيرها.

هذه الأخيرة ظهرت بعد الثورة الصناعية وتطورت كثيرا مؤخرا وتطورها جاء بايجابيات أفادت المجتمع، وسلبيات كثيرة أدت إلى حصول جرائم في المجتمع تعرف بالجريمة الإلكترونية فالجرائم بعد تطور المجتمع في مختلف المجالات اختلفت عن الجرائم التي كانت ترتكب قديما، وذلك باختلاف الزمان والمكان فمثلا التي ترتكب في مكان ما غير الجرائم، التي ترتكب في مكان آخر، وهذا راجع للإختلاف الموجود بين أفراد المجتمع وحتى الدول من حيث المستوى الثقافي العلمي، الفكري، وحتى الديني.

فبالتطور الحديث الإلكتروني والمعلوماتي أصبحت الجريمة عابرة للدول والقارات والمحيطات لأن هذا التطور الحديث في المعلوماتية أصبح العالم قرية صغيرة، ليجعل الجريمة الإلكترونية طابع متعدد الحدود يهدد الأمن والإستقرار الدولي والعالمي، فالجريمة الإلكترونية حسب تعريفها القانوني عند المشرع الجزائري بموجب المادة 02 من القانون 09-04 على أنها: " جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، وأي جريمة أخرى يسهل إرتكابها أو ترتكب ع، ط منظومة معلوماتية أو نظام الإتصالات الإلكترونية"[1].

كما بيّنها في قانون العقوبات من المواد 334 مكرر[2]. وقد اصطلح المشرع الجزائري على تسميتها بمصطلح الجرائم المتصلة بالتكنولوجيا الإعلام والإتصال، فمن أمثلة الجريمة الإلكترونية في الجزائر تسرب أسئلة البكالوريا لسنة 2016، قيام القرصان الجزائري حمزة بن

[1] المادة 02 من القانون 09-04 الصادر في 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية العدد 47 المؤرخة في 16 أوت 2009.

[2] القانون رقم 04-15 الصادر في 10 نوفمبر 2004 يعدل ويتمم الأمر رقم 66-156 الصادر في 08 جوان 1966 المتضمن قانون العقوبات الجريدة الرسمية، العدد 71.

دلاج بقرصة حسابات شبكة العالمية، والذي ألقي القبض عليه من طرف الشرطة الفيدرالية الأمريكية[1].

أما التعريف الفقهي للجريمة الإلكترونية فهناك إتجاهين، فيرى الإتجاه المضيق أنها: كل فعل يمر مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازم ارتكابه (ملاحقته) من ناحية، وملاحقته وتحقيقه من ناحية أخرى"[2].

الإتجاه الموسع يعرفها أنها: " كل جريمة تتم بوسيلة إلكترونية كالحاسوب مثلا، وذلك باستخدام شبكات الأنترنت خلال غرف الدردشة وإختراق البريد الإلكتروني ومختلف وسائل التواصل الإجتماعي بهدف إلحاق الضرر للفرد والمجتمع وحتى للدولة ضمن برنامج استهداف الفردي او الإقتصادي أو الإضرار بسمعتها أو الكشف عن قضايا متستر عليها أو نشر معلومات لفائدة أطراف أخرى من باب التسريب[3] وبذلك نجد أن دوافع ارتكاب هذه الجريمة الإلكترونية تكون شخصية وموضوعية، فالشخصية منها المادية، وذلك لتحقيق الربح ويحقق أعلى المكاسب وبأقل جهد دون أن يترك أثرا وراءه.

ومنها ذهنية فتأثير العنصر الذهني على المجرم الإلكتروني ودفعه لارتكاب الجريمة وتتمثل في المتعة والتحدي والرغبة في فهم النظام المعلوماتي وإثبات الذات، أما الدوافع الموضوعية تدفع المجرم لإقتراف الجرم الإلكتروني كدوافع الإنتقام وإلحاق الضرر برب العمل، فلا يسعى من خلالها للمتعة والتسلية ولا لكسب المال، كما يوجد دافع التعاون والتواطؤ وغالبا ما يحدث بين مختصين في الأنظمة المعلوماتية.

---

[1] جازية سليماني ، موقع العربي الجديد، تاريخ الإطلاع، 2017/02/09 الساعة 30:h20
الموقع: http://www.alraby.com/uk/medianews

[2] حشيفة عبد الهادي التعاون الدولي في مجال مكافحة الجرائم الإلكترونية، مذكرة ماستر في الحقوق تخصص قانون جنائي الموسم الجامعي 2019-2020 جامعة زيان عمشور الجلفة

[3] سميرة بيطام، الجريمة الإلكترونية وتقنية الإجرام المستحدث ص1-4. تاريخ الإطلاع: 2016/11/30،
الموقع: http://alukah.net/culture/

ومع إختلاف الأسباب والعوامل والدوافع لارتكاب الجريمة الإلكترونية، جاءت هذه الأخيرة بأركان لها كغيرها من الجرائم، لها ركن شرعي وهو الصفة الغير مشروعية للفعل، والركن المادي يتمثل في ماديات الجريمة التي تبرز بها إلى العالم الخارجي وأخيرا الركن المعنوي وهو الإرادة التي تقترن بها الفعل سواء في صورة القصد أو الخطأ في الجريمة الإلكترونية، وبذلك تتنوع هذه الجرائم بحسب القانون الجزائري قسمها إلى جرائم مرتكبة باستخدام النظام المعلوماتي وجرائم واقعة على النظام المعلوماتي، أما الأولى فتنقسم بدورها إلى جرائم واقعة على حقوق الملكية الفكرية وقد نص عليه المشرع في الأمر رقم 03-05 الصادر في 2003 المتعلق بحقوق المؤلف والحقوق المجاورة والأمر 03-07 الصادر في 2003 المتعلق ببراءات الإختراع[1]، وهناك جرائم واقعة على حرمة الحياة الخاصة وكلها جرائم واقعة على الأشخاص الطبيعية وغيرها واقعة على نظم المعلوماتية أخرى وغيرها واقعة على الأسرار[2]، أما الثانية وهي الجرائم الإلكترونية الواقعة على النظام المعلوماتي ومنها جريمتي الدخول والبقاء غير المشروعان في منظومة معلوماتية وقد نصت عليها م 394 مكرر من ق ع جريمة المساس بمنظومة معلوماتية وقد نصت فيها م394 مكرر1 من ق العقوبات وثم 04-15 أفعال إجرامية أخرى نصت عليهم المادة 394 مكرر 2 من قانون العقوبات[3] كتصميم أو بحث أو تجميع أو توفير أو نشر أو الأتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق معلوماتية[4].

---

[1] سوير سفيان، جرائم معلوماتية، مذكرة لنيل شهادة ماجيستير في العلوم الجنائية وعلم الإجرام جامعة أبو بكر بلقايد تلمسان، 2010-2011 ص34-35.

[2] صغير يوسف، الجريمة المرتكبة عبر الأنترنت مذكرة لنيل شهادة ماجيستير في القانون تخصص قانون الدولي للأعمال كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو 2013، ص54.

[3] الأمر رقم 04-15 القانون السابق الذكر.

[4] حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي بحث مكمل لنيل شهادة الماجيستار في العلوم القانونية، تخصص علم الإجرام وعلم العقاب، جامعة الحاج لخضر باتنة 2011-2012، ص184

وفي غضون تطور هذه الجريمة الإلكترونية وتنوعها ما أدى إلى ضرورة وضع آليات من أجل مكافحتها لأنه مع التطور العلمي أصبحت من أسهل الوسائل التي يعتمد عليها مرتكبي الجريمة بدون بذل جهد ولا وقت فقد وضعت الدولة مختلف الآليات القانونية والمؤسساتية لمكافحة هذا النوع من الجرائم والآليات القانونية التي سنها المشرع الجزائري يوجد منها الموضوعية وهي التشريعات والقوانين كالقانون العام وما جاء في القانون الدولي العام وكذلك في القانون الإداري باعتباره من أقسام القانون العام فالقانون المتعلق بالتوقيع الإلكتروني جاء في قانون رقم 15-03 المؤرخ في 2015/02/01 المتعلق بعصرنة العدالة جريدة رسمية رقم 06 والقانون رقم 18-07 وغيرها

أما في قانون العقوبات جاء في قانون رقم 04-15 المؤرخ في 2004/11/10 تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات جاءت عدة أوامر وقوانين أخرى بعده، وفي قانون المالية رقم 17-04 المؤرخ في 2017/02/16 والمتضمن قانون الجمارك.

أما في القانون الخاص فيوجد عدة تشريعات وأوامر في القانون الدولي الخاص والقانون المدني والتجاري وقانون العمل، أما الآليات القانونية الإجرائية فجاءت عدة تعديلات في قانون الإجراءات الجزائية الإجرائية وعدة قوانين ومراسيم كالمرسوم الرئاسي رقم 20-183 الذي يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها.

كما دخل عدة تعديلات في الإجراءات المدنية، أما الآليات المؤسساتية كمؤسسات مرحلة التحري والمتابعة والمؤسسات القضائية والعقابية في المحاكم العادية والمتخصصة بالنظر في الملفات الخاصة بالجريمة الإلكترونية.

إلا أن هذه الآليات الخاصة سواء مؤسساتية أو قانونية لمكافحة الجريمة الإلكترونية اصطدمت مع الطبيعة الخاصة لهذه الجريمة مما جعلها غير فعالة نظرا لسهولة ارتكابها

وسرعتها وتطورها الدائم الأمر الذي جعل الدول وخاصة المتقدمة منها تقوم بالمحاولة والبحث المستمر لإيجاد صيغ قانونية يمكن من خلالها الحد من هذه الجرائم المستحدثة وعدم تأثيرها على الفرد والمجتمع وعدم تأثير خصوصية الجريمة الإلكترونية على آليات مكافحتها.

ومنه نطرح الإشكال: كيف يكون تأثير خصوصية الجريمة الإلكترونية على آليات مكافحتها؟

الفصل الأول

خصوصية الطبيعة التقنية

للجريمة الإلكترونية

تمهيد:

في عصرنا الحالي، أصبحت التكنولوجيا الرقمية جزءًا لا يتجزأ من حياتنا اليومية، مما فتح المجال أمام نوع جديد من الجرائم التي تُرتكب باستخدام أجهزة الكمبيوتر والإنترنت. تُعرف هذه الجرائم باسم "**الجرائم الإلكترونية**" وتشمل مجموعة واسعة من الأنشطة غير القانونية مثل القرصنة والاحتيال والتشهير وانتهاك حقوق الملكية الفكرية وغيرها. نظرًا لطبيعتها المعقدة والتقنية، تواجه الجرائم الإلكترونية تحديات كبيرة فيما يتعلق باكتشافها وإثباتها، حيث تتطلب مهارات وأدوات متخصصة للتعامل مع الأدلة الرقمية.

كما تنطوي هذه الجرائم على مجموعة متنوعة من الأطراف المتضررة، بما في ذلك المستهلكين والشركات والمؤسسات الحكومية، إضافة إلى سلطات التحقيق التي تواجه صعوبات في التعامل مع هذا النوع الجديد من الجرائم.

سنتناول في هذا الفصل، جوانب مختلفة من الجريمة الإلكترونية، بدءًا بالتحديات المرتبطة باكتشافها وإثباتها، ثم سنتطرق إلى أطرافها المتعددة وسلطات التحقيق فيها. كما سنركز على شخصية الجاني في هذه الجرائم، ودوافعه، وخصائصه المميزة، إلى جانب التحديات التي تواجهها السلطات في تعقبه وملاحقته قضائيًا.

المبحث الأول: من خلال اكتشاف وإثبات الجريمة الالكترونية

المبحث الثاني: من خلال أطرف الجريمة الالكترونية وسلطات التحقيق فيها

المبحث الأول: من خلال اكتشاف وإثبات الجريمة الالكترونية

شهدنا العصر الرقمي الحالي، تطورًا متسارعًا في تكنولوجيا المعلومات والاتصالات، والذي فتح المجال أمام نوع جديد من الجرائم التي تُرتكب باستخدام أجهزة الكمبيوتر والإنترنت. نظرًا لطبيعتها المعقدة والتقنية، تواجه الجرائم الإلكترونية تحديات كبيرة فيما يتعلق باكتشافها وإثباتها. فعلى عكس الجرائم التقليدية التي تترك آثارًا مادية واضحة، تكون الأدلة في الجرائم الإلكترونية عبارة عن بيانات رقمية معقدة ومشفرة في كثير من الأحيان، مما يتطلب مهارات وأدوات متخصصة للتعامل معها.

المطلب الأول: اكتشاف الجريمة الالكترونية

في عصر التكنولوجيا الرقمية، أصبحت الجريمة الإلكترونية تهديداً متزايداً يعترض الأفراد والمؤسسات على حد سواء. يشمل اكتشاف الجريمة الإلكترونية تحديد وتحليل الأنشطة غير المشروعة التي تُنفَّذ عبر الإنترنت.

الفرع الأول: إحجام الجهات المتضررة عن التبليغ

تواجه عملية كشف وتحقيق الجرائم الإلكترونية تحديًا كبيرًا يتمثل في فقدان الآثار التقليدية للجريمة. فبخلاف الجرائم التقليدية التي تترك آثارًا مادية واضحة مثل بصمات الأصابع أو أدلة جنائية أخرى، فإن الجرائم الإلكترونية تتميز بطبيعتها الافتراضية والرقمية، مما يجعل من الصعب العثور على أدلة ملموسة تساعد في تحديد هوية الجناة وإثبات تورطهم. ففي العالم الرقمي، يتم ارتكاب الجرائم عبر شبكات الإنترنت وأنظمة الحاسوب، حيث لا تترك آثارًا مادية مباشرة على مسرح الجريمة. بدلاً من ذلك، تكون الأدلة الرئيسية عبارة عن بيانات رقمية وملفات وسجلات إلكترونية، والتي قد تكون معقدة وصعبة الفهم للمحققين غير المتخصصين في مجال التقنية.[1]

[1] – محمد أمين الشوابكة، جرائم الحاسب الآلي والإنترنت، ط1، دار الثقافة للنشر والتوزيع، عمان، 2009، ص:125.

وتزداد هذه المشكلة تعقيدًا عندما يستخدم مرتكبو الجرائم الإلكترونية تقنيات التشفير وإخفاء الهوية والتخفي عبر شبكات افتراضية خاصة، مما يصعب عملية تتبع آثارهم الرقمية. كما أن طبيعة الإنترنت العابرة للحدود تضيف تحديًا إضافيًا، حيث يمكن ارتكاب الجريمة من أي مكان في العالم، مما يتطلب تعاونًا دوليًا في التحقيقات. لذلك، تحتاج السلطات المختصة إلى تطوير قدراتها التقنية وتدريب خبراء متخصصين في التحقيق الرقمي والتحليل الالكتروني، حتى تتمكن من جمع الأدلة الرقمية وتحليلها بشكل فعال. كما يجب تعزيز التعاون الدولي في مجال مكافحة الجرائم الإلكترونية، والعمل على تطوير القوانين والإجراءات التي تسهل عملية التحقيق والملاحقة القضائية في هذا النوع الجديد من الجرائم.[1]

كما يمثل مشكل إحجام الجهات المتضررة عن التبليغ عن الجرائم الإلكترونية تحديًا كبيرًا في مكافحة هذا النوع من الجرائم. حيث تخشى العديد من الشركات والمؤسسات من التبليغ عن حوادث القرصنة الإلكترونية أو اختراق أنظمتها الحاسوبية، خوفًا من الآثار السلبية التي قد تلحق بسمعتها وثقة عملائها بها. فغالبًا ما تسعى هذه الجهات إلى التعامل مع الحادث بشكل سري وداخلي، محاولةً تجنب أي ضرر لصورتها العامة أو خسارة العملاء. ولكن هذا الإحجام عن التبليغ يساهم في إضعاف جهود مكافحة الجريمة الإلكترونية، حيث لا تتمكن السلطات المختصة من الحصول على المعلومات اللازمة لتتبع مرتكبي هذه الجرائم ومقاضاتهم[2]. كما أن الكثير من الشركات والمؤسسات تتردد في التبليغ عن حوادث القرصنة الإلكترونية التي تتعرض لها، خشية تضرر سمعتها وفقدان ثقة عملائها فيها[3].

[1] – محمد أمين الشوابكة، جرائم الحاسب الآلي والإنترنت، مرجع سابق، ص:125.

[2]– نفس المرجع السابق

[3]– محمد سامي الشوا، الجرائم المعلوماتية وأساليب مكافحتها، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2010، ص: 187–192.

الفرع الثاني: نقص جاهزية سلطات البحث والتحري

تواجه سلطات التحقيق والبحث تحديات كبيرة في التعامل مع الجرائم الإلكترونية نتيجة لنقص الجاهزية والاستعداد لمواجهة هذا النوع الجديد من الجرائم. فعلى الرغم من التطور التكنولوجي الهائل والانتشار الواسع للأجهزة الرقمية والإنترنت، إلا أن العديد من أجهزة إنفاذ القانون لا تزال تفتقر إلى الخبرات والموارد اللازمة للتعامل بفعالية مع هذه الجرائم المعقدة. يكمن التحدي الأول في نقص التدريب المتخصص للمحققين والخبراء القانونيين في مجال التقنيات الرقمية والجرائم الإلكترونية. فالعديد منهم لا يملك المهارات اللازمة لجمع وتحليل الأدلة الرقمية بطريقة صحيحة، أو فهم كيفية عمل البرامج والشبكات الإلكترونية المستخدمة في ارتكاب هذه الجرائم. مما يجعل من الصعب عليهم تتبع آثار الجرائم وجمع الأدلة الكافية للمقاضاة.[1]

كما تعاني العديد من الأجهزة الأمنية والقضائية من نقص في الموارد المالية والبشرية المخصصة لمكافحة الجرائم الإلكترونية. فغالبًا ما تفتقر إلى الأجهزة والبرامج المتطورة اللازمة للتحقيق الرقمي، وكذلك الكوادر البشرية المدربة والمتخصصة في هذا المجال. مما يحد من قدرتها على مواكبة التطورات السريعة في عالم التقنية والجرائم الإلكترونية. علاوة على ذلك، تواجه سلطات التحقيق تحديات إضافية تتعلق بالطبيعة العابرة للحدود للجرائم الإلكترونية، حيث قد يتم ارتكابها من دول أخرى أو باستخدام شبكات إلكترونية دولية. مما يتطلب تعاونًا وتنسيقًا قويًا بين السلطات القضائية والأمنية في مختلف البلدان، وهو أمر ليس بالسهل تحقيقه في كثير من الأحيان.[2]

لذلك، من الضروري أن تولي الحكومات والمؤسسات القانونية أهمية قصوى لتطوير قدراتها في مجال مكافحة الجرائم الإلكترونية، من خلال تخصيص الموارد اللازمة للتدريب والتأهيل،

[1]– عبد الفتاح بيومي حجازي، الجرائم المعلوماتية ، ط1، دار الفكر الجامعي، الإسكندرية، 2012، ص:89-93.

[2] – عبد الله بن ناصر الغامدي، التحقيق في الجرائم المعلوماتية، ط1، جامعة نايف العربية للعلوم الأمنية، الرياض، 2014، ص:211.

واقتناء التقنيات الحديثة، وتعزيز التعاون الدولي. فقط بهذه الطريقة يمكن للسلطات أن تكون على استعداد لمواجهة هذا التحدي المتنامي ومحاربة الجرائم الإلكترونية بفعالية.

الفرع الثالث: فقدان الآثار التقليدية للجريمة

تشكل طبيعة الجرائم الإلكترونية تحديًا كبيرًا في عملية التحقيق والكشف عن مرتكبيها، حيث تفتقر هذه الجرائم إلى الآثار التقليدية التي نجدها في الجرائم العادية. فبينما تترك الجرائم التقليدية آثارًا مادية واضحة مثل بصمات الأصابع أو أدلة جنائية أخرى، تتميز الجرائم الإلكترونية بطبيعتها الافتراضية والرقمية، مما يجعل من الصعب العثور على أدلة ملموسة تساعد في تحديد هوية الجناة وإثبات تورطهم. في العالم الرقمي، يتم ارتكاب الجرائم عبر شبكات الإنترنت وأنظمة الحاسوب، حيث لا تترك آثارًا مادية مباشرة على مسرح الجريمة. بدلاً من ذلك، تكون الأدلة الرئيسية عبارة عن بيانات رقمية وملفات وسجلات إلكترونية، والتي قد تكون معقدة وصعبة الفهم للمحققين غير المتخصصين في مجال التقنية. كما أن هذه الأدلة الرقمية يمكن محوها أو تعديلها بسهولة، مما يزيد من صعوبة العثور عليها وتأكيد صحتها.[1]

غالبًا ما يلجأ مرتكبو الجرائم الإلكترونية إلى استخدام تقنيات التشفير وإخفاء الهوية والتخفي عبر شبكات افتراضية خاصة، مما يصعب عملية تتبع آثارهم الرقمية. كما أن طبيعة الإنترنت العابرة للحدود تضيف تحديًا إضافيًا، حيث يمكن ارتكاب الجريمة من أي مكان في العالم، مما يتطلب تعاونًا دوليًا في التحقيقات ويزيد من صعوبة جمع الأدلة.

لذلك، تحتاج السلطات المختصة إلى تطوير قدراتها التقنية وتدريب خبراء متخصصين في التحقيق الرقمي والتحليل الالكتروني، حتى تتمكن من جمع الأدلة الرقمية وتحليلها بشكل فعال. كما يجب العمل على تطوير أدوات وتقنيات جديدة للكشف عن الآثار الرقمية للجرائم الإلكترونية وتتبعها، بما في ذلك استخدام تقنيات مثل التعلم الآلي وتحليل البيانات الضخمة. بالإضافة إلى ذلك، يجب تعزيز التعاون الدولي في مجال مكافحة الجرائم الإلكترونية، والعمل

[1] – محمد سامي الشوا، الجرائم المعلوماتية وأساليب مكافحتها، مرجع سابق، ص:167-175.

على تطوير القوانين والإجراءات التي تسهل عملية التحقيق والملاحقة القضائية في هذا النوع الجديد من الجرائم عبر الحدود. فقط من خلال الجهود المنسقة والاستراتيجيات المتكاملة، يمكن التغلب على تحدي فقدان الآثار التقليدية للجريمة في مجال الجرائم الإلكترونية.[1]

الفرع الرابع: فرض الجناية تدابير حماية

تلجأ العديد من الجهات المنخرطة في ارتكاب الجرائم الإلكترونية إلى فرض تدابير حماية وإجراءات أمنية متطورة، بهدف حماية هوياتهم وإخفاء آثار نشاطاتهم الإجرامية. وتشكل هذه التدابير تحديًا إضافيًا أمام سلطات إنفاذ القانون والمحققين في مجال مكافحة الجريمة الإلكترونية. من بين أبرز هذه التدابير الحماية استخدام تقنيات التشفير المتقدمة لحماية البيانات والاتصالات الإلكترونية من التنصت والاختراق. فالعديد من الجماعات الإجرامية تستخدم برامج التشفير القوية لإخفاء محتوى رسائلها وبياناتها، مما يجعل من الصعب على المحققين الوصول إلى هذه المعلومات والاطلاع عليها.[2]

تستخدم هذه الجهات إلى استخدام شبكات افتراضية خاصة (VPN) وخوادم وكالة بروكسي لإخفاء هوياتها الحقيقية وعناوين IP الخاصة بها، مما يصعب عملية تتبعها وتحديد مصدر أنشطتها الإجرامية. وفي بعض الحالات، تستخدم أيضًا تقنيات التخفي الأكثر تعقيدًا مثل شبكات التور (Tor) لإخفاء آثارها بشكل شبه كامل على الإنترنت. علاوة على ذلك، غالبًا ما تعتمد الجماعات الإجرامية على استخدام برامج متطورة لاختراق أنظمة الحاسوب والشبكات، بهدف الوصول إلى البيانات والمعلومات الحساسة أو تخريب الأنظمة. وقد تستخدم أيضًا تقنيات التصيد الاحتيالي (Phishing) وغيرها من الأساليب الخداعية لخداع الضحايا وسرقة معلوماتهم الشخصية.[3]

---

[1] – محمد سعيد الغامدي، مكافحة الجرائم الإلكترونية: التحديات والحلول، ط2، دار الفكر العربي، القاهرة، 2018، ص:156.

[2] – محمد سامي الشوا، الجرائم المعلوماتية وأساليب مكافحتها، مرجع سابق، ص:187–192.

[3] – عبد الله بن ناصر الغامدي، التحقيق في الجرائم المعلوماتية، مرجع سابق، ص:127.

يجب في مواجهة هذه التدابير الحماية المتقدمة، يجب على سلطات إنفاذ القانون والمحققين أن يكونوا على دراية كاملة بأحدث التقنيات والأساليب المستخدمة في مجال الجريمة الإلكترونية. كما يجب عليهم الاستثمار في تدريب متخصص وامتلاك الأدوات والبرامج اللازمة لاختراق هذه التدابير الأمنية وتتبع آثار الجرائم الإلكترونية بشكل فعال. بالإضافة إلى ذلك، يجب تعزيز التعاون الدولي والتنسيق بين وكالات إنفاذ القانون في مختلف البلدان، حيث أن الطبيعة العابرة للحدود للجرائم الإلكترونية تتطلب جهودًا مشتركة ومنسقة للتغلب على التحديات التي تفرضها تدابير الحماية المتطورة المستخدمة من قبل الجناة. فقط من خلال هذه الاستراتيجية الشاملة، يمكن مواجهة تحدي فرض الجناة لتدابير الحماية بشكل فعال ومحاربة الجريمة الإلكترونية بنجاح.[1]

المطلب الثاني: إثبات الجريمة الالكترونية

إن إثبات الجريمة الإلكترونية يعتبر من أكبر التحديات التي تواجه السلطات القضائية والقانونية في العصر الرقمي. فعلى عكس الجرائم التقليدية التي تترك آثارًا مادية واضحة، تتميز الجريمة الإلكترونية بطبيعتها الافتراضية والرقمية، مما يجعل من الصعب جمع الأدلة وإثباتها.

الفرع الأول: غياب الدليل المادي

تكمن إحدى المشكلات الرئيسية في غياب الدليل المادي في الجرائم الإلكترونية. فبدلاً من الآثار المادية التقليدية مثل البصمات أو الأسلحة أو المتفجرات، تتمثل أدلة الجرائم الإلكترونية في البيانات الرقمية والإلكترونية، والتي قد تكون عرضة للتلاعب أو الإتلاف بسهولة من قبل المجرمين. لذلك، يجب على السلطات القضائية والتحقيقية اتباع إجراءات خاصة لضمان سلامة وصحة الأدلة الرقمية. يتضمن ذلك استخدام أساليب متخصصة لجمع

[1] – محمد سعيد الغامدي، مكافحة الجرائم الإلكترونية: التحديات والحلول، مرجع سابق، ص:179.

وحفظ واستخراج البيانات من الأجهزة الإلكترونية والشبكات، مع الحفاظ على سلامة سلسلة الحيازة القانونية للأدلة.[1]

علاوة على ذلك، قد يتطلب الأمر استخدام برامج وأدوات تحليل متقدمة لفك تشفير البيانات وتحليلها، خاصة في حالات الجرائم المعقدة مثل الهجمات الإلكترونية أو جرائم الإنترنت. كما قد يكون من الضروري الاستعانة بخبراء في مجال تقنية المعلومات والأمن السيبراني للمساعدة في فهم وتفسير الأدلة الرقمية. في بعض الحالات، قد تكون هناك حاجة لإجراء تعاون دولي وتبادل للمعلومات بين السلطات القضائية في مختلف البلدان، نظرًا لطبيعة الجرائم الإلكترونية التي قد تتخطى الحدود الوطنية. هذا التعاون يُعد ضروريًا لجمع الأدلة والتحقيق في الجرائم بشكل فعال.[2]

على الرغم من هذه التحديات، إلا أن التطورات التكنولوجية الحديثة والإجراءات القانونية المتخصصة قد ساهمت في تحسين قدرة السلطات على التعامل مع الجرائم الإلكترونية وإثباتها. ومع ذلك، لا يزال هناك حاجة لمزيد من التطوير والتكيف مع التقنيات المتجددة باستمرار في هذا المجال.

الفرع الثاني: إعاقة الوصول إلى الدليل

إن إعاقة الوصول إلى الدليل في حالات الجرائم الإلكترونية تشكل عقبة كبيرة أمام السلطات التحقيقية والقضائية في عملية إثبات هذا النوع من الجرائم. فعلى عكس الجرائم التقليدية التي تترك آثارًا مادية واضحة، تتميز الجرائم الإلكترونية بطبيعتها الافتراضية والرقمية، حيث تكون الأدلة عبارة عن بيانات وملفات إلكترونية قد تكون صعبة المنال أو مخفية بشكل احترافي[3].

[1] – إيهاب فاضل، الجرائم المعلوماتية والإلكترونية، دار الثقافة للنشر والتوزيع، الطبعة الأولى، 2016، ص:145.

[2] – إيهاب فاضل، الجرائم المعلوماتية والإلكترونية، مرجع سابق، ص:178.

[3] – محمد أمين الشوابكة، التحقيق الجنائي في الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، الطبعة الأولى، 2018، ص:87.

1) قد تواجه السلطات التحقيقية صعوبات في الوصول إلى الأدلة الرقمية عندما تكون متواجدة على خوادم أو منصات تابعة لشركات أجنبية أو في بلدان أخرى. فالإجراءات القانونية للحصول على هذه الأدلة قد تكون معقدة وطويلة، مما يعرض الأدلة للتلف أو الفقدان قبل الحصول عليها. كما قد تتعارض هذه الإجراءات مع قوانين وتشريعات البلدان الأخرى، مما يزيد من تعقيد عملية الوصول إلى الأدلة؛
2) قد يلجأ المجرمون إلى استخدام تقنيات متقدمة للتشفير وإخفاء الأدلة الرقمية، مما يجعل من الصعب اكتشافها أو الوصول إليها. كما قد يتم تخزين الأدلة على أجهزة أو وسائط إلكترونية مخفية أو محمية بشكل احترافي، مما يتطلب من السلطات التحقيقية امتلاك المهارات والأدوات التقنية المتطورة للكشف عنها واستردادها؛
3) قد تواجه السلطات التحقيقية تحديات إضافية عندما تتخطى الجريمة الإلكترونية الحدود الوطنية، حيث قد تختلف القوانين واللوائح والإجراءات القانونية من بلد لآخر، مما يصعب عملية التعاون والتنسيق والوصول إلى الأدلة بشكل موحد ومنسق بين جميع الأطراف المعنية؛
4) في بعض الحالات، قد يتم إتلاف الأدلة الرقمية أو محوها بشكل متعمد من قبل المجرمين، مما يجعل من المستحيل الوصول إليها أو استردادها. هذا يتطلب من السلطات التحقيقية التحرك بسرعة وحزم لضمان الحفاظ على الأدلة وعدم تعريضها للتلف أو الإتلاف، وعلى الرغم من هذه الصعوبات، إلا أن التعاون الدولي والجهود المتواصلة لتطوير إجراءات وأدوات أكثر تطورًا للتعامل مع الأدلة الرقمية قد ساهمت في تحسين القدرة على التغلب على عقبات الوصول إلى الأدلة. ومع ذلك، لا يزال هناك حاجة إلى مزيد من الاستثمار والتطوير في هذا المجال الحيوي لضمان سلامة عمليات التحقيق وإثبات الجرائم بشكل قانوني وعادل.[1]

الفرع الثالث: صعوبة فهم الدليل

[1] – إيهاب خليل، الأدلة الجنائية الرقمية: النظرية والتطبيق، دار النهضة العربية، الطبعة الثانية، 2021، ص:93.

تتبع صعوبة فهم الدليل في حالة الجريمة الإلكترونية تتبع من عدة عوامل تتعلق بطبيعة هذا النوع من الجرائم وخصائصها الفريدة. فعلى عكس الجرائم التقليدية التي تترك آثارًا مادية ملموسة، تتميز الجريمة الإلكترونية بكونها تحدث في عالم افتراضي رقمي، حيث تكون الأدلة عبارة عن بيانات وملفات إلكترونية معقدة ومشفرة في كثير من الأحيان.

1) تأتي صعوبة فهم الأدلة الإلكترونية من تعقيد البيانات الرقمية نفسها، والتي قد تكون مكتوبة بلغات برمجية متعددة وتنسيقات متباينة. يتطلب هذا من المحققين امتلاك مهارات تقنية عالية لفك تشفير هذه البيانات وتحليلها بشكل صحيح، وهو ما قد يتجاوز قدرات العديد من المحققين التقليديين غير المدربين على التعامل مع هذا النوع من الأدلة؛
2) قد تكون الأدلة الإلكترونية متشابكة ومترابطة بطرق معقدة للغاية، حيث يمكن أن تمتد عبر عدة أجهزة وشبكات وبيئات افتراضية مختلفة. يصعب في كثير من الأحيان تتبع هذه الروابط والعلاقات وفهمها بشكل كامل، مما يجعل من الصعب استنتاج سلسلة الأحداث بدقة وتحديد مسارات الجريمة وأطرافها المختلفة؛
3) قد تتطلب عملية فهم الدليل الإلكتروني الاستعانة بخبراء في مجالات متخصصة مثل أمن المعلومات والتحليل الرقمي والهندسة العكسية للبرامج. هذا يضيف طبقة إضافية من التعقيد والتكلفة على عملية التحقيق، ويزيد من احتمالية حدوث سوء فهم أو تفسير خاطئ للأدلة، خاصة إذا كان هناك نقص في التنسيق والتواصل بين المحققين والخبراء؛
4) قد تواجه السلطات القضائية تحديات إضافية عندما تتخطى الجريمة الإلكترونية الحدود الوطنية، حيث قد تختلف القوانين واللوائح والإجراءات القانونية من بلد لآخر، مما يصعب عملية التعاون والتنسيق وفهم الأدلة بشكل موحد ومنسق بين جميع الأطراف المعنية.[1]

على الرغم من هذه الصعوبات، فإن التطورات التكنولوجية الحديثة والتدريب المتخصص للمحققين والقضاة قد ساهمت في تحسين قدرتهم على فهم الأدلة الإلكترونية بشكل أفضل.

[1] – محمد أمين الشوابكة، التحقيق الجنائي في الجرائم المعلوماتية، مرجع سابق، ص:132.

ومع ذلك، لا يزال هناك حاجة لمزيد من التطوير والتكيف المستمر مع التقنيات المتجددة باستمرار في هذا المجال المعقد والسريع التغير، وذلك من أجل ضمان فعالية عمليات التحقيق وإثبات الجرائم الإلكترونية بشكل أكثر دقة وكفاءة.

الفرع الرابع: قصور إجراءات الحصول على الدليل الرقمي

يمثل قصور إجراءات الحصول على الدليل الرقمي في حالات الجرائم الإلكترونية يمثل تحديًا كبيرًا للسلطات التحقيقية والقضائية. فعلى الرغم من التطورات التكنولوجية والإجراءات المتخصصة التي تم تطويرها لجمع الأدلة الرقمية، إلا أن هناك العديد من الثغرات والقصور التي لا تزال قائمة في هذا المجال.[1]

أولًا، تواجه السلطات التحقيقية صعوبات في التعامل مع سرعة تطور التقنيات الرقمية والأساليب المستخدمة في ارتكاب الجرائم الإلكترونية. فما قد يكون إجراءً فعالًا لجمع الأدلة اليوم، قد يصبح عديم الفائدة في غضون فترة قصيرة نتيجة لظهور تقنيات جديدة للتشفير أو الإخفاء أو التلاعب بالبيانات. يتطلب هذا تحديثًا مستمرًا للإجراءات والأدوات المستخدمة من قبل المحققين، وهو ما قد لا يتم بالسرعة الكافية في كثير من الأحيان.

ثانيًا، هناك نقص واضح في الموارد البشرية المؤهلة والمدربة بشكل جيد على التعامل مع الأدلة الرقمية. فالمحققون التقليديون قد لا يمتلكون المهارات التقنية اللازمة لفهم وتحليل البيانات الإلكترونية المعقدة، في حين أن الخبراء في مجال تقنية المعلومات قد لا يكونون على دراية كافية بالإجراءات القانونية الصحيحة لجمع الأدلة بطريقة قانونية وقابلة للقبول في المحاكم.

ثالثًا، قد تواجه السلطات القضائية صعوبات في الحصول على الأدلة الرقمية عندما تكون متواجدة على خوادم أو منصات تابعة لشركات أجنبية أو في بلدان أخرى. فالإجراءات القانونية

[1] – عبد الفتاح بيومي حجازي، الجريمة الإلكترونية: التحقيق والإثبات، دار الفكر الجامعي، الطبعة الأولى، 2019، ص:211.

للحصول على هذه الأدلة قد تكون معقدة وطويلة، مما يعرض الأدلة للتلف أو الفقدان قبل الحصول عليها.

رابعًا، هناك مخاوف متزايدة حول حقوق الخصوصية وحماية البيانات الشخصية أثناء عملية جمع الأدلة الرقمية. فالإجراءات التحقيقية قد تنتهك خصوصية أشخاص أبرياء أو تؤدي إلى الكشف عن معلومات حساسة لا علاقة لها بالجريمة المرتكبة. يتطلب هذا توازنًا دقيقًا بين احترام الحقوق الأساسية وضمان فعالية عمليات التحقيق.[1]

على الرغم من هذه التحديات، إلا أن التعاون الدولي والجهود المتواصلة لتطوير إجراءات وأدوات أكثر تطورًا للتعامل مع الأدلة الرقمية قد ساهمت في تحسين القدرة على مواجهة الجرائم الإلكترونية. ومع ذلك، لا يزال هناك حاجة إلى مزيد من الاستثمار والتطوير في هذا المجال الحيوي لضمان سلامة عمليات التحقيق وإثبات الجرائم بشكل قانوني وعادل.

الفرع الخامس: ضخامة البيانات المتعين فحصها

تشكل ضخامة البيانات المتعين فحصها في حالات الجرائم الإلكترونية تحديًا كبيرًا للسلطات التحقيقية والقضائية. فعلى عكس الجرائم التقليدية التي تترك آثارًا محدودة، تتميز الجرائم الإلكترونية بإنتاج كميات هائلة من البيانات الرقمية التي يجب فحصها وتحليلها للوصول إلى الأدلة ذات الصلة.[2]

تنتج أنشطتنا اليومية على الإنترنت وعبر الأجهزة الإلكترونية المختلفة كميات ضخمة من البيانات المتنوعة، بما في ذلك رسائل البريد الإلكتروني، والمحادثات، وسجلات تصفح الإنترنت، وملفات الوسائط المتعددة، وغيرها الكثير. عند التحقيق في جريمة إلكترونية، قد يتعين على المحققين فحص جميع هذه البيانات بحثًا عن أي دليل أو معلومات ذات صلة بالجريمة. تكمن المشكلة الرئيسية في حجم هذه البيانات وتنوعها، حيث يمكن أن تصل إلى

[1] – عبد الفتاح بيومي حجازي، الجريمة الإلكترونية: التحقيق والإثبات، مرجع سابق، ص:256.

[2] – إيهاب خليل، الأدلة الجنائية الرقمية: النظرية والتطبيق، مرجع سابق، ص:142.

ملايين أو حتى مليارات الملفات والسجلات. يتطلب فحص وتحليل كل هذه البيانات وقتًا طويلًا وموارد بشرية وتقنية كبيرة، مما قد يعرقل عملية التحقيق ويؤدي إلى تأخيرات غير مقبولة.[1]

تكون بعض البيانات مشفرة أو مضغوطة أو متعددة التنسيقات، مما يزيد من صعوبة فحصها وتحليلها. كما قد تكون هناك حاجة لاستخدام أدوات وبرامج متخصصة للبحث والفرز والتصفية داخل هذه البيانات الضخمة للعثور على المعلومات ذات الصلة. وفي بعض الحالات، قد تكون البيانات المطلوب فحصها موزعة على عدة أجهزة وشبكات وخوادم في مختلف أنحاء العالم، مما يضيف طبقة إضافية من التعقيد على عملية التحقيق ويتطلب تعاونًا دوليًا وتبادلًا للمعلومات بين السلطات القضائية في مختلف البلدان.[2]

تعمل السلطات التحقيقية لمواجهة هذا التحدي على تطوير أدوات وأساليب متطورة للتعامل مع ضخامة البيانات الرقمية، مثل استخدام تقنيات الذكاء الاصطناعي والتعلم الآلي للمساعدة في عمليات البحث والفرز والتحليل. كما يتم التركيز على تدريب المحققين على المهارات التقنية اللازمة للتعامل مع هذه البيانات بكفاءة وفعالية. على الرغم من هذه الجهود، إلا أن ضخامة البيانات المتعين فحصها في حالات الجرائم الإلكترونية ستظل تشكل تحديًا مستمرًا للسلطات القضائية، خاصة مع التطور المتسارع للتقنيات الرقمية وزيادة استخدامها في جميع جوانب الحياة. لذلك، من الضروري مواصلة الاستثمار والتطوير في هذا المجال لضمان قدرة السلطات على مواكبة هذا التحدي والتعامل معه بشكل فعال.[3]

[1] – محمد عبيد الكعبي، مكافحة الجرائم الإلكترونية: الإطار القانوني والتقني، دار الحامد للنشر والتوزيع، الطبعة الأولى، 2022، ص:167.

[2] – محمد عبيد الكعبي، مكافحة الجرائم الإلكترونية: الإطار القانوني والتقني، المرجع السابق: ص:209.

[3] – إيهاب خليل، الأدلة الجنائية الرقمية: النظرية والتطبيق، مرجع سابق، ص:148.

المبحث الثاني: من خلال أطرف الجريمة الالكترونية وسلطات التحقيق فيها

الجرائم الإلكترونية هي ظاهرة معقدة ومتشعبة، تنطوي على العديد من الأطراف المختلفة. فهي لا تؤثر فقط على الضحايا المباشرين، سواء كانوا أفرادًا أو شركات أو مؤسسات حكومية، ولكنها تشكل أيضًا تحديًا كبيرًا لسلطات إنفاذ القانون والتحقيق.

المطلب الأول: الجاني في الجريمة الالكترونية

لم يكن لارتباط الجريمة الالكترونية بالحاسب الالي أثره على تمييز الجريمة الالكترونية عن غيرها من الجرائم التقليدية فحسب، وإنما كان له أثره أيضا على تمييز المجرم الالكتروني عن غيره من المجرمين. ولقد اختلف الباحثون في تحديد هذه السمات، ويعد الأستاذ PARKER واحد من أهم الباحثين الذين عالجوا الجريمة الالكترونية بالدراسة بصفة عامة والمجرم الالكتروني بصفة خاصة، ومع ذلك يعد المجرم الالكتروني مجرما لارتكابه فعل اجرامي يتطلب توقيع العقاب عليه، وكل ما في الأمر أنه ينتمي إلى طائفة خاصة من المجرمين تقترب في سماتها من جرائم ذوي الياقات البيضاء، وإن كانت في رأيه لا تتطابق معها.[1]

ينتمي المجرم الالكتروني من ناحية في أكثر الحالات إلى وسط اجتماعي متميز كما أنه يكون على درجة من العلم والمعرفة. ويتفق مجرمو المعلوماتية مع ذوي الياقات البيضاء في كون أن الفاعل في الحالتين يبرر جريمته كونه لا ينظر إلى سلوكه، باعتباره جريمة أو فعل يتنافى مع الأخلاق ويتميز المجرم الالكتروني بإضافة إلى ذلك بمجموعة من الخصائص التي تميزه بصفة عامة عن غيره من المجرمين ويرمز إليها الأستاذ PARKER بكلمة S.K.RAM وهي تعني: المهارة Skills، المعرفة Knowledge، الوسيلة Resources، السلطة Authority، وأخيرا الباعث Motives. .[2]

وتعد:

- **المهارة:** المتطلبة لتنفيذ النشاط الإجرامي أبرز خصائص المجرم الالكتروني، والتي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال، أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات، أو بمجرد التفاعل الاجتماعي مع الأخرين إلا أن ذلك لا يعني ضرورة أن يكون المجرم الالكتروني على قدر كبير من العلم في هذا المجال، بل إن الواقع العلمي قد

[1] – سمية مزغيش، جرائم المساس بالأنظمة المعلوماتية ، مذكرة مكملة من متطلبات نيل شهادة الماستر في الحقوق ، تخصص قانون جنائي ، جامعة محمد خيضر ، بسكرة ، 2013-2014 ، ص:18.

[2] – سمية مزغيش، جرائم المساس بالأنظمة المعلوماتية ، مرجع سابق، ص:54.

أثبت أن بعض أنجح مجرمي المعلوماتية لم يتلقوا المهارة اللازمة لارتكاب الجريمة عن طريق التعليم أو الخبرة المكتسبة من العمل في هذا المجال؛

- **المعرفة:** فتتلخص في التعرف على كافة الظروف التي تحيط بالجريمة المراد تنفيذها بكامل ملابستها ومدى إمكانية نجاحها أو فشلها، إذ أن المجرم الالكتروني باستطاعته أن يكون له تصورا كاملا لجريمته، كون أن مسرح الجريمة المعلوماتية هو النظام الالكتروني، فالفاعل يستطيع أن يطبق جريمته على أنظمة مماثلة لتلك التي يستهدفها والمعلوماتي ذلك قبل تنفيذ جريمته؛
- **الوسيلة:** فيراد بها الإمكانيات التي يتزود بها الفاعل لارتكاب جريمته ففيما يتعلق بالمجرم الالكتروني فإن الوسائل المتطلبة للتلاعب بأنظمة الحاسبات الآلية في أغلب الحالات تتميز نسبيا بالبساطة وبسهولة الحصول عليها، كما أنه نظرا لمهارته وقدرته يستطيع حتى ابتكارها، إذ أن الواقع أثبت أنه كلما كان النظام الالكتروني غير مألوف ويتميز بالخصوصية كانت الوسائل المتطلبة لارتكاب الجريمة أكثر صعوبة؛
- **السلطة:** فيقصد بها الحقوق أو المزايا التي يتمتع بها المجرم الالكتروني والتي تمكنه من ارتكاب جريمته، وهذه السلطة إما تكون مباشرة كالشفرة الخاصة بالدخول إلى النظام الالكتروني والتي تعطي للفاعل مزايا متعددة مثل فتح الملفات ومحو تعديل محتوياتها، مجرد قراءتها منها أو كتابتها.[1]

تتمثل هذه السلطة في حق استعمال الحاسب الألي نفسه أو الدخول إلى مكان تواجده كما هو الحال في الشبكات الداخلية لبعض الإدارات مثلا. وقد تكون هذه السلطة غير مباشرة كما في حالة استخدام شفرة الدخول الخاصة بشخص آخر.[2]

المطلب الثاني: المجني عليه وسلطات التحقيق في الجريمة الالكترونية

[1] – نائلة عادل، محمد فريد قورة، جرائم الحاسب الألي الاقتصادية، دراسة نظرية وتطبيقية، منشورات الحلبي الحقوقية، بيروت، 2005، ط1، ص:54.

[2] – نائلة عادل محمد فريد قورة، جرائم الحاسب الألي الاقتصادية، مرجع سابق، ص:57.

عندما نتحدث عن المجني عليهم في الجرائم الإلكترونية، فإننا نتعامل مع فئتين رئيسيتين: الضحايا المباشرين للجريمة، وكذلك السلطات المعنية بالتحقيق فيها. فكلاهما يعتبر طرفًا متضررًا من هذا النوع من الجرائم، ولكن بطرق مختلفة.

الفرع الأول: المجني عليه

يمكن أن يكون المجني عليهم في الجرائم الإلكترونية من مختلف الفئات والخلفيات. في كثير من الأحيان، تكون الضحايا هي المستهلكين العاديين الذين يقعون ضحية لعمليات الاحتيال والنصب عبر الإنترنت. فقد ينجرف هؤلاء الأشخاص وراء عروض مغرية أو يُخدعون بطرق ماكرة لدفعهم نحو الإفصاح عن معلوماتهم المالية الحساسة أو تحويل الأموال دون علمهم الحقيقي بالمخاطر. من ناحية أخرى، قد تكون الشركات والمؤسسات التجارية هي الهدف للمجرمين الإلكترونيين. حيث يسعى هؤلاء لاختراق أنظمة الشركات وسرقة البيانات السرية أو تعطيل عملياتها بهدف الابتزاز المالي. كما قد تتعرض حتى المؤسسات الحكومية لهجمات إلكترونية خطيرة تستهدف البنية التحتية الحيوية أو أنظمة المعلومات الحساسة. على صعيد آخر، لا تقتصر الجرائم الإلكترونية على الجوانب المالية فحسب، بل قد يكون المجني عليهم هم ضحايا انتهاكات للخصوصية أو التشهير عبر الإنترنت. حيث يتم تسريب بياناتهم الشخصية أو نشر محتوى مسيء لهم على مواقع التواصل الاجتماعي دون موافقتهم، مما قد يُلحق بهم أضرارًا نفسية وشخصية كبيرة. [1]

كما يجب أن ندرك أن المجني عليهم في جرائم الإنترنت هم من مختلف الأعمار والخلفيات والمستويات الاجتماعية، مما يجعل الحماية والتصدي لهذه الجرائم أمرًا في غاية الأهمية لصالح المجتمع بأكمله.

[1] – عبد الرحمن، خالد فهمي، ضحايا الجرائم الإلكترونية: دراسة ميدانية، رسالة دكتوراه، جامعة القاهرة، كلية الحقوق، 2020، ص:80-115 .

يختلف مرتكبو الجرائم الإلكترونية عن مجرمي الجرائم التقليدية في العديد من الجوانب. فغالبًا ما يتمتع هؤلاء الجناة بمهارات تقنية عالية ومعرفة متقدمة بأنظمة الكمبيوتر والبرمجيات، مما يمكنهم من اختراق الأنظمة الإلكترونية واستغلال ثغراتها الأمنية لتحقيق أغراضهم الإجرامية. ومع ذلك، فإن دوافعهم قد تختلف من جانٍ لآخر. البعض قد يكون مدفوعًا بالفضول والرغبة في اختبار حدود قدراتهم التقنية، في حين أن آخرين قد يسعون إلى تحقيق مكاسب مالية من خلال سرقة البيانات أو الابتزاز. كما قد تكون هناك دوافع سياسية أو إيديولوجية وراء بعض هذه الجرائم، حيث يسعى المجرمون إلى إلحاق الضرر بمؤسسات أو حكومات معينة. ومن الخصائص المميزة لمرتكبي الجرائم الإلكترونية هي قدرتهم على التخفي والإخفاء وراء شخصيات افتراضية، مما يجعل من الصعب تعقبهم وكشف هوياتهم الحقيقية. كما أنهم غالبًا ما يعملون في مجموعات أو شبكات إجرامية منظمة، مستغلين الطبيعة العابرة للحدود لهذا النوع من الجرائم. علاوة على ذلك، قد يمتلك بعض هؤلاء المجرمين خلفيات تعليمية أو مهنية في مجالات تقنية مرتبطة بأنظمة المعلومات والأمن السيبراني، مما يزيد من قدرتهم على ارتكاب جرائم إلكترونية معقدة ومتطورة تكنولوجيًا. [1]

ولمواجهة هذا التهديد المتنامي، تحتاج سلطات إنفاذ القانون إلى تطوير استراتيجيات وآليات متخصصة للتعامل مع هذا النوع من المجرمين، بما في ذلك تدريب الكوادر البشرية على أحدث التقنيات وأساليب التحقيق الرقمي، فضلاً عن التعاون الدولي لمواجهة هذه الظاهرة العابرة للحدود.

الفرع الثاني: سلطات التحقيق

عندما نتحدث عن سلطات التحقيق في الجرائم الإلكترونية، فإننا نتعامل مع طرف رئيسي يواجه تحديات كبيرة في أداء واجباته. فهذه السلطات، سواء كانت الشرطة أو هيئات

[1] – الزبيدي، مروان خالد، آليات حماية ضحايا الجرائم الإلكترونية: تحليل مقارن للتشريعات المحلية والدولية"، المجلة العربية لقانون تكنولوجيا المعلومات، المجلد 9، جامعة الملك سعود، العدد 1، 2020، ص: 55.

حكومية أخرى، تعتبر ضحية لهذا النوع من الجرائم بسبب الطبيعة المعقدة والتقنية التي تتميز بها. وتكمن صعوبة جمع الأدلة الرقمية وتحليلها تشكل عقبة رئيسية أمام سلطات التحقيق في الجرائم الإلكترونية. فعلى عكس الجرائم التقليدية التي تترك آثارًا مادية واضحة، تتميز الجرائم الإلكترونية بأن الأدلة تكون عبارة عن بيانات رقمية معقدة ومشفرة في كثير من الأحيان، مما يتطلب مهارات تقنية عالية للتعامل معها.[1]

تواجه سلطات التحقيق نقصًا في الموارد البشرية المؤهلة تقنيًا للتعامل مع هذا النوع من الأدلة، حيث قد لا يمتلك المحققون التقليديون المهارات اللازمة لفهم وتحليل البيانات الإلكترونية المعقدة. كما قد تفتقر هذه السلطات إلى الإجراءات والأدوات المناسبة لجمع الأدلة الرقمية وتحليلها بشكل فعال.

قد تصطدم سلطات التحقيق بعوائق قانونية وتشريعية عندما تتخطى الجريمة الإلكترونية الحدود الوطنية، مما يتطلب التعاون الدولي والتنسيق بين السلطات المختلفة في مختلف البلدان. هذا التعاون قد يكون معقدًا ويستغرق وقتًا طويلًا، مما يعرض الأدلة للتلف أو الفقدان. من جانب آخر، قد تكون سلطات التحقيق عرضة للهجمات الإلكترونية والتلاعب ببياناتها الرقمية من قبل المجرمين، مما يزيد من تعقيد عملية التحقيق ويعرض أمنها الالكتروني للخطر. لذلك، فإن هذه السلطات بحاجة إلى تطوير إستراتيجيات وآليات دفاعية متقدمة للحماية من مثل هذه التهديدات.[2]

عندما نتحدث عن سلطات التحقيق في الجرائم الإلكترونية، نقصد بذلك وجود طرف يواجه تحديات متعددة ومتشابكة. فهي تعاني من نقص في الموارد البشرية والتقنية المؤهلة، وتواجه عقبات قانونية وتشريعية، وهي عرضة للهجمات الإلكترونية والتلاعب ببياناتها. كل هذه العوامل تجعل من مهمة التحقيق في الجرائم الإلكترونية مهمة شاقة وصعبة للغاية.

---

[1] – السويدي، نورة سالم، التعاون الدولي في مكافحة الجرائم الإلكترونية: نحو إطار عمل فعال، مجلة سياسات الأمن السيبراني، المجلد 5، ع3، جامعة الملك سعود، 2019، ص 367.

[2] – السويدي، نورة سالم، التعاون الدولي في مكافحة الجرائم الإلكترونية: نحو إطار عمل فعال، مرجع سابق، 369.

تحتاج سلطات التحقيق لمواجهة هذه التحديات إلى الدعم والاستثمار الكافي من قبل الحكومات والمؤسسات المعنية. يجب توفير التدريب المناسب للموارد البشرية وتزويدها بالأدوات والإجراءات المتطورة للتعامل مع الأدلة الرقمية بكفاءة. كما يجب تحديث التشريعات والقوانين لمواكبة التطورات التقنية والتسهيل على سلطات التحقيق في التعامل مع الجرائم الإلكترونية عبر الحدود الوطنية.

فقط من خلال تضافر الجهود وتوفير الدعم اللازم لسلطات التحقيق، يمكن التغلب على التحديات التي تواجهها في مكافحة الجرائم الإلكترونية، وضمان تحقيق العدالة بشكل فعال في هذا المجال المتنامي والمعقد.[1]

خلاصة الفصل:

تناولنا في ختام هذا الفصل، جوانب مختلفة من الجريمة الإلكترونية بشكل شامل. بدءًا باستعراض التحديات المتعلقة باكتشاف وإثبات هذا النوع من الجرائم نظرًا لطبيعتها التقنية المعقدة. كما تم التطرق إلى أطراف الجريمة الإلكترونية بما في ذلك المجني عليهم من مختلف الفئات والخلفيات، وسلطات التحقيق التي تواجه صعوبات عديدة في أداء مهامها.

[1]– الأمم المتحدة، مكتب المخدرات والجريمة، الجرائم الإلكترونية: دراسة عالمية، منشورات الأمم المتحدة، 2013، ص:40–55.

تطرقنا إلى شخصية الجاني في الجرائم الإلكترونية، حيث تم مناقشة الخصائص والدوافع المحتملة لهؤلاء المجرمين، وكذلك التحديات التي تواجه السلطات في تعقبهم وملاحقتهم قضائيًا بسبب طبيعة هذه الجرائم العابرة للحدود.

يتضح أخيرا أن الجريمة الإلكترونية تشكل تحديًا كبيرًا للمجتمعات والدول في العصر الرقمي الحالي، ويتطلب التصدي لها بشكل فعال تضافر الجهود على جميع المستويات، سواء من حيث تطوير التشريعات والآليات القانونية، أو تدريب وتأهيل الكوادر البشرية المتخصصة، أو التعاون الدولي لمواجهة هذه الظاهرة العابرة للحدود.

الفصل الثاني:

خصوصيات الطبيعة

الدولية للجريمة الالكترونية

المبحث الأول : صعوبة تجسيد التعاون الدولي في مجال الجريمة الالكترونية

و لتجسيد التعاون الدولي في مجال الجريمة الالكترونية توجد صعوبات إجرائية و صعوبات موضوعية

المطلب الأول : الصعوبات الاجرائية في تجسيد التعاون الدولي في مكافحة الجريمة الالكترونية

الفرع الأول : اختلاف النظم القانونية الاجرائية بين الدول

ان سبب تنوع واختلاف النظم القانونية يعود الى اختلاف العادات والأعراف والديانات مما يؤدى لاختلاف القوانين من دولة لاخرى كما ان طرق التحري والتحقيق والمحاكمة التي تثبت فاعليتها في دولة ما قد تكون عديمة الفعالية في دولة اخرى وقد لا يسمح باجرائها، كما هو الحال بالنسبة للمراقبة الالكترونية والتسليم المراقب وغيرها من الاجراءات الشبيهة ، فاذا اعتبرت طريقة ما من طرق جمع الادلة او التحقيق انها قانونية في دولة معنية تكون في دولة اخرى غير قانونية وبالتالي فان الدولة الأولى تشعر بخيبة أمل لعدم قدرة السلطات تطبيق القانون في الدولة الأخرى على استخدام ما تعتبره هي اداة فعالة ، بالاضافة الى ان السلطات القضائية الدى الدولة الثانية قد لا تسمح باستخدام أي دليل اثبات جرى جمعه بطرق تراها انها غير مشروعة حتى وان كان هذا الدليل تم الحصول عليه في اختصاص قضائي وبشكل مشروع [1]

وأحسن دليل على اختلاف النهج القانونية بين الدول قضية الدودة الحاسوبية " لوف باغ love bug " التي اعدت في الفلبين عام 2000 وقيل انها عطلت ملايين الحواسيب في

[1] براء منذر كمال عبد اللطيف، ناظر أحمد منديل – التعاون القضائي الدولي في مواجهة جرائم الأنترنت، المؤتمر العلمي الأول تحولات القانون العام في مطلع الألفية الثالثة كلية القانون جامعة تكريت العراق، 2009 ص11.

جميع انحاء العالم حيث اعاقت هذه القضية التحقيقات بسبب ان ذلك العمل المؤدي والضار لم يكن آنذاك مجرما بشكل كاف في الفلبين [1]

الفرع الثاني : عدم وجود قنوات اتصال

أهم الاهداف الموجودة في التعاون الدولي في مجال تسليم المجرمين للحد من الجريمة الحصول على معلومات وبيانات متعلقة بالمجرمين الفارين وذلك يكون عن طريق اتصال فيما بين الدول للتعاون بينهم وذلك لجمع الادلة والبحث والتحري والتحقيق وجمع المعلومات المهمة عن المجرمين، فعدم وجود نظام الاتصال فيما بينهم يؤدي الى عدم التصدي للجرائم والمجرمين [2]

فيعتبر عدم وجود اتصال وتنسيق في شان الجريمة المرتكبة عبر الانترنيت بين الدول خاصة هو أمر في غاية الصعوبة خاصة ان عملية الحصول على دليل في مثل هذه الجرائم خارج نطاق حدود الدولة عن طريق الضبط او التفتيش في نظام معلوماتي معين هو امر غاية في الصعوبة ، فظلا عن الصعوبة الفنية في الحصول على الدليل ذاته [3].

الفرع الثالث: الصعوبات الخاصة بتبادل المساعدات القضائية

التعاون القضائي الدولي أو ما يعرف بالمساعدة القضائية المتبادلة في المسائل الجنائية من أبرز أهم تطبيقات التعاون الدولي في مجال محاربة الجريمة الإلكترونية.

ويهدف التنسيق بين السلطات القضائية بدءا من التحقيق ووصولا إلى صدور حكم على المحكوم عليه وضمان عدم الإفلات من العقاب.

---

[1] مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية – المرجع السابق ص6.

[2] شاشوة الزهرة، مكافحة الجريمة المنظمة في إطار نظام تسليم المجرمين، مذكرة ماستر في الحقوق تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة أكلي محند أولحاج البويرة، 2019–2020 ص 86

[3] عبد الفتاح بيومي حجازي، دليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت . دراسة متعمقة في جرائم الحاسب الالي والانترنيت – المرجع السابق ص 104 و 105

وتعرف المساعدة القضائية الدولية على أنها " كل إجراء قضائي تقوم به الدولة من شأنها تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم" [1]

ولقد نص المشرع، ج في القانون 09-04 المادة 16 الفصل السادس على مبدأ المساعدة القضائية المتبادلة معتبرا أنه في إطار التحريات والتحقيقات القضائية الجارية لمعاينة جريمة الإلكترونية يمكن للسلطات المختصة[2]

تبادل المساعدة القضائية التي لا تتحقق إلا بواسطة 3 خطوات:

1-الطلب: وتقدمه الدولة صاحبة الإختصاص الجنائي بالمحاكمة، فالإتفاقيات الدولية تسمح بالإتصال المباشر بين جهات العدل في الدولتين كسبا للوقت.

2-فحص الطلب: وتقوم به الدولة التي ستقدم المساعدة.

3-تنفيذ المساعدة القضائية: وتتم وفقا لقواعد الدولة المطلوب منها. وتتخذ المساعدة القضائية الدولية عدة صور أبرزها تبادل المعلومات، الإنابة القضائية، تسليم المجرمين، إلا أن ثمة صعوبات تقف دون تحقيق هذه المساعدة القضائية الدولية، فتعد جرائم الأنترنت نموذجا عمليا لمشكلة الاختصاص القضائي الدولي ويقصد به مجموعة القواعد التي تبين حدود ولاية المحاكم فيما يخص العلاقات القانونية ذات العنصر الأجنبي إزاء المحاكم الأجنبية التي تنازع هذا الاختصاص.

وباعتبار جريمة إلكترونية ذات طابع عالمي عابرة للحدود، فتعد من أكثر المسائل التي يثار بشانها موضوع التنازع بين الدول فتقدم دعوى في نفس الجريمة إلى جهتين من

---

[1] سليمان أبو نمر، يوسف بوكشريدة، مكافحة الجريمة المعلوماتية في إطار القانون الدولي، مذكرة ماستر في الحقوق تخصص قانون دولي كلية الحقوق جامعة محمد خيضر بسكرة، 2020-2021، (الجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني) ص31.

[2] المادة 16 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها.

الجهات التحقيق أو الحكم وإدعاء كل جهة إختصاصها كإختصاص إيجابي أو رفض كل من الجهتين النظر في الدعوى على أساس عدم الاختصاص كاختصاص سلبي.

وهذا ما يساهم في إفلات المجرمين من العقاب والإشكال في الاختصاص القضائي الدولي عدم تحديد القانون الواجب التطبيق لاستكمال إجراءات التحري والتفتيش خارج الحدود الوطنية.

كما يوجد صعوبات ومعوقات وتحديات فيما يخص الإنابة القضائية وهي تحديات مرتبطة بفكرة السيادة والأخرى بإجراءات الإنابة القضائية

أما الأولى فنقصد بالسيادة " السلطة العليا للدولة على رعاياها وغير مقيدة بأي تبعية أو تأثير يأتي من خارج الدولة، وتستأثر بمباشرة جميع الاختصاصات داخل حدود الإقليم في مواجهة الرعايا، وتتصرف في الخارج على قدم المساواة مع غيرها من السيادات المماثلة [1] فعند ارتكاب جريمة معلوماتية في إحدى الدول، وتجري محاكمته في دولة أخرى فمن المنطق البحث عن كافة الأدلة لتلك الجريمة أو نفيها لمساعدة الدولة التي وقعت فيها الجريمة الإلكترونية وهذا ما يعرف بالذكاء القضائي الدولي غير أن هذا التعاون قد يصطدم بفكرة سيادة كل دولة على إقليمها وبالتالي فإن الزج بفكرة السيادة قد يصعب من التعاون القضائي الدولي أو المساعدة القضائية المتبادلة بين الدول المختلفة في مجال مكافحة جريمة المعلوماتية.

أما التحديات المرتبطة بإجراءات الإنابة، فباعتبار أن الإنابة القضائية طلب إجراء قضائي من إجراءات الدعوى الجزائية، تتقدم به الدولة الطالبة إلى الدولة المطلوبة إليها لضرورة ذلك الإجراء في الفصل في مسألة معروضة على السلطة القضائية في الدولة الطالبة ويتعذر عليها القيام به بنفسها، وهذا ما أبرزته المادة 16 و17 من القانون 04/09.

فإجراءات الإنابة القضائية تتم وفقا للطرق الدبلوماسية وتتسم الغالب ببطء وتعقد اجراءاتها التي لا تتماشى مع طبيعة الأنترنت التي تتميز بالسرعة والتطور وسرعة الانتشار

[1] يوسف بوكشريدة، مرجع سابق، ص48.

ما ينعكس عليها بالسلب ويؤدي إلى عرقلة التعاون الدولي كما ان عامل نقص الموظفين المديريين في هذا المجال الإلكتروني يزيد الطين بلة ما يؤدي إلى عدم كبح جريمة الإلكترونية.

فلقد أقر المشرع، ج. في المادة 18 فقرة 1 من ق 09-04 مجموعة من القيود ترفض بموجبها طلبات المساعدة القضائية الأجنبية كما رأينا وهي طلبات المساعدة التي من شأنها المساس بالسيادة الوطنية أو النظام العام وهو أمر بترك للدولة لوزارة العدل غالبا حسب الإتفاقيات الدولية في تقدير تنفيذ أو عدم تنفيذ ما يطلب إليها، وبالتالي لا يمكن للدولة تقديم المساعدة القضائية لدولة أخرى في تحقيقات أو تحريات تخص أفعال غير مجرمة لديها ما يعوق التعاون القضائي الدولي.

أما التعاون الدولي في مجال تسليم المجرمين لمكافحة الجرائم الإلكترونية بين الدول لتسليط العقاب اللازم عليهم، فبموجبه تقوم الدولة المطلوب منها التسليم بتسليم الشخص المطلوب سواء كان منهما او محكوما عليه لى الدولة الطالبة وذلك بموجب نص تشريعي أو تعاهدي أو بمقتضى العرف الدولي أو إتفاقيات بين الدول[1] وبذلك يجب التعاون بين الدول.

وتنفيذ هذه القاعدة لأن المجرم في الجرائم المعلوماتية يستطيع ارتكاب الجرم في دولة وإحداث آثارها في دولة أخرى أو عدة دول، بالتالي كان على الدول أن تتعاون فيما بينها من خلال تطبيق مواثيق دولية ذات الصلة بشأن التعاون الدولي في المسائل الجنائية وعلى وجه الخصوص في مجال تسليم المجرمين، هذا الإجراء نصت عليه المادة 82 من دستور 2016[2] وبذلك نجد أن اغلب الصعوبات الموضوعية وإجرائية في تجسيد التعاون لتسليم المجرمين كعدم وجود نموذج موحد للنشاط الإجرامي، التزاحم في طلبات التسليم وتنوع النظم القانونية الإجرائية وعدم وجود قنوات إتصال.

---

[1] زغودي عمر، مجلة البحوث القانونية والإقتصادية، الآليات القضائية للتعاون الدولي في مجال مكافحة الجريمة المنظمة عبر الوطنية، معهد الحقوق آفلو، 2020، ص107.

[2] تنص المادة 82 من ق 01/16 المؤرخ في 06 مارس 2016 المتضمن التعديل الدستوري بأنه: "لا يسلم أحد خارج التراب الوطني إلا بناء على قانون تسليم المجرمين وتطبيقاته".

ومن صور التعاون والمساعدة القضائية المتبادلة تبادل المعلومات فالمشرع ج في قانون 09-04 في المادة 17 منه نص صراحة على تبادل المعلومات واتخاذ الإجراءات التحفظية من خلال الإستجابة لطلبات المساعدة وفقا للإتفاقيات الدولية ذات الصلة او الثنائية ومبدأ المعاملة بالمثل[1].

فعدم تقديم المعلومات من وثائق، أدلة وغيرها إلى السلطة القضائية الطالبة يعوق ويصعب التعاون فيما بين الدول، فيجب تقديم كل المعلومات عن المتهم أو المحكوم عليه والسوابق القضائية له قصد التعرف على الماضي الجنائي للفرد ومساعدتهم قضائيا بذلك، هذا ما أوردته م15 فقرة 1و2 من الإتفاقية المتعلقة بالتعاون القضائي في المجال الجزائي بين الجمهورية الجزائرية ومملكة إسبانيا.

الفرع الرابع: الصعوبات الخاصة بالتعاون الأمني الدولي

أدى الإنتشار الواسع للجريمة المعلوماتية إلى ضرورة وجود آليات لمكافحتها وباعتبارها جرائم عابرة للحدود وجب التعاون الأمني بين الدول للقضاء على هذه الجرائم الإلكترونية.

ويعرف التعاون الأمني الدولي بأنه تبادل العون والمساعدة وتظافر الجهود المشتركة بين طرفين دوليين أو أكثر لتحقيق خدمة أو مصلحة مشتركة للتصدي للجرائم المعلوماتية وما يرتبط به من مجالات أخرى مثل مجال العدالة الإجتماعية ومجال الأمن، أو لتخطي مشكلات الحدود والسيادة التي قد تعترض الجهود الوطنية لملاحقة المجرمين، سواء كانت مساعدة متبادلة قانونية أو قضائية[2].

فضروري وجود التعاون الأمني الدولي لمكافحة الجريمة المعلوماتية لأنه مهم لإلتقاء الجهود الدولية لإتخاذ تدابير تدعم سبل التعاون الدولي في مكافحتها، ويتمثل بين أجهزة

---

[1] م 17 من القانون 09-04 المرجع السابق.

[2] خالد بن مبارك القحطاني، التعاون الأمني الدولي في مواجهة ج، إ عبر الوطنية، أطروحة دكتوراه كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، دار النهضة العربية، الرياض، 2006، ص38.

الشرطة الجنائية المتخصصة في مكافحة الجريمة الإلكترونية حيث يستحيل على الدولة بمفردها القضاء على هذه الجرائم الدولية العابرة للحدود لأن جهاز الأمن في هذه الدولة لا يمكنها تعقب المجرم وملاحقته إلى في حدود الإقليم دولته، وهذه تعتبر من الصعوبات الخاصة بالتعاون الأمني الدولي.

فلملاحقة هؤلاء المجرمين وتقديمهم للعدالة يجب التعاون الأمني بين الدول، فتقدم دولة مساعدات أمنية بغيرها من الدول لمعاقبة المجرمين بالسماح لهم بإجراء التحريات حيث ارتكبت الجريمة أو جزء منها، ومن هذه الإجراءات معاينة مواقع الأنترنت في الخارج ضبط الأقراص الصلبة أو تفتيش نظم الحاسوب[1] ... إلخ، فمتى فر المجرم خارج حدود الدولة يقف الجهاز الأمني عاجزا، لذا أصبحت الحاجة ماسة إلى وجود تعاون دولي، فتسمح لها بإجراء تحريات وتحقيقات باستخدام التكنولوجيا الحديثة في الإتصال مثل الدوائر التلفزيونية، واستخدام أساليب خاصة للتحري والمراقبة، واستحداث قنوات للإتصال، والتنسيق الأمني والقضائي بين الجهات المختصة ع/ط الأقمار الصناعية وشبكة الأنترنت لتبادل المعلومات سريعا، فانعدام هذه الإجراءات تصعب من مكافحة جريمة الإلكترونية فيجب مثلا انتقال القاضي إلى دول المعنية للتحقيق ولإتخاذ ما يلزم من إجراءات، لبيس فقط في مرحلة التحقيق الإبتدائي ولكن في مرحلة الحكم أيضا، ويجب مراعاة تنفيذ الأحكام الأجنبية وفقا لضوابط تتفق عليها الدول فيما بينها، من خلال الإتفاق عن الإجراءات الجنائية وعلى معايير موحدة والإتفاق على كيفية مصادرة الأموال محل الجريمة المعلوماتية عبر الحدود وارسال المسجونين[2].

فنظرا للطبيعة الخاصة بالجرائم المعلوماتية فينبغي أن يبنى هذا التعاون على أسس معينة وهي:

---

[1] فهد عبد الله العبيد، الإجراءات الجنائية المعلوماتية، رسالة دكتوراه، كلية الحقوق، عين شمس، 2012، ص514.

[2] هدى حامد قشقوش، الجريمة المنظمة القواعد الموضوعية والإجرائية والتعاون الدولي، دار النهضة العربية، القاهرة 2002، ص83.

1-الدراسة العلمية لبحث ظاهرة جريمة الإلكترونية وتوفير البيانات الإحصائية المتعلقة بالجريمة بمرتكبيها لسير نظام القضاء الجنائي.

2-إعداد مشروع اتفاقية دولية تتضمن قانون موحد للجريمة المعلوماتية.

3-تحديد أساليب التعاون في مجال التدريب وتحقيق التكامل الأمني بين الأجهزة الشرطة على المستوى الدولي.

4-وضع إستراتيجيات وقائية واحترازية توفر الجو الملائم لمكافحة وإنهاء أنشطة المنظمات الإجرامية، وزيادة الوعي العام لدى الأفراد بنشر البيانات اللازمة عن هذه الجرائم ومرتكبيها[1] .

5-التنسيق بين المؤسسات الأمنية بآلياتها المختلفة في المساحات الأمنية والإقليمية والدولية، بما يحقق حصر معدلات الجريمة ويحول دون استكمال أي نقص في المعلومات الأمنية، وبذلك يجب التعاون الأمني بين الدول لتجميع عناصر تلك المعلومات ليكتمل وتكشف أبعاد الجرائم وخطط الإعداد لأرتكابها وإتاحة الفرصة لإمكان مدارسة الثغرات الأمنية الدولية، والعمل على إيجاد أفضل أساليب التصدي لها منعا للجريمة وضبطا للجناة وإتاحة الفرصة للتعرف على التجارب الأمنية الدولية في المؤسسات الأمنية لدى الدول الأخرى، فتبادل المعلومات والخبرات ونتائج البحوث والدراسات بخصوص جريمة الإلكترونية يتيح حصر الأساليب والوسائل الجديدة المستخدمة، ويوسع نطاق المعرفة بأنماط المجرمين فيها وأنشطتهم الإجرامية.

وبذلك يجب التعاون الأمني بين الدول لمكافحة جريمة المعلوماتية كربط شبكات الإتصال والمعلومات فالإتصالات الشرطية تحتاج إلى وسائل الإتصال لتحقيق السرعة

[1] عادل عبد العال ابراهيم خراشي، إشكاليات التعاون الدولي في مكافحة ج.م وسبل التغلب عليها، ط1، دار الجامعة الجديدة، الإسكندرية، 2015، ص23-24.

الملائمة لتتمكن أجهزة العدالة الجنائية من التواصل بين سلطات التحقيق والملاحقة المختلفة.

ومن صور التعاون الأمني القيام ببعض العمليات الشرطية والأمنية المشتركة كتعقب المجرم المعلوماتي وتعقب الأدلة الرقمية، وضبطها والقيام بعمليات التفتيش العابر للحدود لمكونات الحاسب الآلي بحث ما يحويه من أدلة وبراهين على ارتكاب الجريمة الإلكترونية[1]

كما أنشأت أكبر منظمة دولية للشرطة الجنائية والأنتربول لمكافحة الجرائم المعلوماتية وذلك عام 1929 وتضم 182 دولة وطريقة عملها تتمثل بتبادل أعضاء الشرطة الدولية المعلومات عن المجرمين الدوليين ويتعاونون في مكافحة الجرائم الدولية مثل جرائم التهريب وعمليات البيع والشراء الغير مشروع للأسلحة وج.إ، وأنشأت خلال عام 2004 وحدة خاصة لمكافحة جرائم التكنولوجيا نظرا لتطورها وانتشارها[2]

لكن ضرورة وجود مثل هذه المنظمات وتعددها للقضاء على الصعوبات الخاصة بالتعاون الأمني الدولي وتظافر جهود بين الدول بالتعاون فيما بينهم من أجل مكافحة الجريمة الإلكترونية.

المطلب الثاني : الصعوبات الموضوعية في تجسيد التعاون الدولي في مجال مكافحة الجريمة الالكترونية.

الفرع الأول : الفراغ التشريعي لدى بعض الدول

[1] عادل عبد العال ابراهيم خراشي، المرجع السابق، ص24

[2] الشمري محمد غانم، مرجع سابق ص96.

يعتبر الفراغ أو القصور التشريعي اكبر تحدي يواجه مكافحة الجرائم المعلوماتية لما ينتج عنه بين الدول من مشاكل في تطبيق القانون من الناحية العملية ويجعل التعاون بينهم أمرا صعب[1] وذلك راجع إلى عدم وجود نظام قانوني خاص بمكافحة الجرائم المعلوماتية وما يكون مباح في احد الأنظمة أو إحدى الدول يكون مجرما في نظام آخر أو دولة أخرى وذلك لعدة أسباب أهمها:

1- اختلاف البيئات العادات والتقاليد والثقافات والديانات من مجتمع لآخر يؤثر في وضع نظام سياسي تشريعي واحد .

2- كثرة المفاهيم القانونية المتعلقة بالجرائم المعلوماتية فكل دولة تضع تعريفات ومفاهيم حسب أنظمتها القانونية الجنائية [2] وبذلك كل هذه الأسباب تنعكس سلبا على تجسيد التعاون الدولي بحيث أن عدم النص على جميع الجرائم المعلوماتية يؤثر على صانعي القرار في المجالات المختلفة [3] وبذلك القصور التشريعي للدول في وضع نظام قانوني خاص بالجرائم المعلوماتية يؤدي إلى إفلات المجرمين من العقاب وإحضار الحقوق للأفراد المجني عليهم ، كما إن تعارض مصالح الدول فيما بينهم يمثل صعوبة في حد ذاتها تعترض سبل التعاون الدولي حيث تلجأ الدول إلى تغليب مصالحها على حساب العدالة الجنائية وتنفيذ القوانين

الفرع الثاني : عدم وجود نموذج موحد للنشاط الاجرامي

نظرا لعدم وجود مفهوم عام مشترك بين الدول فيما يخص نماذج الجريمة الالكترونية ونظرا لاختلاف هذه المفاهيم وذلك باختلاف العادات الأعراف القانونية الدولية وحتى الدينية فان هذا يضعف من ضبط منظومة القانون الدولي وبالتالي يسهل على الجناة الافلات من

---

[1] سامح احمد الجوانب الاجرائية للحماية الجنائية لجرائم الانترنيت ص 538.

[2] عال عبد العال خراشي ص 57

[3] هشام عبد العزيز مبارك – تسليم المجرمين بين الواقع و القانون 10 دار النهضة العربية القاهرة 2006 ص 529.

المسائلة الجنائية [1] وبذلك يضفي عدم توفر تعريف مشترك للجريمة المرتكبة عبر الانترنيت الى بقاء افعال اجرامية دون تجريم، حيث في بعض الدول تعتبر أفعال اجرامية وغيرها تعتبرها مباحة [2]

هذه المفاهيم أعاقت وصعبت من وجود نوذج موحد للنشاط الإجرامي مما أدى الى صعوبة التعاون بين الدول تثير الطبيعة الدولية للجريمة المرتكبة عبر الانترنيت مشاكل فيما يتعلق بتحدي القانون الواجب التطبيق هل هو قانون الدولة التي ارتكب فيها الفعل أم قانون الدولة التي ظهرت فيها لآثار الضارة إضافة الى تعارض القوانين من ناحية موضوعية وإجرائية، الأمر الذي يستلزم ضرورة العمل على توحيد التشريعات فيما يتعلق بمكافحة الجرائم المرتكبة عبر الانترنيت إضافة الى ابرام الاتفاقيات في هذا المجال[3] كآليات للتغلب على صعوبات التعاون الدولي في مكافحة الجريمة الالكترونية.

الفرع الثالث: التجريم المزدوج للسلوك الإجرامي وقصور المعاهدات الدولية

يعتبر شرط التجريم المزدوج من أهم الشروط الخاصة بنظام تسليم المجرمين ، فهو منصوص عليه في اغلب التشريعات الوطنية والاتفاقيات الدولية المعنية بتسليم المجرمين وبالرغم من أهميته نجده عقبة أمام التعاون الدولي في مجال تسليم المجرمين بالنسبة للجريمة الالكترونية لان معظم الدول لا تجرم هذه الجرائم والأخرى تجرمها بالإضافة الى صعوبة تحديد فيما اذ كانت النصوص التقليدية لدى الدولة المطلوب منها التسليم ان تنطبق على الجريمة الالكترونية .

---

[1] إيهاب ماهر السنباطي، الجرائم الإلكترونية، قضية جديدة أم فئة مختلفة؟ التناغم القانوني هو السبيل الوحيدة الندوة الإقليمية حول الجرائم المتصلة بالكومبيوتر، المملكة المغربية يونيو 2007. ص68.

[2] فريد منعم جبور – حماية المستهلك عبر الأنترنت ومكافحة الجريمة ودراسة مقارنة منشورات الحلبي الحقوقية بيروت، ط 2010 ص215.

[3] عواطف محمد عثمان عبد الحليم جرائم المعلوماتية، تعريفها،صورها، جهود مكافحتها، دوليا وإقليميا ووطنيا، مجلة العدل العدد 24، السنة العاشرة دون سنة أو بلد النشر ص68.

فالتجريم المزدوج أساسه ان تبتغي الدولة طالبة التسليم من وراء طلبها محاكمة من نسب اليه ارتكاب الجريمة او تنفيذ العقوبة عليه وهذا يفترض ان الدول تعتبره اجراما في تشريعها، بحيث اذ لم يكن مجرما في نظرها فلا تكون هناك دعوى عمومية أو ملاحقة جزائية ضده ولا يتصور قيام حكم جزائي يقضي بعقوبته كما لا يجوز مطالبة الدولة المطلوب اليها التسليم بإيقاع عقوبة على ارتكاب سلوك لا يعتبر إجراميا وفقا لقوانينها [1]

يرجع هذا الى عدم وجود معاهدات ثنائية وجماعية بين الدول الأمر الذي ادى الى صعوبة التعاون بين الدول وحتى في حال وجودها فهي قاصرة عن تحقيق الحماية المطلوبة في ضل التقدم السريع لنظم الحاسوب والانترنيت وتطور الجرائم الالكترونية المرتكبة عبر الانترنيت ما يبين الأثر السلبي في قصور التعاون الدولي [2]

المبحث الثاني: الصعوبات المتعلقة بتنازع الإختصاص

المطلب الأول: صعوبات تحديد القانون الواجب التطبيق في مجال الجريمة الإلكترونية.

[1] حسين بن سعيد بن سبق الغافري – الجهود الدولية في مواجهة الجرائم الأنترنت– مقال متوفر على الموقع التالي: www.minchaoui.com

[2] عبد الفتاح بيومي حجازي – الدليل الجباني والتزوير في جرائم الكومبيوتر والأنترنت دراسة معمة في جرائم الحاسب الذكي والأنترنت المرجع السابق ص 105

إمتداد مسرح الجرائم الأنترنت إلى أكثر من إقليم دولة أدى إلى تنازع الإختصاص في جرائم الأنترنت ذلك أن أهم خصائصها أنها عابرة للحدود وهو ما يصطدم بمبدأ أصيل في تطبيق القانون الجزائي هو مبدأ الإقليمية دون إنتهاك سيادة الدولة في تحصيل الدليل الجنائي الإلكتروني والمبادئ الإحتياطية وهي الشخصية والعينية، وبذلك سنتعرف على المبادئ العامة في تطبيق القانون الجزائي والصعوبات هذه التي واجهتها في تطبيقها على الجرائم الإلكترونية[1].

الفرع الأول: المبادئ العامة في تطبيق القانون الجزائي

أولا: مبدأ إقليمية النص الجنائي:

يعد مبدأ إقليمية النص الجنائي هو من المبادئ المستقرة في قوانين كل دول العالم، وقد تم اعتماده في التشريعات الجنائية لكل الدول[2].

تنظر المحاكم الجزائرية في الجرائم الإلكترونية ما يقع على إقليمها كل السلوك الإجرامي أو جزء منه دون الأخذ بعين الإعتبار الشخص المتهم وهو المبدأ المجسد في م3 الفقرة 1 من قانون العقوبات الجزائري فيقصد به كل جريمة ترتكب على إقليم هذه الدولة سواء كان الجاني يحمل جنسية هذه الدولة أو دولة أخرى أجنبية[3].

والأصل أن عناصر الركن المادي لأي جريمة يكون في نطاف جغرافي واحد أي إقليم دولة واحدة بداية من وقوع السلوك الإجرامي إلى تحقيق النتيجة الإجرامية غير أن الجرائم الإلكترونية قد يتجزأ فيها الركن المادي قد يتوزع على اكثر من منظومة المعلوماتية التي تكون ضمن دولة أخرى غير الدولة التي ارتكبت فيها الجريمة كالتلاعب بالبيانات والمتاجرة بها او

---

(1) عادل عزام سقف الحيط، المرجع السابق ص349

(2) غازي عبد الرحمان هيان الرشيد، الحماية القانونية، من الجرائم المعلوماتية، (الحاسب والأنترنت) أطروحة أعدت لنيل درجة الدكتوراه في القانون الجامعة الإسلامية في لبنان، كلية الحقوق، 2004 ، ص499.

(3) مريم عراب، الإختصاص القضائي في الجرائم المعلوماتية، مجلة حوليات، كلية، ح.و.ع.س جامعة وهران، 2 العدد3 2015/12/22، ص277.

تخريبها الذي يتم في دولة والنتائج تكون في دولة أخرى، وهنا نكون أمام ما يعرف بتنازع القوانين[1]

وهنا انقسم رأي الفقهاء إلى ثلاث إتجاهات.

1- مذهب السلوك أن النشاط الإجرامي: بوصفه معيارا لتحديد مكان وقع الجريمة: وينعقد الإختصاص هنا للمحكمة التي يقع في دائرة إختصاصها السلوك الإجرامي لأنه أيسر في عملية الإثبات وجمع الأدلة فهو أقرب إلى مسرح الجريمة حسب نظر السلطات المختصة.

2- مذهب النتيجة الإجرامية كمعيار لتحديد مكان وقوع الجريمة: ويأخذ هذا الإتجاه بمبدأ وحدة الجريمة وعد الفصل بين عناصرها وأنه أكثر واقعية في نظر المدافعين على إعتبار أن الضرر له مظهر خارجي ملموس على خلاف السلوك الإجرامي الذي قد لا يكون كذلك وقد يتخذ فعل إيجابي، وقد تم تبني هذا المذهب في بعض التشريعات المقارنة منها ق الألماني.

3- المذهب المختلط: أمام الإنتقادات التي وجهت لكلا المذهبين السابقيين، برز هذا الإتجاه مفاده أن الجريمة تعد واقعة في مكان حصول النشاط الإجرامي وكذلك المكان الذي تحققت فيه النتيجة الإجرامية، وهذا المذهب تلق موافقة أغلب الفقهاء وبعد مبرره أن الركن المادي للجريمة الإلكترونية له ثلاث عناصر الفعل الإجرامي والنتيجة والعلاقة السببية بينهما، ما يعني أن الجريمة وقعت في كل مكان تحقق فيه الفعل وهو عنصر من عناصر الركن المادي للجريمة.

ثانيا: مبدأ العينية:

ويقصد به تطبيق القانون الجزائي على الجرائم التي تمس المصالح الأساسية للدولة المرتكبة خارج إقليمها وكانت جنسية مرتكبيها أجنبية وأن يستهدف مؤسسات الدولة الجزائرية الدفاع الوطني المصالح الإستراتيجية للإقتصاد الوطني وأن يتعلق الأمر بجرائم تكنولوجيا

[1] دلال مولاي مرجع سابق، ص252.

الإعلام والإتصال[1] هذه الشروط التي نص عليها المشرع (ج) في نص المادة 15 من ق 09-04[2] إضافة إلى م588 من ق.إ.ج.

ومن هذا المبدأ يغطي العجز الذي يتلقاه مبدأ الإقليمية في جرائم الأنترنت التي تتحقق أركانها على أكثر من إقليم إفتراضي، فهذا المبدأ يحمي المصالح الوطنية خارج إقليم الدولة حتى وان كان افتراضي هو حال مسرح الجريمة في الجرائم الإلكترونية.

ثالثا: مبدأ الشخصية:

يقصد بمبدأ الشخصية ملاحقة القانون الوطني للأشخاص الذين يحملون جنسية الدولة أينما وجدوا ليحكم أفعالهم الإجرامية بالخارج، ويرى الفقهاء أن لهذا المبدأ وجهان: أحدهما إيجابي والآخر سلبي، فالإيجابي يعني تطبيق النص الجنائي على كل من يحمل جنسية الدولة ولو ارتكبت جريمته خارج إقليمها، أما الوجه السلبي للمبدأ فيعني تطبيق النص على كل جريمة يكون المجني عليه فيها منتميا إلى جنسية الدولة ولو كان مرتكبها أجنبيا وارتكبها خارج إقليم الدولة.

الفرع الثاني: صعوبة تطبيق المبادئ العامة على الجرائم الإلكترونية.

أثارت الجرائم المرتكبة عبر الأنترنت مسألة تنازع في الإختصاص على المستوى المحلي والدولي، بالرغم أنه لا يوجود أي إشكال على المستوى الوطني حيث يتم الرجوع إلى المعايير المحددة قانونا لتلك الدولة.

أما على المستوى الدولي ينجم عن إختلاف التشريعات والنظم القانونية تنازع في الإختصاص بين الدول لكونها عابرة للحدود من قبل أجنبي، فهنا تكون الجريمة الإلكترونية خاضعة للإختصاص الجنائي للدولة الأولى استنادا إلى مبدأ الإقليمية، وقد تخضع كذلك للدولة الثانية على أساس مبدأ الشخصية وقد تكون هذه الجريمة من الجرائم التي تهدد أمن وسلامة

---

[1] مريم عراب، مرجع سابق، ص278-279.

[2] المادة 15 من ق 09-04، مرجع سابق

دولة أخرى فتدخل عندئذ في إختصاصها استنادا إلى مبدأ العينية، كما تثار فكرة تنازع الإختصاص القضائي في حالة تأسيس الإختصاص على مبدأ الإقليمية، كما لو قام الجاني ببث الصور الخليعة والإباحة من إقليم دولة معينة ويتم إطلاع عليها في دولة أخرى، ففي هذه الحالة يثبت الإختصاص وفقا لمبدأ الإقليمية لكل دولة من الدول التي مستها الجريمة[1] .

فما يلاحظ أن إختصاص القضاء في الجرائم الإلكترونية غير واضح، فالقانون الواجب تطبيقه لا يحض بالقبول أمام حقيقة أن غالبية الأفعال من قبل أشخاص خارج حدود الدولة أو أنه تمر عبر شبكات المعلومات خارج حدود الدولة حتى عندما يتكبها شخص من داخل الدولة على نظام في الدولة نفسها.

وهذا ما يبرز أهمية اختبار مدى ملائمة قواعد الإختصاص والقانون الواجب التطبيق، ما إذا كانت النظريات والقواعد القائمة في هذا الحقل تطال هذه الجرائم أم يتعين إفراد قواعد خاصة بها في ضوء خصوصيتها وماتثيره من مشكلات في حقل الإختصاص القضائي، كما يرتبط بمشكلات الإختصاص وتطبيق القانون مشكلات إمتداد أنشطة الملاحقة والتحري والضبط والتفتيش خارج الحدود[2].

وبذلك أدى هذا البعد الدولي للجريمة الإلكترونية إلى تشتيت الجهود وإعاقة التعاون الدولي لمواجهة هذا النوع من الجرائم، وذلك لإختلاف الإجراءات الجنائية أو النزاع حول القانون الواجب التطبيق[3]

المطلب الثاني: تحديد المحكمة المختصة

---

[1] حسين بن سعيد بن سيف الغافري: " الجهود الدولية في مواجهة جرائم الأنترنت، ص52-53.
http:\\ www.minchaoui.com\

[2] عبد الله عبد الكريم عبد الله، ، الجرائم المعلوماتية والأنترنت (الجرائم الإلكترونية) الطبعة الأولى منشورات الحلبي الحقوقية، بيروت، 2007، 47-48.

[3] محمود أحمد عبابنة، جرائم الحاسةب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، عمان، 2005، ص35.

الفرع الأول: معايير تحديد الإختصاص:

تباينت المعايير الفقهية التي اعتمدت لتحديد المحكمة المختصة بنظر الجرائم المرتكبة عبر الأنترنت إلى ثلاثة معايير هم:

أولا: معيار الإختصاص المكاني:

تعتمد أغلب التشريعات في معيارها على تحديد الإختصاص المكاني والذي يتبع ثلاثة ضوابط وهي مكان وقع الجريمة أو محل إقامة المتهم أز مكان ضبطه وإلقاء القبض عليه، وفي حالة إجتماع أكثر من ضابط تكون المحكمة التي ترفع إليها الدعوى أولا، هي المختصة مكانيا بالنظر في الدعوى[1].

ويقصد بمكان ارتكاب الجريمة هو المكان الذي ارتكب فيه السلوك والنشاط الإجرامي وليس الذي تحققت في النتيجة، كون السلوك هو التعبير المادي عن إرادة مخالفة القانون، أما النتيجة فهي حدث خارجي يترتب عن السلوك، فمعيار حصول النشاط الإجرامي يسهل عملية الإثبات وجمع الأدلة، والمحكمة التي لها ولاية النظر في الدعوى تكون قريبة من مسرح الجريمة، ناهيك أن الحكم الذي يصدر في الواقعة يكون أكثر فعالية ويسهل معه ملاحقة الجناة[2].

ثانيا: معيار القانون الأكثر ملائمة

يرى أصحاب هذا الإتجاه أنه نظرا للطبيعة الخاصة للجرائم الإلكترونية والأضرار الناجمة عنها التي يشمل أكثر من دولة واحدة، وأحيانا قد تتفاوت نسبة الضرر بين الدولة وأخرى، فيجب التوسع في قاعدة اختصاص محكمة وقوع الفعل لأنها منطقة حصول الضرر لأن مع الجرائم المعلوماتية كل الدول تتضرر، فمن التطبيقات القضائية ما أعلنته إحدى محاكم ولاية نيويورك بعدم إختصاصها في قضية تزوير ماركات التجارية،

---

(1) غازي عبد الرحمان هيان الرشيد، المرجع السابق، ص518

(2) موسى مسعود أرحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية" المؤتمر المغاربي الأول حول المعلوماتية والقانون أكادمية الدراسات العليا، طرابلس 2009، ص15.

أقدم عليها موقع ويب أحد وادي الجاز في ولاية ميسوري، وعللت المحكمة قرارها بأن صلاحيتها لا تنشأ منه من داخل هذه الولاية، بل تنشأ فقط إذا ألحق هذا الموقع ضرر فعليا ضمن نطاقها[1].

ثالثا: معيار الضرر المرتقب:

مع ظهور شبكة الأنترنت وجد عالم افتراضي، حيث تسري فيه مختلف المواد المعلوماتية دون إمكانية تحديد وجهتها، وهذا العالم الإفتراضي طبعا لا يخضع لأي سلطة إقليمية وبالتالي الضرر الذي تسببه الجريمة الإلكترونية أيضا يكون متسعا في أكثر من دولة، وهذا هو معيار الضرر المرتقب أو الإفتراضي.

فلقد قد المجلس الأوروربي العدلي تفسيرا خاصا بشأن مفهوم قاعدة إختصاص كل محل وقوع الفعل الضار وذلك بالتأكيد على حق المتضرر باللجوء حسب خياره إلى محكمة محل ارتكاب الفعال أو إلى محل وقوع الضرر، ولكن مع إضافة قيد هام أو أساسي في حالة لجوء المتضرر إل محكمة وقوع الضرر يقضي بحجب إختصاص هذه المحكمة إذا أثبت المدعى عليه أنه لم يكون قادرا على الأرتقاب بصورة معقولة، وأن الفعل أو الإمتناع كان من شأنه إحداث أو إنتاج ضرر مماثل في دولته[2]

الفرع الثاني صعوبات تطبيق معايير الإختصاص على الجريمة الإلكترونية

أولا: صعوبات تطبيق معيار الإختصاص المكاني على الجريمة الإلكترونية

تثير هذه القاعدة بعض الصعوبات عند التطبيق بحث أنه معيار مرن وفضفاض، والجرائم الوقتية لا صعوبة في الفصل فيها لأنها ترتكب وتتم في لحظة واحدة ولذلك من اختصاص المحكمة التي وقع الفعل في دائرتها، أما بالنسبة للجرائم المستمرة والتي تظل قائمة يبقى التدخل الإداري من جانب الفاعل كجريمة حبس الأشخاص بغير حق او اخفاء الأشياء

[1] غازي عبد الرحمن هيان الرشيد، المرجع السابق، ص523.

[2] غازي عبد الرحمن هيان الرشيد، المرجع السابق، ص524.

المتحصلة من الجريمة، فيتخذ الإختصاص المكاني هنا بأي مكان قامت فيه حالة الإستمرار أما الجرائم الشبيهة بالجرائم المستمرة بالنظر إلى ما بداخلها من عنصر زمني ومثالها الإعتياد، والجرائم المتتابعة وجرائم الشروع حيث يعتبر مكانا للجريمة كل محل يقع فيه فعل من أفعال الإعتياد أو التتابع أو البدء في التنفيذ.

تتمثل أيضا الصعوبات في أن مكان إلقاء القبض على المتهم غير المكان الذي يتم توقيفه فيه أو حبسه، والحق أن هذا الأخير يعد بمثابة مكان حكمي للمتهم لكن الأمر لم تعد له أهمية قانونية طالما أن القانون يساوي بين مكان الإقامة ومكان الإلقاء القبض ومكان ارتكاب الجريمة في تحديد الإختصاص المكاني.

ويمثل السلوك الإجرامي والنتيجة الإجرامية بنظري الجريمة في إطار جريمة الإلكترونية وعلى ذلك إذا تم بث الفيروس المعلوماتي كسلوك إجرامي في مكان، وتحققت النتيجة في مكان آخر وألقي القبض على الجاني في مكان ثالث، فإن الإختصاص ينعقد لمحاكم أحدى هذه الأماكن[1]

وينقد بعض الفقهاء فكرة المساواة بين هذه المحاكم أو يجب أن ينظر إلى إختصاص محل ارتكاب الجريمة كإختصاص رئيسي يقدم على غيره ويتبعه إختصاص محل الإقامة، ثم اختصاص مكان الإلقاء القبض على المتهم.

ثانيا: صعوبات تطبيق معيار القانون الأكثر ملائمة على جريمة الإلكترونية

بني هذا المعيار على الأخذ بعين الإعتبار نقطة الإتصال المميزة والسلطة الفعلية، أي بإختصاص قضاء الدولة التي قانونها هو الأكثر تعرضا للإنتهاك بسبب الفعل الجرمي، ومن أمثلة ذلك ما أصدرته إحدى المحاكم الأمريكية التي اعتبرت فيه أنه لا يمكن الإرتكاز على

[1] عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجبائية في جرائم الكمبيوتر والأنترنت، المرجع السابق ص51-52.

مجرد النفاذ أو الإتصال بهذا الموقع أو المورد انطلاقا من الأراضي الأمريكية، حيث قضى بذلك بإختصاص قضاء الدولة من منطق وقوع الضرر الفعلي لا الإحتمالي[1].

ثالثا: صعوبات تطبيق معيار الضرر المرتقب على جريمة الإلكترونية

ورد في حيثيات هذا القرار أن المعلومات المنتشرة في شبكة الأنترنت يمكن معاينتها من قبل جميع الدول الموصولة بها ومن دون أن تكون موجهة بالضرورة محددة، لكن طبيعة هذه الوسيلة الإعلامية وهذه الشبكة الإلكترونية الجديدة تفرض هذه الصعوبات وبذلك لا نستطيع تطبيق جميع القوانين الموجودة بل يجب أن نطبق معيار الإرتقاب على المسؤول على المعلومات الضارة فيها، وهذا المعيار لا يمكن إيجاده إلا من خلال إيجاد الصلة أو علاقة للقانون المختص مع مبدأ موضوعي، وذلك بمعزل عن تذرع كل دولة بإختصاصها المحتمل، وأول المعالم الموضوعية في الإختصاص هي محل تمركز الموقع الذي نشرت الأقوال أو المعلومات بواسطته وهو أكيد على عكس مكان تلقيها الذي يبقى احتماليا.

وقد وجد هذا المعيار طريقة إلى التطبيق في بعض الدول ومنها فرنسا حيث أصدرت محكمة استئناف باريس في عام 1999 قرارا اعتبر فيه أن الطبيعة الكونية لشبكة الأنترنت يجب أن تؤدي إلى تطبيق محتمل لجميع القوانين الموجودة، بل إلى تطبيق القانون ذي الصلة مع مبدأ موضوعي هو إرتقاب المسؤول للمتحوى الصار الذي ينشره[2].

---

[1] فريد منعم جبور مرجع سابق، ص207.

[2] عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والأنترنت، المرجع السابق، ص52.

خلاصة الفصل:

الجريمة الإلكترونية بطبيعتها تتميز بالسرعة والتطور الدائم في إرتكابها مما جعلها تتلقى عدة صعوبات في تجسيد التعاون الدولي لمكافحتها منها صعوبات موضوعية كالفراغ التشريعي لدى بعض الدول، وقصور المعاهدات والإتفاقيات بين الدول وعدم وجود نموذج موحد للنشاط الإجرامي والتجريم المزدوج للسلوك الإجرامي ومنها صعوبات إجرائية في تجسيد التعاون الدولي في مكافحة الجريمة الإلكترونية كإختلاف النظم القانونية الإجرائية بين الدول وعدم وجود قنوات إتصال وصعوبات خاصة بتبادل المساعدات القضائية بين الدول والتعاون الأمني الدولي.

أما الصعوبات المتعلقة بتنازع الإختصاص كالصعوبات التي تلقتها لتحديد القانون الواجب التطبيق فيا يخص المبادئ العامة في تطبيق القانون الجزائي وصعوبة تطبيق هذه المبادئ على الجرائم الإلكترونية كما يوجد معايير لتحديد المحكمة المختصة في مكافحة هذه الجريمة الإلكترونية. إلا أنها تلقت صعوبات في تطبيقها.

خاتمة

في ختام هذا البحث، نجد أن خصوصية الجريمة الإلكترونية تؤثر بشكل كبير على فعالية آليات مكافحتها. إن الطبيعة المعقدة والعابرة للحدود لهذه الجرائم تفرض تحديات فريدة على الجهات المعنية. فالمجرمون الإلكترونيون يستغلون الفجوات القانونية والتقنية بين الدول، مما يجعل من الضروري تعزيز التعاون الدولي لمواجهة هذه التحديات بشكل فعال.

لقد أظهرت الدراسة أن التشريعات الحالية غالباً ما تكون غير كافية أو غير محدثة لمواكبة التطورات السريعة في مجال التكنولوجيا. لذلك، يجب على الدول العمل على تحديث قوانينها لتشمل أنواع جديدة من الجرائم الإلكترونية وتوفير إطار قانوني يمكن من خلاله مقاضاة المجرمين بفعالية. كما يعد التعاون الدولي أمراً حيوياً في مكافحة الجريمة الإلكترونية، الذي يتطلب ذلك تنسيق الجهود بين الدول لتبادل المعلومات والخبرات وتوحيد الإجراءات القانونية والتقنية.

من الناحية التقنية، تتطلب مكافحة الجريمة الإلكترونية تطوير أدوات وتحسين القدرات التقنية بشكل مستمر. التكنولوجيا المستخدمة في ارتكاب الجرائم الإلكترونية تتطور بوتيرة سريعة، مما يستدعي الحاجة إلى استثمارات مستمرة في الأبحاث والتطوير في مجال الأمن السيبراني. إن التدريب المستمر للعاملين في هذا المجال وتعزيز الوعي بين الجمهور حول كيفية حماية أنفسهم من الهجمات الإلكترونية يعدان أيضاً جزءاً أساسياً من الاستراتيجية الشاملة لمكافحة هذه الجرائم.

يمكن القول أن مواجهة الجريمة الإلكترونية تستدعي جهداً مشتركاً بين الحكومات والقطاع الخاص والمؤسسات الأكاديمية. يجب أن يتم تبني نهج شامل ومتكامل يأخذ في الاعتبار الخصوصيات المتنوعة للجريمة الإلكترونية وتحدياتها، ويعمل على تطوير استراتيجيات فعالة لمكافحتها. إن تطوير التشريعات، تعزيز التعاون الدولي، وتحسين القدرات التقنية تعد جميعها خطوات ضرورية لضمان مجتمع أكثر أماناً في مواجهة تهديدات الجريمة الإلكترونية.

وبناءاً على هذا البحث توصلنا إلى النتائج التالية:

- ✓ غياب الآثار المادية التقليدية في الجرائم الإلكترونية مما يصعب عملية جمع الأدلة ويتطلب مهارات تقنية متخصصة؛
- ✓ تعقيد الأدلة الرقمية وصعوبة فهمها وتحليله الأمر الذي يتطلب خبرات متخصصة وأدوات متطورة للتعامل معها؛
- ✓ إحجام الجهات المتضررة عن التبليغ عن الجرائم الإلكترونية خوفًا على سمعتها وثقة عملائها، مما يعيق جهود المكافحة؛
- ✓ نقص جاهزية سلطات البحث والتحري للتعامل مع الجرائم الإلكترونية مما يستدعي تدريبًا متخصصًا وتوفير موارد تقنية متطورة؛
- ✓ ضخامة حجم البيانات التي يتعين فحصها في التحقيقات وهو ما يتطلب وقتًا طويلًا وموارد بشرية وتقنية كبيرة؛
- ✓ تمتع المجرم الإلكتروني بمهارات تقنية عالية ومعرفة متقدمة مما يمكنه من اختراق الأنظمة واستغلال الثغرات الأمنية بسهولة؛
- ✓ قدرة المجرم الإلكتروني على التخفي وراء شخصيات افتراضية الأمر الذي يصعب عملية تعقبه وكشف هويته الحقيقية؛
- ✓ تنوع المجني عليهم في الجرائم الإلكترونية حيث يشمل الأفراد والشركات والمؤسسات الحكومية؛
- ✓ تعدد أنواع الأضرار الناتجة عن الجرائم الإلكترونية والتي تتراوح بين الخسائر المالية وانتهاك الخصوصية والتشهير؛
- ✓ صعوبة التعامل مع الجرائم الإلكترونية العابرة للحدود مما يتطلب تعاونًا دوليًا وتنسيقًا بين السلطات في مختلف البلدان؛

- ✓ الحاجة إلى تطوير استراتيجيات متكاملة لمواجهة الجرائم الإلكترونية تشمل التدريب وتحديث التشريعات وتعزيز التعاون الدولي؛
- ✓ ضرورة توفير الموارد والأدوات اللازمة لسلطات التحقيق لتمكينها من التعامل بفعالية مع تحديات الجرائم الإلكترونية

الإجابة على إشكالية:

تأثير خصـــوصـــية الجريمة الإلكترونية على آليات مكافحتها يتجلى في الحاجة إلى تحديث وتطوير التشـــريعات والقوانين لتشـــمل هذه الجرائم بفعالية. كما أن التعقيدات التقنية تتطلب استثمارات مستمرة في تطوير أدوات وتقنيات مكافحة الجريمة الإلكترونية، بالإضافة إلى ذلك، يُعتبر التعاون الدولي أمراً حيوياً في مواجهة الطابع العابر للحدود لهذه الجرائم، مما يســـتدعي وجود معاهدات واتفاقيات دولية تســـهل تبادل المعلومات والتنســـيق القانوني والفني، كما يلعب الوعي والتدريب دوراً محورياً في تعزيز الجهود الوقائية والعلاجية لمكافحة الجريمة الإلكترونية. بالتالي، فإن خصـــوصـــية الجريمة الإلكترونية تتطلب اســـتجابة شـــاملة ومتكاملة تشـــمل تحديث التشـــريعات، تطوير القدرات التقنية، تعزيز التعاون الدولي، وزيادة الوعي والتدريب لضمان حماية فعالة ضد هذه الجرائم المعقدة.

التوصيات والاقتراحات:

- ✓ **تطوير القوانين الوطنية** :يجب على الدول تحديث قوانينها الجنائية لتشمل الجرائم الإلكترونية الجديدة والمتطورة. وأن تكون هذه القوانين مرنة وقابلة للتكيف مع التطورات التكنولوجية السريعة.
- ✓ **إنشاء إطار قانوني موحد دولياً:** العمل على تطوير إطار قانوني دولي موحد يمكن الدول من التعاون بشكل أكثر فعالية في مكافحة الجرائم الإلكترونية العابرة للحدود.
- ✓ **إنشاء منصات تبادل المعلومات** :إنشاء منصات ومنظمات دولية لتبادل المعلومات والخبرات بين الدول في مجال مكافحة الجريمة الإلكترونية.

- ✓ **الاتفاقيات والمعاهدات الدولية** :تشجيع الدول على توقيع معاهدات واتفاقيات دولية تضمن التعاون القانوني والفني في مكافحة الجريمة الإلكترونية، وتسهيل تسليم المجرمين بين الدول.
- ✓ **تمويل الأبحاث والتطوير** :دعم الأبحاث والتطوير في مجال الأمن السيبراني لتطوير تقنيات وأدوات جديدة لمكافحة الجرائم الإلكترونية.
- ✓ **تعزيز البنية التحتية للأمن السيبراني** :الاستثمار في تحسين البنية التحتية للأمن السيبراني للدول والمؤسسات لتكون قادرة على مواجهة التهديدات الإلكترونية المتزايدة.

توعية وتدريب المجتمع: إطلاق حملات توعية تستهدف الجمهور العام والشركات لزيادة الوعي بأهمية الأمن السيبراني وكيفية حماية البيانات الشخصية والمعلومات الحساسة، وتدريب العاملين في مجالات إنفاذ القانون والقضاء على أحدث التقنيات وأساليب التحقيق في الجرائم الإلكترونية لضمان قدرتهم على ملاحقة المجرمين بفعالية.

قائمة

المصادر والمراجع

أ- النصوص القانونية:

- القانون رقم 09-04 الصادر في 05 أوت 2009 يتمضن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، جريدة الرسمية العدد47.
- القانون 16-01 المؤرخ في 06 مارس 2016 المتضمن التعديل الدستوري.
- المادة 02 من القانون 09-04 الصادر في 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، الجريدة الرسمية العدد 47 المؤرخة في 16 أوت 2009.
- القانون رقم 04-15 الصادر في 10 نوفمبر 2004 يعدل ويتمم الأمر رقم 66-156 الصادر في 08 جوان 1966 المتضمن قانون العقوبات الجريدة الرسمية، العدد 71.
- القانون رقم 15-03 المرخ في 11 ربيع الثاني عام 1436 الموافق 1 فبراير 2015 المتعلق بعصرنة العدالة جريدة رسمية عدد 6.
- القانون رقم 17-07 مؤرخ في 19 جمادى الأولى عام 1438 الموافق ل 16 فبراير سنة 2017 يعدل ويتمم القانون رقم 79-07 المؤرخ في 26 شعبان عام 1399 الموافق ل: 21 يونيو سنة 1979 والمتضمن قانو الجمارك.
- القانون رقم 18-07 المؤرخ في 25 رمضان عام 1439 الموافق ل: 10 يونيو 2018 يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي جريدة رسمية عدد34.
- المرسوم الرئاسي رقم 20-183 مؤرخ في 21 ذي القعدة 1441 الموافق ل 13 يوليو لسنة 2020 يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها جريدة رسمية عدد 40 **ملغى**.

- أمر رقم 20-04 مؤرخ في 11 محرم عام 1442 الموافق 30 غشت سنة 2020 يعدل ويتمم الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق ل 8 يوليو سنة 1966 والمتمضن قانون الإجراءات الجزائية جريدة رسمية رقم: 51.

ب- الكتب:

- إيهاب خليل، الأدلة الجنائية الرقمية: النظرية والتطبيق، دار النهضة العربية، الطبعة الثانية، 2021.
- إيهاب فاضل، الجرائم المعلوماتية والإلكترونية، دار الثقافة للنشر والتوزيع، الطبعة الأولى، 2016.
- حسين بن سعيد بن سيف الغافري: " الجهود الدولية في مواجهة جرائم الأنترنت
- سامح احمد، الجوانب الاجرائية للحماية الجنائية لجرائم الانترنيت
- عادل عبد العال ابراهيم خراشي، إشكاليات التعاون الدولي في مكافحة ج.م وسبل التغلب عليها، ط1، دار الجامعة الجديدة، الإسكندرية، 2015.
- عبد الفتاح بيومي حجازي، الجرائم المعلوماتية ، ط1، دار الفكر الجامعي، الإسكندرية، 2012.
- عبد الفتاح بيومي حجازي، الجريمة الإلكترونية: التحقيق والإثبات، دار الفكر الجامعي، الطبعة الأولى، 2019.
- عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكومبيوتر والأنترنت دراسة متعمقة في جرائم الحاسب الآلي والأنترنت ، ط1، دار الكتب القانونية القاهرة 2002.
- عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في الجرائم الكومبيوتر والأنترنت ، ط1، دار الفكر الجامعي، الإسكندرية، 2006.
- عبد الله بن ناصر الغامدي، التحقيق في الجرائم المعلوماتية، ط1، جامعة نايف العربية للعلوم الأمنية، الرياض، 2014.

- عبد الله عبد الكريم عبد الله، ، الجرائم المعلوماتية والأنترنت (الجرائم الإلكترونية) الطبعة الأولى منشورات الحلبي الحقوقية، بيروت، 2007
- فريد منعم جبور حماية المستهلك عبر الأنترنت ومكافحة الجريمة ودراسة مقارنة منشورات الحلبي الحقوقية بيروت، ط 2010 .
- محمد أمين الشوابكة، التحقيق الجنائي في الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، الطبعة الأولى، 2018.
- محمد أمين الشوابكة، جرائم الحاسب الآلي والإنترنت، ط1، دار الثقافة للنشر والتوزيع، عمان، 2009،
- محمد سامي الشوا، الجرائم المعلوماتية وأساليب مكافحتها، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2010.
- محمد سعيد الغامدي، مكافحة الجرائم الإلكترونية: التحديات والحلول، ط2، دار الفكر العربي، القاهرة، 2018.
- محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، عمان، 2005.
- نائلة عادل، محمد فريد قورة، جرائم الحاسب الألي الاقتصادية، دراسة نظرية وتطبيقية، منشورات الحلبي الحقوقية، بيروت، 2005، ط1.
- هدى حامد قشقوش، الجريمة المنظمة القواعد الموضوعية والإجرائية والتعاون الدولي، دار النهضة العربية، القاهرة 2002.
- هشام عبد العزيز مبارك، تسليم المجرمين بين الواقع و القانون دار النهضة العربية القاهرة 2006.

ج- المجلات:

- الأمم المتحدة، مكتب المخدرات والجريمة، الجرائم الإلكترونية: دراسة عالمية، منشورات الأمم المتحدة، 2013

- الزبيدي، مروان خالد، آليات حماية ضحايا الجرائم الإلكترونية: تحليل مقارن للتشريعات المحلية والدولية"، المجلة العربية لقانون تكنولوجيا المعلومات، المجلد 9، جامعة الملك سعود، العدد 1، 2020.
- السويدي، نورة سالم، التعاون الدولي في مكافحة الجرائم الإلكترونية: نحو إطار عمل فعال، مجلة سياسات الأمن السيبراني، المجلد 5، ع3، جامعة الملك سعود، 2019.
- زغودي عمر، مجلة البحوث القانونية والإقتصادية، الآليات القضائية للتعاون الدولي في مجال مكافحة الجريمة المنظمة عبر الوطنية، معهد الحقوق آفلو، 2020،
- عواطف محمد عثمان عبد الحليم جرائم المعلوماتية، تعريفها، صورها، جهود مكافحتها، دوليا وإقليميا ووطنيا، مجلة العدل العدد 24، السنة العاشرة دون سنة أو بلد النشر
- مريم عراب، الإختصاص القضائي في الجرائم المعلوماتية، مجلة حوليات، كلية، ح.و.ع.س جامعة وهران، 2 العدد3 2015/12/22.

د- المذكرات:

- حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي بحث مكمل لنيل شهادة الماجيستار في العلوم القانونية، تخصص علم الإجرام وعلم العقاب، جامعة الحاج لخضر باتنة 2011-2012.
- خالد بن مبارك القحطاني، التعاون الأمني الدولي في مواجهة ج، إ عبر الوطنية، أطروحة دكتوراه كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2006.
- سليمان أبو نمر، يوسف بوكشريدة، مكافحة الجريمة المعلوماتية في إطار القانون الدولي، مذكرة ماستر في الحقوق تخصص قانون دولي كلية الحقوق جامعة محمد خيضر بسكرة، 2020-2021، (جمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني)

- سمية مزغيش، جرائم المساس بالأنظمة المعلوماتية ، مذكرة مكملة من متطلبات نيل شهادة الماستر في الحقوق ، تخصص قانون جنائي ، جامعة محمد خيضر، بسكرة، 2013-2014.
- سوير سفيان، جرائم معلوماتية، مذكرة لنيل شهادة ماجيستير في العلوم الجنائية وعلم الإجرام جامعة أبو بكر بلقايد تلمسان، 2010-2011.
- شاشوة الزهرة، مكافحة الجريمة المنظمة في إطار نظام تسليم المجرمين، مذكرة ماستر في الحقوق تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة أكلي محند أولحاج البويرة، 2019-2020.
- صغير يوسف، الجريمة المرتكبة عبر الأنترنت، أطروحة مذكرة لنيل شهادة الماجيستير في القانون، تخصص القانون الدولي للأعمال كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو 2013.
- عبد الرحمن، خالد فهمي، ضحايا الجرائم الإلكترونية: دراسة ميدانية، رسالة دكتوراه، جامعة القاهرة، كلية الحقوق، 2020.
- غازي عبد الرحمان هيان الرشيد، الحماية القانونية، من الجرائم المعلوماتية، (الحاسب والأنترنت) أطروحة أعدت لنيل درجة الدكتوراه في القانون الجامعة الإسلامية في لبنان، كلية الحقوق، 2004.
- فهد عبد الله العبيد، الإجراءات الجنائية المعلوماتية، رسالة دكتوراه، كلية الحقوق، عين شمس، 2012.

هـ- مؤتمرات وندوات:

- إيهاب ماهر السنباطي، الجرائم الإلكترونية، قضية جديدة أم فئة مختلفة؟ التناغم القانوني هو السبيل الوحيدة الندوة الإقليمية حول الجرائم المتصلة بالكومبيوتر، المملكة المغربية يونيو 2007.

- براء منذر كمال عبد اللطيف، ناظر أحمد منديل – التعاون القضائي الدولي في مواجهة جرائم الأنترنت، المؤتمر العلمي الأول تحولات القانون العام في مطلع الألفية الثالثة كلية القانون جامعة تكريت العراق، 2009.
- مؤتمر الأمم المتحدة 12 لمنع الجريمة والعدالة الجنائية، البند 8 من جدول الأعمال المؤقت التطورات الأخيرة في إستخدام العلم والتكنولوجيا من جانب المجرمين والسلطات المختصة في مكافحة الجريمة بما فيها الجرائم الحاسوبية المنعقد بالبرازيل 12-19 أفريل 2010، رقم A/Conf 213/9
- موسى مسعود أرحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية" المؤتمر المغاربي الأول حول المعلوماتية والقانون أكادمية الدراسات العليا، طرابلس 2009.

و- المواقع الإلكترونية:

- http://www.alraby.com/uk/medianews/
- http://alukah.net/culture/
- http://minchaoui.com/

فهرس المحتويات