الإشكاليات القانونية للجرائم الإلكترونية العابرة للحدود وسُبل مواجهتها

Legal problems of cross-border cybercrime and ways to confront them

إعداد

د / هدية أحمد محمد زعتر

أستاذ القانون العام المساعد

كلية إدارة الأعمال – قسم القانون

جامعة المجمعة – المملكة العربية السعودية

Hedia Ahmed Mohamed Zaater

College of Business Administration

Majmaah University- KSA

الإشكاليات القانونية للجرائم الإلكترونية العابرة للحدود وسُبل مواجهتها

المستخلص:

يتناول البحث الجرائم الإلكترونية العابرة للحدود من حيث ماهيتها وطبيعتها القانونية والصور الشائعة لها والتي تمثل تهديداً خطيراً على الأمن المعلوماتي فيما يخص الاعتداء على الحياة الخاصة و على الأموال ، وما تثيره من صعوبات تتعلق بحجية الدليل الرقمي في الإثبات ، واشكاليات أثناء المعاينة والتفتيش وضعف خبرة سلطات التحقيق في مجالات التقنية ، وصعوبة الملاحقة الأمنية ، إلى جانب مشكلة تحديد القانون الواجب التطبيق ، وكيفية مواجهة تلك التحديات على الصعيد الدولي والوطني العربي .

الكلمات المفتاحية: الجرائم الإلكترونية ؛ المعلوماتية ؛ الإنترنت ؛ الفضاء السيبراني ؛ المتسللسن .

Abstract:

The research deals with cross-border cybercrime in terms of their nature, legal nature their common forms, which represent a serious threat to information security with regard to attacks on private life and funds, and the difficulties they raise related to the authenticity of digital evidence in proof, also problems during inspection and the weak expertise of the investigation authorities in the fields of technology, the difficulty of security pursuit, in addition to the problem of determining the applicable law, how to face those challenges at the international and the Arab national levels.

Keywords: cybercrime; Informatics; Internet; Cyberspace; Hackers.

المقدمة

نتيجة لما يمر به العالم من ثورة علمية هائلة وبخاصة في مجال تقنية الاتصالات والمعلومات ، و مع عبور شبكة الإنترنت المعلوماتية الحدود السياسية عبر القارات متخطية بسهولة كل الحواجز المكانية والزمانية بين دول العالم ، ورغم الميزات التقدمية الهائلة التي حققتها تلك الثورة المعلوماتية في خدمة الإنسانية ، إلا إنها أصبحت أداة لارتكاب جرائم رقمية خطرة وغير تقليدية (كالتجسس الإلكتروني – سرقة المعلومات الإلكترونية – النسخ غير المشروع للبرامج - الغش الإلكتروني والتلاعب في المصنفات الفنية الرقمية - إتلاف الأجهزة والسجلات الإلكترونية عن بُعد .. الخ) ، وهو ما يُعرف بظاهرة الإجرام المعلوماتي أو الإلكتروني.

وتُثير تلك الظواهر الإجرامية المُستحدثة العديد من الاشكاليات القانونية وبخاصة في نطاق الإجراءات الجزائية ، لصعوبة المعاينة والتحقيق في أحوال كونها عابرة الحدود ، ولصعوبة جمع الأدلة الجنائية الخاصة بها لسرعة ارتكابها في دقائق معدودة ولسهولة محو أدلتها ذات الطبيعة الرقمية ، فهي جرائم ذات طبيعة خاصة ويتمتع مجرميها بمهارات خاصة ، الأمر الذي أصبح معه حماية أمن المعلومات والاتصالات والشبكات حكومية كانت أو غير حكومية تمثل الأولوية العظمى .

أسباب اختيار موضوع البحث:

نتناول في بحثنا هذا موضوع " الاشكاليات القانونية للجرائم الإلكترونية العابرة للحدود وسُبل مواجهتها " لمحاولة الوقوف على التحديات والصعوبات التي تواجه جهات التحقيق عند ارتكاب الجرائم الإلكترونية وبخاصة تلك التي تكون عابرة للحدود ، و من ثم محاولة إيجاد المقترحات القانونية المناسبة لمواجهة تلك التحديات ،

وبخاصة تلك التي تمس المصلحة الوطنية الجديرة بالحماية أمام حالات تنازع الاختصاص بين الدول نظراً لكونها جرائم دولية، بهدف ترقية التشريعات الوطنية والوصول لاتفاقيات دولية ملائمة للتصدي لتلك الجرائم ومكافحاتها بما يضمن تحقيق الأمن و العدالة.

إشكالية البحث:

يُعد التطور التقني الهائل و السريع سبباً قوياً في التحور المستمر في طرق ارتكاب الجرائم الإلكترونية ، والتي قد تصل لدرجات مرعبة من الذكاء الإجرامي الذي قد يصعب ضبطه وملاحقته، الأمر الذي يحتاج دائماً لتدريب جهات التحقيق من الناحية التقنية على أعلى مستوى لاستيعاب الإحداثيات المتتابعة والمتلاحقة على تكنولوجيا المعلومات أولاً بأول ، وذلك لخدمة التدقيق الجنائي في كل مراحل الجريمة ، وإعداد المقترحات التشريعية الملائمة لهذه التطورات أولاً بأول لسد الفراغ بين النص التشريعي وتطورات التقنية المتلاحقة .

وقد واجهنا أثناء اعداد البحث عدد من التساؤلات الهامة التي سعينا جاهدين لإيجاد إيجابات لها ومحاولة وضع الرؤى نحو الحلول الأمثل ، منها:

كيف نحمي المعلومات والبيانات الخاصة للأفراد من القرصنة الإلكترونية ؟ ، كيف نضع إطار من الحماية الجنائية للأموال في مواجهة التحايل الإلكتروني ؟ ، إلى أي مدى يمكن اعتبار المعلومات من الأموال التي يمكن سرقتها ؟ ، وهل من الممكن إعمال حجية للمستندات الإلكترونية والأدلة الرقمية في الإثبات ؟ ، وهل تجوز المعاينة في الفضاء الإلكتروني ؟ ، وكيفية التغلب على صعوبة جمع الأدلة الإلكترونية السهلة وسريعة التلف والاختفاء ؟ ، و كيف يمكن التغلب على التنازع الإجابي للاختصاص

القضائي لأكثر من دولة لكون تلك الجرائم عابرة للحدود ؟ ، وأخيراً: ما هي التدابير التي يجب اتباعها لمواجهة تلك الجرائم تقنياً وتشريعياً؟.

منهج البحث:

وجدنا في المنهج الوصفي التحليلي خير وسيلة للتعرف على أنواع تلك الجرائم المستحدثة وطبيعة مُرتكبيها ومن ثم الطبيعة القانونية لها ، للوقوف على المصلحة الجديرة بالحماية ومن ثم تحليل المشكلات القانونية التي تثيرها تلك الجرائم ، لتحديد التدابير القانونية الأنسب لمواجهتها.

الدراسات السابقة:

من الدراسات السابقة المتميزة ، دراسة بعنوان (المشكلات العملية والقانونية للجرائم الإلكترونية – دراسة مقارنة)، عبد الله دغش العجمي ، رسالة ماجستير ، جامعة الشرق الأوسط ، الأردن ٢٠١٣ ، حيث جائت الدراسة شاملة لمفهوم وصور الجرائم الإلكترونية و تطرقت لطبيعة المشكلات الموضوعية والإجرائية التي تثيرها تلك الجرائم ، وأوردت تطبيقات قضائية في مجال تلك الجرائم مع بيان موقف بعض التشريعات المقارنة ، وكذلك بينت الإطار الدولي والإقليمي في مجال مكافحة مشكلات الجرائم الإلكترونية.

وكذلك دراسة بعنوان (مبدأ العالمية في القانون الجنائي) ، مروى السيد الحصاوي، رسالة دكتوراه ، جامعة المنصورة ٢٠١٩، والتي اهتمت بطرح المعايير البديلة لمبدأ الإقليمية ، الذي أصبح من الصعب التمسك به في ظل الجرائم العابرة للحدود متعددة التنازع في الاختصاص ، وعلى رأسهم مبدأ العالمية والأخذ بجنسية المجنى عليهم ، وهو مستحسن لدينا إلى جانب الأخذ بمدأ العينية التي تأخذ به مصر .

خطة البحث:

قمنا بتقسيم البحث إلى خمسة مباحث ، نتناول في الأول ؛ الطبيعة القانونية لتلك الجرائم ، وفي الثاني ؛ التطرق لأنواع الجرائم الإلكترونية ، وفي الثالث؛ التعرف على المصلحة الجديرة بالحماية الجنائية، وفي الرابع؛ طرح التحديات الموضوعية والإجرائية المتعلقة بتلك الجرائم ، وأخيرًا؛ التعرف على التدابير الواجب اتباعها لمواجهة الجرائم الإلكترونية .

المبحث الأول

الطبيعة القانونية للجرائم الإلكترونية

يُطلق على الجرائم الإلكترونية مسميات عدة : الجرائم المعلوماتية ، الجرائم السيبرانية ، جرائم الفضاء الإلكتروني ، جرائم الحاسب والإنترنت ، الجرائم الرقمية ، والجرائم النظيفة ، وهي بطبيعتها تشير إلى أي جريمة تتضمن استخدام الحاسب الآلي و الشبكة المعلوماتية / الإنترنت. (١)

(١) بدأت فكرة الإنترنت مع إنشاء وزارة الدفاع الأمريكية عام ١٩٦٤ شبكة من الحواسيب ذات قدرة على الاستمرار في العمل حال حدوث أية كوارث ، نفذتها وكالة الأبحاث المتقدمة ARPA وحملت اسم (أربانت) ١٩٦٩ ، كانت في بدايتها تربط أربعة حواسيب آلية ضخمة ، ثم تم إيصالها إلى معظم الجامعات الأمريكية ١٩٧٢ ، وفي عام ١٩٧٣ بدأت الاتصالات الدولية عبر هذه الشبكة بين إنجلترا والنرويج ، وفي ذات العام ، تم اكتشاف بروتوكولي الإنترنت (TCP/IP) ، واصبحت أربانت متاحة لجميع أشكال البحث العلمي في أمريكا عام ١٩٨٦ ، وظلت الشبكة محصورة الاستعمال للأغراض العسكرية والبحثية العلمية حتى إنهيار الاتحاد السوفيتي ١٩٩٠ تم إطلاق العنان أمام استخدامها وتحولت إلى تسمية جديدة (إنترنت) ، وفي ١٩٩١ تم اختراع تقنية الويب ((wwwوالتي ساعدت على تصفح المعلومات واستعراضها بسهولة على شبكة الإنترنت من خلال بروتوكول نقل النصوص الترابطية HTTP الذي يسمح بربط مواقع الويب الموصولة بالشبكة فيما بينها ، وهو لا يعمل إلا بواسطة برامج تصفح خاصة مثل Internet Explorer، وتشرف على شبكة الإنترنت جهات متخصصة ليست مالكة له مثل: جمعية الإنترنت ISOC الأمريكية - الاتحاد الدولي للاتصالات ITU - منظمة الأيكان ICANN المسئولة عن منح أسماء المواقع والعناوين ، كرموز التعريف الجغرافي للدول (.sa- eg- uk) ، عدا USA ليس لها تعريف جغرافي، و أسماء النطاقات حسب النشاط (.edu للتعليمية – .gov للحكومية .com للتجارية) - وهيئة IANA تتولى تنظيم المواقع والنطاقات. للمزيد أنظر: الحسيني، عبد الحسن .(٢٠٠٤) ، القاموس الموسوعي في المعلومات والاتصالات والمعلوماتية القانونية ، مكتبة صادر ، الطبعة الأولى ، بيروت .

ويُستخدم مصطلح الإلكترونية - cyber- للدلالة على استخدام الحاسب والإنترنت معاً ، و قد يكون الحاسب إما أداةً لارتكاب الجريمة ، أو هدف للجريمة ذاتها.

ومن جانبنا نُرجح تعريف OECD للجرائم الإلكترونية والتي تصفها بأنها : كل سلوك غير مشروع أو غير قانوني أوغير أخلاقي يكون مرتبط بالمعالجة الآلية للبيانات او نقلها [١] ، حيث جاء التعريف مبسطاً وشاملاً لكل سلوك فيه اعتداء ويشمل كل آلة ممكن تصلح أداة ولوج عبر الإنترنت لارتكاب الجريمة (حاسب ، أندرويد ، وما قد يُستجد مثل الـ (Metaverse). [٢].

وعرفها النظام السعودي الصادر عام ٢٠٠٧ : أي فعل يخالف النظام وينتهك أحكام القانون ويتم ارتكابه باستخدام الحاسب الآلي أو شبكة المعلومات و يكون مرتبط بالحاسب وشبكة المعلومات. [٣]

ونرى أن مصطلح الجريمة الإلكترونية الأكثر شمولاً عن غيره من المصطلحات ، لقدرته على استيعاب وسائل الاتصال الإلكترونية المعروفة حالياً ، وما قد تستجد في المستقبل .

---

(١) دليل الأمن السيبراني للبلدان النامية ، الاتحاد الدولي للاتصالات ITU ، طبعة ٢٠٠٧ ، ص٢٧ متاح على موقع الاتحاد: www.itu.int

(٢) أعلن مارك زوكيربيرج مالك شركة فيس بوك ٢٨ اكتوبر ٢٠٢١ عن بدء اطلاق نظام تواصل اجتماعي Metaverse جديد عبر عوالم افتراضية بدلا من منصات التواصل الاجتماعي التقليدية ، من خلال استخدام نظارات ثلاثية الأبعاد . للمزيد أنظر: مقال منشور بجريدة الاهرام بتاريخ ٢٠٢١/١٠/٢٨ على الرابط : https://gate.ahram.org.eg/News/3079513.aspx

(٣) مادة ١ من نظام مكافحة الجرائم المعلوماتية الصادر بالمرسوم الملكي رقم م/١٧ بتاريخ ٨ / ٣ / ١٤٢٨

ويعتبرالإنترنت العنصر الأساسي في اعتبار الجريمة إلكترونية لكونه الوسيلة وأداة التواصل بين شبكات المعلومات عبر الحدود ، مرتكزاًعلى وسيلة التخاطب الرقمي ، والتي تتم من خلال بروتوكولي: (IP&TPC) [١] .

وتلعب شبكة الإنترنت دور رئيسي في الجريمة الإلكترونية : فهي إما أن تكون هدف للجريمة - كما في حالة الدخول الغير مُصرح به لبعض الشبكات بهدف تدمير الملفات أو الاستيلاء على البيانات المخزنة بها [٢] ، أو تكون هي ذاتها: أداة الجريمة ، حيث لا يتصور وقوع الجريمة بدونها - كحالة استخدام الإنترنت في عمليات التزييف والتزوير ، وقد يكون الإنترنت بمثابة البيئة التي ينمو في رحمها الإجرام المعلوماتي (كتنظيم اللجان الإلكترونية الغير مشروعة).

و ينقسم الفقه حول الطبيعة القانونية لمحل الجريمة الإلكترونية إلى اتجاهين:

الاتجاه الأول: يرى أن المعلومات ذات طبيعة معنوية لا يمكن حيازتها أو سرقتها ، ما لم تكن محمية وفقاً لحقوق الملكية الفكرية ومخزنة في وسائل تخزين مادية . [٣]

---

(١) يتم التراسل من خلال بروتوكولين أساسيين : ١- بروتوكول التحكم في النقل TCP (Transfer Control Protocol) المسئول عن تجزءة الرسالة المراد إرسالها إلى رزم من المعلومات تحمل معلومات تعريفية عن الراسل والمرسل إليه ، و ٢- بروتوكول الـ IP (Internet Protocol وهو المسؤول عن عنونة وترقيم وتوجيه الرسائل إلى عناوينها المقصودة ، ويمنح كل جهاز على الشبكة رقم معين وصل إلى ١٢٨ رقمًا مع النمو المتزايد للمتصلين بالشبكات ، للمزيد : يونس ، بن عمر (٢٠٠٤) الجرائم الناشئة عن استخدام الإنترنت ، الطبعة الأولى ، دار النهضة العربية ، القاهرة ، ص ٣٨

(٢) العجمي ،عبد الله دغش ، (٢٠١٤) ، " المشكلات العملية والقانونية للجرائم الإلكترونية – دراسة مقارنة " ، أطروحة لاستكمال رسالة الماجستير في القانون العام ، جامعة الشرق الأوسط، ص ص ٣٧-٣٩

(٣) المطردي ، مفتاح بو بكر . (٢٠١٢) ، المستشار بالمحكمة العليا الليبية ، " الجريمة الإلكترونية والتغلب على تحدياتها " ورقة مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية بجمهورية السودان المنعقد في ٢٣-٢٥ /٢٠١٢/٩.

الاتجاه الثاني : يرى أن المعلومات ذات قيمة اقتصادية قابلة للحيازة غير المشروعة ، لذلك فهي تستحق الحماية القانونية ومعاملتها معاملة المال المادي. [١]

وفي رؤيتنا وما نميل إلى ترجيحه: هو أن المعلومات كيان مادي يمكن الاستحواذ عليه حتى ولو بصورة ذهنية عبر الحاسة البصرية.

*** خصائص الجرائم الإلكترونية:**

تتمتع الجريمة الإلكترونية بمجموعة من الخصائص التي تميزها عن الجرائم التقليدية : حيث أنها: [٢]

١. **جرائم ترتكب عبر شبكة الإنترنت أو عليها.**
٢. **يستخدم المجرم الإلكتروني أدوات وتقنيات خاصة باستخدام شبكة الإنترنت الذي لا تصور تنفيذ الجريمة بدونها .**
٣. **مُرتكبيها ذو مهارات فنية خاصة في أنظمة الشبكات و الاتصالات والحواسيب ، ولديهم من المهارة والذكاء ما يمكنهم من محو أثر جريمتهم بسهولة ، يطلق على الهواة منهم الهاكرز Hackers ، ويطلق على المحترفين الأشد خطورة الكراكرز Crackers وهم معتادي الإجرام الإلكتروني.**
٤. **جريمة لا تعرف الحدود الجغرافية فقد تقع داخل الدولة ، وقد تقع في نطاق القانون الدولي متى كان أحد أطرافها شخصاً دولياً ، وقد تكون جريمة ذات بُعد**

---

(١) العفيفي ، يوسف خليل يوسف. (٢٠١٣) ، " الجريمة الإلكترونية في التشريع الفلسطيني " رسالة لاستكمال متطلبات الحصول على درجة الماجستير في القانون العام من كلية الشريعة والقانون، بالجامعة الإسلامية بغزة ، ص ٤٦ وما بعدها.

(٢) قطب ، محمد علي (بدون سنة نشر)، "الجرائم المعلوماتية وطرق مواجهتها "، الأكاديمية الملكية للشرطة وزارة الداخلية ص ١٢-١٣.

دولي متى تم اتفاق المجتمع الدولي على اعتبار جريمة إلكترونية معينة تُشكل عدواناً على كل الدول .

٥. جريمة من الصعب اكتشافها واثباتها لكونها لا تترك أثراً مادياً يمكن ضبطه ، لكونها تتم من خلال نبضة إلكترونية ينتهي دورها خلال أقل من ثانية .

٦. جريمة تستهدف المعلومات لذلك فهي أكثر تعقيداً وصعوبة في الإثبات لأن الجاني بها غالباً ما يكون محترف معلوماتي لا يترك وراؤه أثر مادي ملموس.

٧. جريمة مُستحدثة فرضتها ظروف العصر والعولمة وتُعد من أشد الجرائم الجديدة خطورة وجسامة.

٨. تتعدد الأوصاف القانونية (للمعلومات التي تعتبر محلاً للجريمة) ، فقد تظهر بصورة مادية محفوظة على اسطوانات ممغنطة ، وقد تكون في حالة غير مادية / إلكترونية حال وجودها في ذاكرة النظام الإلكتروني ذاته.

٩. ليس لها مسرح جريمة محدد ، لكونها سريعة وسهلة التنفيذ في أي مكان ومن أي مكان المهم توافر الأدوات.

١٠. جريمة ذات تكلفة أقل ، لا تحتاج تدخل شخصي من الجاني ولا تعتمد على العنف، ويسهل ارتكابها عن بُعد.

١١. يمكن استخدام أدوات الجريمة أكثر من مرة (الحاسب ومرفقاته - شبكة الإنترنت).

١٢. الإنترنت في تلك الجرائم أداة تنفيذ للجريمة وتتبع لها في ذات الوقت.

وتُعد تلك الخصائص للجريمة الإلكترونية أسبابًا في حد ذاتها جاذبة لارتكاب الجرائم الإلكترونية ، لتوفرها وسهولتها وصعوبة اكتشافها وإدانه مُرتكبيها وضبطهم .

المبحث الثاني

أنواع الجرائم الإلكترونية

يجب التفرقة بين جرائم الكمبيوتر ، وجرائم الإنترنت ، فالأولى: تتحقق بالاعتداء على الحاسب الآلي ومكوناته ، أما الثانية : فتتحقق بمعالجة المعلومات أو نقلها بطريقة غير مشروعة عبر شبكة الإنترنت ، ولكن الواقع التقني فرض الدمج بين الجريمتين ، لذلك ظهر مصطلح (Cybercrime).

أولاً: أنواع الجرائم الإلكترونية/ المعلوماتية:

تناولت اتفاقية بودابست الأوروبية الصادرة عن المجلس الأوروبي ٢٣ نوفمبر ٢٠٠١ [١] أربعة أنواع لجرائم الحاسب الآلي والإنترنت ، وهي:

١) الجرائم التي تمس أمن المعلومات (كالاختراق والدخول الغير مصرح به).

٢) الجرائم المرتبطة في ارتكابها بجهاز الحاسب الآلي نفسه (كجريمة التزوير المتعلقة بالحاسب).

٣) جرائم الإنتاج و النشر غير المشروع للمواد الإباحية والفاضحة .

---

(١) اتفاقية بودابست الصادرة عن المجلس الأوروبي عام ٢٠٠١ أول اتفاقية دولية تضع الاطار العام لحماية أمن المعلومات، ، دخلت حيز التنفيذ مايو ٢٠٠٤. للاطلاع على الاتفاقية تصفح الرابط : https://rm.coe.int/budapest-convention-in-arabic/1680739173

وللاطلاع على التقرير التفسيري لها تصفح الرابط:

https://rm.coe.int/explanatory-report-budapest-convention-in-arabic/1680739174

٤) جرائم الاعتداء على حقوق الملكية الفكرية وحقوق الطبع والنشر،

وقد صنفها مكتب الأمم المتحدة للمخدرات والجريمة [١] من خلال استبيان تم عرضه على الدول ومنظمات القطاع الخاص والمنظمات الحكومية الدولية إلى ثلاث فئات:

١- الأفعال الماسة بسرية المعلومات وحماية بيانات الحاسب ، كالدخول غير المشروع لجهاز الحاسب واختراق الخصوصية.

٢- الأعمال ذات الصلة بأجهزة الحاسب الشخصية التي تسبب الضرر.

٣- الأفعال ذات الصلة بمحتويات الحاسب كانتاج وحيازة الصورالإباحية.

ثانياً: الصور الشائعة للجرائم الإلكترونية/ المعلوماتية: [٢] .

١. قرصنة أجهزة الحاسب بالقنابل البريدية و الفيروسات المدمرة بغرض اتلاف البيانات والمعلومات بغرض التخريب ، وهذا يشكل خطورة أمنية كبرى عندما يتم اقتحام خوادم البنوك والمؤسسات الحكومية السيادية لتخريب ما بها من بيانات ومعلومات أو سرقتها .

٢. نسخ برامج الـ Software بشكل غير قانوني واستخدامها وبيعها مرة أخرى كنسخ مقلدة ، وهذا انتهاك لحقوق الملكية الفكرية لصانعي البرامج الأصليين.

---

(1) UNODC United Nations Office on Drugs and Crime (2013).Comprehensive Study on Cybercrime. United nations.

(٢) الخن ، طارق . (٢٠١٨) ، " جرائم المعلوماتية " الجامعة الافتراضية السورية ص. ٢٩ – ٧٢ متاح على الرابط : https://pedia.svuonline.org بصيغة pdf

٣. الدخول بطرق غير قانونية بغرض سرقة المعلومات أوالاطلاع عليها ونسخها وإعادة استخدامها بدون ترخيص أو بغرض التخريب.

٤. تزوير وتزييف المعلومات وتحريفها، مثل تغيير علامات الطلاب، أو إصدار سجلات شهادات لم تنسب حقيقة لنظام تعليمي معتمد.

٥. التسلسل للحسابات الخاصة والتطفل على معلومات وصور ذات طبيعة خاصة ونشرها بغرض التشهير.

٦. التصنت وسرقة المحادثات واستخدامها بطريق الابتزاز.

٧. قرصنة البيانات عالية السرية بهدف السطو والاحتيال ـ كسرقة بيانات البطاقة الائتمانية ، والأرقام السرية للدخول .

٨. نشر ما يُحث على الخلاعة و الجنس التخيلي Cyber Six.

٩. المضايقة بالتطفل والتتبع الإلكتروني واستهداف الخصوصيات ، والتحرشات اللفظية الخادشة للحياء.

١٠. الإرهاب الإلكتروني : ويقوم به مجموعة من المحترفين الإلكترونيين Cracker و أحياناً تكون وكالات دوليّة متخصصة، مستغلة ثغرات المواقع والأنظمة . [١]

---

(١) جرمها النظام السعودي في المادة السابعة حيث نص على : يعاقب بالسجن مدة لا تزيد على عشر سنوات وبغرامة لا تزيد على خمسة ملايين ريال، أو بإحدى هاتين العقوبتين كلُّ شخص يرتكب ..... ١ ـ إنشاء موقع لمنظمات إرهابية على الشبكة المعلوماتية ، أو أحد أجهزة الحاسب الآلي أو نشره؛ لتسهيل الاتصال بقيادات تلك المنظمات، أو أي من أعضائها أو ترويج أفكارها أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرات، أو أي أداة تستخدم في الأعمال الإرهابية .

وقد عدد قانون مكافحة جرائم تقنية المعلومات المصري ٢٠١٨ الجرائم الإلكترونية بالباب الثالث منه وصنفها إلى ما يلي : [١]

١- جرائم الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات:

- **جريمة الانتفاع بدون حق بخدمات الاتصالات والمعلومات وتقنيتها.**
- **جريمة الدخول غير المشروع.**
- **جريمة تجاوز حدود الحق في الدخول.**
- **جريمة الاعتراض غير المشروع.**
- **جريمة الاعتداء على سلامة البيانات والمعلومات والنظم المعلوماتية.**
- **جريمة الاعتداء على البريد الإلكتروني أو المواقع أو الحسابات الخاصة.**
- **جريمة الاعتداء على تصميم موقع.**
- **جريمة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة.**
- **جريمة الاعتداء على سلامة الشبكة المعلوماتية.**
- **حيازة البرامج والأجهزة والمعدات المستخدمة في ارتكاب جرائم تقنية المعلومات.**

---

(١) قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ متاح على الرابط :
https://manshurat.org/node/31487

٢- الجرائم المُرتكبة بواسطة أنظمة وتقنيات المعلومات:

- جرائم الاحتيال والاعتداء على بطاقات البنوك والخدمات وأدوات الدفع الإلكتروني.
- الجرائم المتعلقة باصطناع المواقع والحسابات الخاصة والبريد الإلكتروني.

٣- الجرائم المتعلقة بالاعتداء على حرمة الحياة الخاصة والمحتوى المعلوماتي غير المشروع

٤- الجرائم المُرتكبة من مدير الموقع

ومن التشريعات العربية التي تناولت مكافحة الجرائم الإلكترونية : القانون العماني لمكافحة الجرائم الإلكترونية ٢٠٠١ ، والقانون العربي الاسترشادي لمكافحة الجرائم المعلوماتية عام ٢٠٠٤ ، والقانون الإماراتي ٢٠٠٦ ، والنظام السعودي عام ٢٠٠٧ ، و القانون العربي الإسترشادي للإثبات بالتقنيات الحديثة ٢٠٠٨ ، والقانون الأردني ٢٠١٥ ، والقانون المصري الجديد ٢٠١٨، و الفلسطيني ٢٠١٨.

المبحث الثالث

المصلحة الجديرة بالحماية الجنائية في الجرائم الإلكترونية

حتى يتسنى لنا التعرف على المسئولية الجنائية والمصلحة الأولى بالحماية في هذا النوع من الجرائم يتعين لنا أولاً: التعرف على أركان الجريمة الإلكترونية ، ومن ثم المصلحة الجديرة بالحماية الجنائية.

المطلب الأول

أركان الجرائم الإلكترونية

يشترط لوقوع أي جريمة يعاقب عليها القانون وجود ثلاثة أركان أساسية وهما : الركن المادي والركن المعنوي والركن الشرعي ، وبدونهما ينتفي وجود الجريمة .

أولا: الركن القانوني / الشرعي للجريمة :

يُقصد به وجود نص تشريعي يُجرم الفعل ويحدد العقاب المترتب علي إتيان الفعل غير المشروع ، فلا جريمة ولا عقوبة بغير نص قانوني .

وعلى الصعيد الدولي : أولت الأمم المتحدة و أغلب المنظمات الدولية اهتمامًا كبيراً بالجرائم الإلكترونية لخطورتها الكبيرة، عن طريق إبرام مجموعة من الاتفاقيات

الدولية التي تناولت تلك الجرائم وآليات مكافحتها والتصدي لها، ومن أهم تلك الاتفاقيات الدولية :

- اتفاقية برن لحماية المصنفات الأدبية والفنية. (١)
- معاهدة الويبو ١٩٩٦ بشأن حق المؤلف / والحق في الأداء والتسجيل الصوتيضمت لها المملكة في ٢٢ فبراير ١٩٨٢ . (٢)
- اتفاقية تريبس ١٩٩٤: بغرض حماية الجوانب التجارية لحقوق الملكية الفكرية من السطو الإلكتروني. (٣) .
- اتفاقية بودابست بشأن جرائم الإنترنت ٢٠٠١ : و تعد أول معاهدة دولية لمواجهة جرائم الإنترنت و الحاسوب ، عن طريق مواءمة القوانين الوطنية ، وتحسين أساليب التحري، وزيادة التعاون بين الدول (٤)

و تعتبر اتفاقية بودابست الصادرة عن المجلس الأوروبي عام ٢٠٠١ أول اتفاقية دولية تضع الإطار العام لحماية أمن المعلومات ، وتعد أهم الاتفاقيات الدولية المنظمة للجريمة الإلكترونية ، ومن رحمها أصدرت و عدلت كثير من الدول تشريعاتها الداخلية بما يتواكب وأحكام تلك الاتفاقية في مكافحة الجريمة الإلكترونية الدولية وبما يضمن التعاون الدولي فيما بينها.

---

(١) انضمت لها المملكة العربية السعودية في ١١ ديسمبر ٢٠٠٣ ، بخصوص اتفاقية برن تصفح الرابط : https://www.wipo.int/treaties/ar/ip/berne/index.html

(٢) الويبو(هي المنظمة العالمية للملكية الفكرية) وهي منظمة دولية حكومية تتبع الأمم المتحدة. تصفح الموقع الرسمي للمنظمة على الرابط : https://www.wipo.int/portal/ar

(٣) بخصوص اتفاقية TRIPSتصفح الرابط :

https://www.wto.org/english/tratop_e/trips_e/trips_e.htm

(٤) بخصوص اتفاقية بودابست : رابط سابق الاشارة هامش ص ٧

ثانيًا: الركن المادي للجريمة : [١]

يتمثل في كافة الاعتداءات المادية وانتهاك كل ما هو محل حماية قانونية ؛ ويعتمد على ثلاثة عناصر أساسيّة:

١. **الفعل أو السلوك الإجرامي: سواء كان إيجابي يخالف القانون (كتعمد اختراق شبكة معلومات غير مصرح بالولوج إليها) أو فعل سلبي بالامتناع عن اتيان عمل كان يتعين الاتيان به (كإغفال مهندس النظم والمعلومات بالمؤسسة بتطوير وتحديث نظم حماية البيانات والمعلومات لفترات طويلة مما تسبب في سهولة اختراقها وسرقة معلوماتها) [٢] .**

٢. **النتيجة: هي كل ضرر ناتج عن فعل أو سلوك إجرامي ، وتختلف درجة الضرر في الجرائم الإلكترونية : فهناك ضرر قد يصل للقتل (كتعمد طبيب الولوج إلى قاعدة بيانات المستشفى التي يعمل بها ، وتغيير تركيبة دواء خاصة بمريض بعينه لإحداث الوفاة العمدية له) ، وهناك ضرر مادي (كخسائر اتلاف الاجهزة والبيانات) ، أو معنوي (كالتعرض للسب والقذف وتشويه السمعة بدون وجه حق باستخدام وسائل التواصل الاجتماعي) [٣] .**

٣. **علاقة السببية:هي تلك الرابطة التي تجمع بين السلوك الإجرامي، وما ترتب عليه من نتيجة ، وهي العنصر الأساسي المكون للركن المادي للجريمة الإلكترونية ، وتحققها شرط جوهري لثبوت المسئولية الجنائية.**

---

(١) قورة ، نائلة عادل محمد فريد .(٢٠٠٥). " جرائم الحاسب الآلي الاقتصادية ، الطبعة الأولى ، منشورات الحلبي الحقوقية بيروت ،ص.ص٣٢٢- ٣٤٣

(٢) العفيفي ، يوسف خليل يوسف. (٢٠١٣) ، مرجع سالف الذكر ص.ص ٥٢-٥٣

(٣) المرجع سابق ص ٥٤

وتوفر الركن المادي في الجرائم الإلكترونية يفترض وجود بيئة رقمية واتصال بالشبكة المعلوماتية ، ويتطلب معرفة النشاط الإجرامي وبداية الشروع فيه وصولاً لموعد حدوث النتيجة.

و يُعتبر العمل التحضيري في الجريمة الإلكترونية - جريمة في حد ذاته- كشراء البرامج المخصصة لعملية اختراق الأنظمة المعلوماتية ، ومعدات فك الشفرات واختراق كلمات المرور، وحيازة صور مُخلة لأغراض الابتزاز أو التحرش المُجرَم ، ويصحبه بالتبعية دخول غير مشروع أو غير مصرح به للموقع الإلكتروني المستهدف ، بغرض: السرقة ، الاستيلاء ، التزوير ، التحايل ، أو النسخ الغير مشروع للمعلومات المستهدفة... الخ [١] ، والواقع يشير دائماً إلى صعوبة الفصل بين العمل التحضيري وبين البدء في النشاط الإجرامي .

ثالثا: الركن المعنوي للجريمة :

يمثل الركن المعنوي الحالة النفسية للجاني [٢] ، وهو القصد الجنائي في الاتيان بسلوك غير مشروع وضار بهدف تحقق نتيجة ما ، وله دور هام في معرفة طبيعة السلوك المُرتكب وماهيته والهدف منه ، وتحديد التكييف القانوني المناسب للجريمة لتحديد النص الواجب التطبيق، ونفرق بين :

(١) قورة ، نائلة عادل محمد فريد .(٢٠٠٥). مرجع سابق ص ٣٣٣

(٢) حسني ، محمود نجيب .(١٩٧١) " النظرية العامة للقصد الجنائي " ، دار النهضة العربية ، ط٢ ، ص ٩٠

- القصد العمدي : كتعمد الاختراق غير المشروع لمنصة ما ، هنا نكون أمام جريمة عمدية يتوفر فيها القصد الجنائي العام بعنصريه :العلم والإرادة الآثمة. (١)

- القصد الغير متعمد : كحالة الدخول المشروع مع تجاوز الصلاحيات المسموح بها، فقد تكيف الواقعة بأنه خطأ غير مقصود من المُستخدم (قد يكون سببه عيب في أنظمة الحماية الخاصة بالشبكة المستخدمة) ومن ثم فلا مسئولية جنائية على الشخص ، أما لو ثبت التعمد في إختراق الصلاحيات المحظورة عليه ، هنا يتوفر القصد الجنائي وتقع الجريمة .

وقد اتجه القضاء الأمريكي إلى ضرورة توفر العلم (بدخول محظور) والإرادة (الصريحة المتعمدة) لثبوت القصد الجنائي في جرائم الإنترنت ، ويتمثل العلم هنا بمثابة القصد الخاص الذي يُطبق عليه الظرف المُشدد للعقوبة (٢)، بينما اكتفى القضاء الفرنسي بإثبات سوء النية في جرائم الإنترنت. (٣)

(١) من القضايا التي مثلت دخول غير مشروع / القبض على عصابة في مصر مكونة من ثلاثة أشخاص قامو بتصميم موقع يشبه موقع بعض المصارف ، وقاموا بإرسال رسائل عشوائية عن طريق البريد الإلكتروني إلى عملاء حقيقيين ، لينخدعوا ويدخلو بيانتهم المصرفية على الموقع المزيف بالطرق التي يحددها المُتهمون ، ومن ثم وبعد التعرف على البيانات السرية ، يتم الاستيلاء على أموالهم ، للمزيد: الشناوي ، محمد. (٢٠٠٨) " جرائم النصب المستحدثة " ، دار الكتب القانونية ، المحلة الكبرى ، القاهرة ص ١٣٣

(٢) برزت تلك المشكلة في قضية موريس الذي كان متهما في قضية دخول غير مصرح به علي جهاز حاسوب فيدرالي وقد دفع محامي موريس علي انتفاء الركن المعنوي الأمر الذي جعل المحكمة تقول " هل يلزم أن يقوم الادعاء بإثبات القصد الجنائي في جريمة الدخول غير المصرح به، بحيث تثبت نية المُتهم في الولوج إلي حاسوب فيدرالي، ثم يلزم إثبات نية المُتهم في تحدي الحظر الوارد علي استخدام نظم المعلومات في الحاسب وتحقيق خسائر، ومثل هذا الأمر يستدعي التوصل إلي تحديد أركان جريمة الدخول دون تصريح ". وبذلك ذهبت المحكمة إلي تبني معيارين هنا هما : الإرادة بالدخول غير المصرح به، وكذلك معيار العلم بالحظر الوارد علي استخدام نظم معلومات فيدرالية دون تصريح.

(٣) يونس ، بن عمر (٢٠٠٤) ، مرجع سابق ذكره ص ٣٢٢- ٤٠٢.

- **ويتوفر القصد الجنائى فى حق الجانى الإلكترونى فى الحالات الآتية:** [1]

١. إذا كان الجاني يتعمد من فعله أو امتناعه ، حدوث نتيجة تمثل ضرر أو خطر يعلم أنها محل تجريم للقانون.

٢. إذا نجم عن فعله/أو امتناعه ضرر أو خطر أكثر جسامة عما كان متوقعاً ، وهذه الحالة تستوجب مساءلة هواة الاختراق من أجل الخبرة ، حتى لو لم يقصدون ايقاع ضرر بالآخرين.

٣. الحالات التي يفترض فيها القانون توفر القصد الجنائي بمجرد القيام بالفعل أو الامتناع عن الفعل.

رابعا: (الشروع) أو المحاولة فى الجرائم الإلكترونية:

اهتم المشرع الفرنسي بتجريم مجرد المحاولة في الجرائم الإلكترونية وعاقب عليها بنفس عقوبة الجريمة التامة ، رغبة منه في حماية المصالح المعتدى عليها (م١٩ العقوبات الفرنسي ، ١٩٨٨) ، وهناك من شرع للمحاولة نصف عقوبة الجريمة التامة (فلسطين) .

- **والمحاولة فى الجريمة الإلكترونية ، إما :**

- **محاولة ناقصة** : كاقتحام نظام بنكي لسرقة بيانات ومعلومات تخص حسابات بنكية ولكن تبوء المحاولة بالفشل بسبب قوة نظام الحماية الأمني لشبكة البنك.

(١) العجمي ،عبد الله دغش ، (٢٠١٤) ، مرجع سابق، ص ٣٠

- أو محاولة تامة : كاقتحام الجاني لنظام بنكي بهدف سرقة حسابات العملاء ، وبعد الانتهاء من العملية يكتشف أنه سرق بيانات لا علاقة لها بحسابات العملاء فيفشل في الوصول لمراده الجنائي.
- أما العدول عن المحاولة إراديًا : فليس محلاً للعقاب .

ويتحقق الشروع في الجرائم الإلكترونية بكل عمل يعتبر من شأنه تحضير وتجهيز لتنفيذ جريمة ذات طابع إلكتروني مثل : (تحضير الأجهزة والبرامج تمهيدًا لاختراق موقع معين ، كتابة أخبار مغلوطة تمهيداً لنشرها ، كتابة رسائل تمهيداً لإرسالها بهدف الذم او الابتزاز .... الخ) [١]

المطلب الثاني

المسئولية الجنائية للجرائم المعلوماتية

تتحقق المسؤولية الجنائية بتوفر ركنان أساسيان: الأول : هو الرابط المادي بين الواقعة والنشاط ، والثاني : هو الرابط المعنوي بين الشخص و السلوك ، ولكي تتحقق المسئولية الجنائية في الجرائم الإلكترونية لابد من وجود مصلحة جديرة بالحماية جنائياً . [٢]

(١) العفيفي ، يوسف خليل يوسف. (٢٠١٣) ، مرجع سالف الذكر ص٦٦

(٢) ربايعة ، عبد اللطيف محمود .(٢٠١٦) . " الجرائم الإلكترونية – التجريم والملاحقة والإثبات " ورقة عمل مقدمة إلى المؤتمر الأول للجرائم الإلكترونية في فلسطين ، جامعة النجاح الوطنية ، نابلس ١٧ إبريل ٢٠١٦ ، ص ص ٩ ، ١٠

وتتحقق الحماية المعلوماتية في إطار مجموعة من القواعد القانونية تقرر الحقوق والإلتزامات لكل أفراد المجتمع فيما يتعلق بسلامة استخدام شبكات وأنظمة وتقنيات المعلومات [١] ، ومن ثم إقرار تجريم لكل فعل أو امتناع عن فعل يمكن اعتباره اعتداء على الحقوق المعلوماتية الخاصة أو الرسمية ، مع إقرار العقوبات المناسبة والمتناسبة لحجم الفعل المُرتكب ودرجة خطورته .

وتتعدد وسائل وأهداف ارتكاب تلك الجرائم ، كما تتعدد الأفعال التي تصلح أن ترتكب عن طريق الحاسب والإنترنت (التجسس والاختراق غير المشروع - سرقة الأرصدة البنكية ، تدمير البيانات والأجهزة عن بُعد ، النصب والاحتيال ، السب والقذف ، التشهير ، تزوير البيانات أو اتلافها عمدياً ، التحريض ، نشر الصور الإباحية ، دعارة الأطفال ، النسخ غير المشروع – القرصنة - الاعتداء على حقوق الطبع والنشر والمؤلف ... الخ. [٢]

والقاعدة العامة : أن المسئولية الجنائية شخصية ، تتحقق في مواجهة شخص طبيعي ، ومن ثم لا يُسأل إنسان إلا عن عمل أو سلوك ارتكبه غير مشروع فقط ، بينما في الجرائم الإلكترونية اتسع الأمر ليشمل المسئولية الجنائية المفترضة. [٣]

---

(١) أيوب ، برلين .(٢٠٠٩) ، " الحماية القانونية للحياة الشخصية في مجال المعلوماتية " ، منشورات الحلبي الحقوقية ، ط ١، بيروت ص ٤٥

(٢) عطا الله ، شيماء عبد الغني (٢٠٠٧) ، " الحماية الجنائية للتعاملات الإلكترونية " ، دار الجامعة الجديدة ، ص ٩٤

(٣) أخذ المشرع الليبي بالمسؤولية الجنائية المفترضة عن الغير في مجال النشر على أساس تضامني يتمثل في افتراض علم رئيس التحرير بالمضمون المنشور في الصحيفة واعتباره الفاعل الأصلي في الجرائم المُرتكبة بواسطة النشر وهي ما تسمى أيضاً بالمسؤولية المتتابعة . أنظر: حسين ، محمد عبد الطاهر. (٢٠٠٠) ، " المسئولية القانونية في مجال شبكات الإنترنت " ، دار النهضة العربية ، القاهرة ، ص ٣٨

وقد حثت معاهدة بودابست في (م١٢) الدول الأطراف على اتخاذ التدابير التشريعية اللازمة التي تمكن من مسائلة الأشخاص الاعتبارية ، التي ترتكب لمصلحتها جرائم إلكترونية ، بواسطة أي شخص طبيعي تحت سلطتها أو تابع لها.

فوفقًا للمادة سالفة الاشارة: كل شخص اعتباري يمارس نشاط إلكتروني وكان سبب مباشر أو غير مباشر في تحقق جريمة إلكترونية سببت ضرر للغير سواء كانوا أشخاص طبيعية أو اعتبارية ، فإنه يجوز مساءلته جنائياً عن الجريمة الإلكترونية التي تمت بل ومطالبته بالتعويض، ويترك الأمر لظروف كل جريمة إلكترونية على حده، مع الأخذ في الاعتبار مراعاة البُعد الدولي لتلك الجرائم . (١)

ويعرف الشخص الاعتباري / المعنوي في الجرائم الإلكترونية بأنه :هو كل شخص يكتسب صفة الاعتبارية وفقاً للقانون المنظم ويمارس نشاط إلكتروني من أي نوع ، ويشارك في ارتكاب جريمة إلكترونية أو أكثر لمرة واحدة أو بصفة اعتيادية ، إما بواسطة برامج إلكترونية مصنعة بواسطته أو عن طريقه أو لصالحه تستخدم في تلك الأعمال المجرمة ، أو من خلال أشخاص طبيعيين يعملون لصالحه ويرتكبون الجرائم الإلكترونية وفقاً لأوامر صادرة منه ، وعليه من الممكن أن يكون هذا الشخص الاعتباري. (٢)

- مزود الخدمة ISP　　- المستضيف لصفحات الـ WEB

(١) أحمد ، هلالي عبد اللاه .(٢٠٠٧) ، " اتفاقية بودابست لمكافحة جرائم المعلوماتية - معلقًا عليها " ، دار النهضة العربية، الطبعة الأولى ، القاهرة ، ص٤٧ وما بعدها.

(٢) الكثيري ، متعب بن هتدي بن حمد .(٢٠١٩) ، " المسئولية الجنائية للشخص المعنوي عن جرائم المعلوماتية في النظام السعودي : دراسة مقارنة بالقانون المصري ، رسالة ماجستير ، جامعة نايف العربية للعلوم الأمنية ، كلية العدالة الجنائية ، قسم الشريعة والقانون..

- أحد الشركات التي تمتلك أشهر تطبيقات التواصل الاجتماعي ، أمثال فيس بوك ، تويتر، واتس اب .

و من جانبنا نرى أنه وفقاً لحرفية نص المادة (١٢) من اتفاقية بودابست فكل شخص اعتباري يمارس نشاط إلكتروني وكان سبب مباشر أو غير مباشر في تحقق جريمة إلكترونية سببت ضرر للغير سواء كانوا أشخاص طبيعية أو اعتبارية أخرى ، فإنه يجوز مساءلته جنائياً عن الجريمة الإلكترونية المُرتكبة بل ومطالبته بالتعويض، ويترك الأمر لظروف كل جريمة على حده ، مع مراعاة البُعد الدولي لتلك الجرائم.

المبحث الرابع

التحديات الموضوعية والإجرائية المتعلقة بالجرائم الإلكترونية

تثير الجرائم الإلكترونية مجموعة من الإشكاليات ، فقد يقوم مجرم معلوماتي يحمل الجنسية الصينية بعمل فعل غير مشروع على أرض تايلاند ، مستهدفًا حساب بنكي يخص مليادير هندي بأحد فروع بنك في بريطانيا ، باستخدام خادم / Serverأمريكي .

فكيف يمكن معرفة وقت حدوث الجريمة هل هو توقيت بلد المجرم أم توقيت بلد البنك المسروق أم توقيت الخادم المستخدم؟ وما هو القانون الواجب التطبيق في هذا الشأن ؟ هذا بخلاف ما ستثيره هذه الجريمة العابرة للحدود للعديد من التحديات من الناحية الموضوعية والإجرائية .

المطلب الأول

التحديات الموضوعية

تثير الجرائم الإلكترونية والمعلوماتية مجموعة من المشكلات عند تطبيق النصوص القانونية عليها ، إما لعدم مطابقة النصوص الجنائية التقليدية ، أو لعدم وجود نصوص خاصة بمكافحة تلك الجرائم ، ومن أكثر الجرائم الإلكترونية إثارة

للمشكلات: جرائم الاعتداء على الحياة الخاصة ، والاعتداء على الأموال و التزوير الإلكتروني ، وجرائم سرقة المال المعلوماتي [١]

الفرع الأول

المشكلات المتعلقة بجرائم الاعتداء على الحياة الخاصة للأفراد

اصبحت الشبكات المعلوماتية في الآونة الأخيرة مستودعًا خطيرًا للكثير من الأسرار الخاصة للإنسان التي يمكن الوصول إليها بسهولة وسرعة ويُسر من خلال الوصول إلى البيانات الخاصة للمستخدم عن طريق زيارة بعض المواقع التي تعمل من خلال بروتوكول HITP والذي يساهم في نقل المعلومات الخاصة كـ (رقم جهاز الحاسب الشخصي IP ومكانه وبريده الإلكتروني) بين الأجهزة .

و هناك بعض المواقع التي يؤدي الاشتراك فيها الى وضع ملفات Cookies على القرص الصلب للحاسب الشخصي بشكل تلقائي بهدف جمع معلومات عن المستخدمين ،والخطورة في استخدام شبكة الإنترنت تكمن في إن ما يكتبه الشخص من رسائل يحفظ في أرشيف خاص يسمح بالرجوع إليه ولو بعد عشرون عامًا . [٢]

ويعتقد الكثيرون أن الدخول باسم مستعار أو بعنوان بريدي زائف لساحات الحوار ومجموعات المناقشة قد يحميهم ويخفي هويتهم، إلا إن مزود الخدمة أو

(١) حجازي ، عبد الفتاح بيومي حجازي (٢٠٠٧) . " صراع الكمبيوتر والإنترنت – في القانون العربي النموذجي " ، دار الفكر الجامعي ، القاهرة ، ص ٦٠٩.

(٢) لبشير ، سيدي محمد .(٢٠١٠) ، " دور الدليل الرقمي في إثبات الجرائم المعلوماتية، دراسة تحليلية تطبيقية " ،رسالة ماجستير في العلوم الشرطية تخصص التحقيق والبحث الجنائي، كلية الدراسات . العليا ،جامعة نايف العربية للعلوم الأمنية، الرياض،. ص ٧٣ .

(ISP)Internet Service Provider يمكنه الوصول إلى كل هذه المعلومات بل و معرفه المواقع التي يزورها العميل.

لذلك اهتمت كثير من القوانين الوطنية بهذه الاشكالية واتجهت إلى تبني العديد من الضمانات لحماية المعلومات الخاصة و التى يمكن تلخيصها فى الآتى:

١- ضرورة الأخطار العام : وفرض قيود على إنشاء أي نظام معلوماتي يتعلق بمعالجة البيانات.

٢- على الجهة الراغبة في إقامة أي نظام معلوماتي أن تحدد الهدف من إقامته، حتى يتم التأكد من أنه ليس تطفل لسرقة المعلومات الخاصة . (١)

٣- منع تسجيل أي معلومة إلا برضاء صاحب الشأن(م٢٥ من قانون المعلوماتية الفرنسي).

وقد أصدرت المملكة العربية السعودية مؤخراً في (سبتمبر ٢٠٢١) نظاماً خاصاً بحماية البيانات الشخصية يهدف إلى حماية الخصوصية الفردية من خلال تنظيم عملية جمع البيانات الشخصية ومعالجتها والإفصاح عنها والاحتفاظ بها، من خلال معايير خاصة لمعالجة البيانات، و بيان حقوق أصحابها، وتحديد التزامات الهيئات المعنيّة عند معالجة البيانات الشخصية، والسيادة على البيانات، و عقوبات رادعة في حالات عدم الامتثال، بخلاف الحماية التي تقررها المادة الثالثة من نظام مكافحة الجرائم المعلوماتية ٢٠٠٧م .

وفي رأينا أن هناك صورة مستحدثة لجرائم الاعتداء على حرمة الحياة الخاصة للفرد أو للمجتمع ، يجب التصدي لها وهي جريمة التربح

(١) حجازي ، عبد الفتاح بيومي حجازي (٢٠٠٧) . مرجع سابق ص ٦٢٠.

الأولى (الـ TREND [١] حديث الساعة) هذا السلاح الإلكتروني الذي يستهدف ترويج أكاذيب أو ادعاءات مزعجة أومدمرة للأفراد طبيعية كانت أو اعتبارية ، أو ترويج وبث عادات شاذة عن المجتمع بهدف ضرب القيم المجتمعية ، بهدف التربح عن طريق جذب أعلى نسبة المشاهدات.

الفرع الثاني

المشكلات المتعلقة بجرائم الاعتداء على الأموال

من أمثلة الجرائم الإلكترونية التي تمثل اعتداء على الأموال :

١. تحويل الأموال غير المشروع بوسائل إلكترونية احترافية . [٢]

٢. استخدام برامج متخصصة لتسهيل أعمال الاختلاس : كتصميم برامج تستهدف إجراء عمليات التحويل الآلي بين الحسابات المصرفية وفي وقت يتحكم فيه مصمم البرنامج .

---

(١) الترند : يقصد به الأمر الرائج والمنتشر بشكل عام عبر مواقع التواصل ، وعادة ما تكون أنباء ساخنة عاجلة تجذب اهتمام رواد مواقع التواصل االجتماعي، الذين هم صناع المحتوى بمختلف أشكاله، ويكون أهتمامهم موجه تجاه التفاعل مع الترندات ويعبرون عن رأيهم تجاهها أو يعلقون بطريقتهم الخاصة، فالبعض ممن يريدون الشهرة يحاولون مواكبة التريند ويتحدثون عنه ليضمنوا زيادة مشاهدتهم بكثرة ويصلوا لأكبر عدد ممكن من الأشخاص إذا لقي حديثهم وطريقتهم إستحسان من الغالبية.

(٢) وأشهر هذه الوقائع قيام أحد العاملين بمركز الحاسبات المتعاقد مع مصرف الكويت التجاري لتطوير أنظمة المعلومات بالاستيلاء على مبالغ طائلة من المصرف بعد أن تمكن من اختيار خمسة حسابات راكدة في خمس فروع محليه للمصرف واعد لها برنامجا تمثلت مهمته في تحويل مبالغ معينة من هذه الحسابات التي حسابات أخرى فتحت باسمه في الفروع نفسها على أن تتم عملية التحويل أثناء وجوده بالطائرة في طريقة إلى المملكة المتحدة عائدا إلى بلاده بعد انتهاء عقد عمله ، ثم فتح حسابات أخرى فور وصوله وطلب من المصرف تحويل هذه المبالغ إلى حساباته الجديدة في بريطانيا.

١- استخدام برامج إلكترونية لخصم (الكسور العشرية) من أرصدة العملاء بالبنوك وتحويلها لحساب خاص بالجاني ، وهي عملية يصعب الانتباه إليها لضئالة المبالغ المسحوبة.

٢- تحويل أرصدة من حسابات العملاء مباشرة من خلال برامج تخترق شفرات الحسابات البنكية أو اختراق كروت الائتمان المتصلة بشبكة الـ (wifi (وقد عالجت المادة (٥) من اتفاقية بودابست هذه الاشكالية. (١)

٣- اختراق المواقع التجارية الخاصة بالتسوق الإلكتروني المسجل عليها بيانات بطاقات العملاء الإئتمانية و استخدام تلك البطاقات في خصم مشتريات لحساب الجاني المخترق .

٤- جرائم الاعتداء على أجهزة الصراف الآلي للنقود وسحب أموال منها بطرق احتيالية.(٢)

٥- جرائم الاستيلاء على النقود الإلكترونية cash-e : وهي نقود رقمية ذات قيمة نقدية مدفوعة مقدماً ، مخزنة على وسيلة إلكترونية مثل :

- عملات الألعاب الافتراضية المستخدمة عبر منصات الألعاب الإلكترونية الشائعة.

- والعملات الافتراضية ذات القيمة السوقية مثل (بيتكوين) .

---

(١) أشهرها قيام أحد خبراء الحاسب الآلي في الولايات المتحدة باختزاق النظام المعلوماتي لأحد المصارف وقيامه بتحويل ١٢ مليون دولار إلى حسابه الخاص في ثلاث دقائق فقط.

(٢) العجمي ،عبد الله دغش ، (٢٠١٤) ، مرجع سابق، ص ٥٢

- **الحماية الجنائية للأموال في مواجهة التحايل الإلكتروني Computer related frau:**

- يعاقب أي يقوم بتعديل أو محو أو إيقاف أي بيانات مخزنة في أي نظام إلكتروني معلوماتي، بهدف الإضرار بالغير (م/٨ بودابست،٢٠٠١).

- يعاقب كل من استخدم بطاقة ائتمانية للسحب الإلكتروني الاحتيالي أو استخدم بطاقة مسروقة أو استحوذ عليها بدون وجه حق لاستخدامها في سحب شراء مع العلم بذلك. (م/٦ القانون ع النموذجي ، ٢٠٠٣) ، وعلى ذات النهج نصت المواد (١٦و١٧) ، من وثيقة الرياض لنظام القانون الموحد لمكافحة جرائم التقنية بدول مجلس التعاون الخليجي ٢٠١٣.

الفرع الثالث

المشكلات المتعلقة بجريمة التزوير

جريمة التزوير من الجرائم التي لا تتخذ شكل معين للسلوك الإجرامي ، وعادةً ما يكون محلها تزوير محرر أو مستند أو وثيقة محمية بموجب القانون باعتبارها وسيلة للإثبات يترتب عليها آثار قانونية.

وتعد المملكة الأردنية من أولى الدول العربية التي اعترفت بحجية المستندات الإلكترونية في الإثبات و محلاً لجريمة التزوير منذ أن نصت في قانون الأوراق المالية ٢٣ / ١٩٩٧ اعتبار القيود المدونة في سجلات البورصة يدوياً أو إلكترونيا دليلاً على تداول الأوراق (م/٢٤).

إلى أن بدأت التشريعات الحديثة تجيز اتخاذ أي من الوسائل الإلكترونية طرقاً للإخطار أو الإثبات ، وهو ما يشير بالتبعية إلى إمكانية الاتفاق على الإثبات بالوسائل

الإلكترونيـة تماشـياً مـع عـصر الوثـائق الإلكترونيـة [١] ، ومـن أمثلـة تجـريم تزويـر المستندات الإلكترونية:

- يعاقب كل من ارتكب فعل من شأنه تزوير المستندات المعلوماتية أيا كان شكلها بأي طريقة تحدث الضرر بالغير (م ٥/٤٦٢ عقوبات فرنسي) ، حتى لو ارتكبت جريمة التزوير بطريق الخطأ.
- يعاقب كل من استخدم مستندات معلوماتية مزورة وهو على علم بذلك. (م /٦ الفرنسي)
- يجرم أي تغيير مقصود ببيانات مخزنة في أي نظام معلوماتي يؤدي إلى إنتاج بيانات غير حقيقية بغرض استعمالها لأغراض قانونية على أنها صحيحة .(م/٧ بودابست ، ٢٠٠١)
- يعاقب بالسجن كل من قام بدخول غير مشروع لإلغاء بيانات خاصة، أو حذفها، أو تدميرها، أو تسريبها، أو إتلافها أو تغييرها، أو إعادة نشرها. (م/٥ السعودي ، ٢٠٠٧)

وعليه بات الاعتراف بحجية المستندات الإلكترونية في الإثبات أمراً معترف به دولياً ، ويحظى بالحماية الجنائية اللازمة. [٢]

(١) المرجع السابق، ص ٥٢

(٢) عبد المطلب ، ممدوح عبد الحميد. (٢٠٠٦) ."البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت"، دار الكتب القانونية ، القاهرة. ص ٨٨

الفرع الرابع

المشكلات المتعلقة بجريمة سرقة المال المعلوماتي

تثور المشكلات حول سرقة المال المعلوماتي عندما تتم بطريقة القرصنة بغرض الاستيلاء على معلومات مخزنة داخل جهاز إلكتروني بطريقة غير مشروعة ، فالإشكالية هنا تتمثل في مدى اعتبار المعلومات من الأموال التي يمكن سرقتها ؟

وهنا يرى البعض صعوبة تطبيق النصوص القانونية التقليدية للسرقة على حالة سرقة المعلومات إلكترونيا وذلك لسببين [١] : الأول : انتفاء الركن المادي لجريمة السرقة في هذه الحالة لكون السارق استحوذ فقط على المعلومات باستنساخها ولم تخرج من حيازة المالك ، والثاني: السرقة في هذه الحالة لم تقع على مال منقول له كيان مادي .

و رغم ذلك ، نجد المشرع الفرنسي لم يضع نص خاص لجريمة سرقة المعلومات (م٣٢٣) ، لذا يفهم ضمنياً سريان القواعد العامة للسرقة على سرقة المعلومات ، بينما في الولايات المتحدة الأمريكية ، يعاقب القانون الفيدرالي الصادر في هذا الشأن ١٩٨٤ على الوصول غير المرخص للمعلومات ، وتوسع القانون ليشمل جريمة سرقة المال المعلوماتي (إتلاف المعلومات والاعتداء على برامج الحاسب بأي وسيلة كانت) . [٢]

---

(١) العجمي ،عبد الله دغش ، (٢٠١٤) ، مرجع سابق، ص ٦٢

(٢) وهو ما حدث في جامعة مونماوث في الولايات المتحدة الأمريكية حيث استهدفت قنبلة إلكترونية نظام البريد الإلكتروني الذي ترتبط به أعمال وأنشطة على درجة عالية من الأهمية للجامعة (كالتسجيل – وتبادل الأبحاث – ودفع الرسوم) ، وقدرت الخسائر بعشرات الآلاف من الدولارات، =

وفي النظام السعودي م/٥ : لم يرد تجريم سرقة المال المعلوماتي صراحة ، على اعتبار أن التصرف في البيانات الخاصة للغير من خلال دخول غير مصرح به يُعد في حكم السرقة بصرف النظرعن توفر قصد جنائي لدى المُتهم أم لا.

المطلب الثاني

التحديات الإجرائية

يُعتبر مسرح الجريمة أهم عناصر الجريمة ، وهو العنصر الرئيسي لضبط وتحري الجريمة وملاحقة مُرتكبيها ، و تتميز الجريمة الإلكترونية بأنها تُرتكب في مسرح إلكتروني فضائي يختلف كلياً عن مسرح الجريمة التقليدية ، الأمر الذي يثير العديد من التحديات الإجرائية والصعوبات و العقبات القانونية من حيث : ضبط الجريمة و إثباتها و جمع الادلة والتفتيش والملاحقة الأمنية و القانون الواجب التطبيق ، و من ثم الاختصاص القضائي المرتبط ارتباط وثيق بسيادة الدولة ومبدأ الإقليمية.... الخ.

=

واستطاع فريق تحقيق فيدرالي من تحديد اليوم والساعة وعنوان الكمبيوتر المستخدم في الجريمة، واعترف المُتهم وحاول تبرير فعله بأنه فعل غير مقصود إلا أن المحكمة اعتبرته مذنباً وحكم عليه بالسجن ثلاث سنوات وغرامة مالية قدرها مائة ألف دولار. انظر: الشوا ، محمد سامي. (١٩٩٤). ثورة المعلومات وانعكاساتها على قانون العقوبات ، دار النهضة العربية ، القاهرة. ص ١٩٤

الفرع الأول

المشكلات المتعلقة بحجية الدليل الرقمي في الإثبات

عادة ما يتعلق السلوك الإجرامي بأكثر من دولة في الجرائم الإلكترونية (دولة ارتكاب السلوك ، الدولة التي ضبطت الجاني ، دولة النتيجة الإجرامية ، ودولة جنسية المجرم المعلوماتي).

وتعتبر الشبكة العنكبوتية مسرحاً للجريمة الإلكترونية ، من الممكن ضبط الجاني بها من خلال تتبع عنوانه الإلكتروني الـ IP ، أو تحديد نوع الجهاز الذي يستخدمه والمكان الذي يدخل منه ، ودائما ما تُثار الصعوبات أمام المجرمين المتخصصين ذو القدرات الفائقة في التقنية مثل الكراكز ، فيصعب اكتشافهم نتيجة لكونهم يقومون بمحو آثارهم التي تم تسجيلها من خلال مسح ملفات الكوكيز cookies [1] وكذلك إخفاء عناوين أجهزتهم الإلكترونية.

يعتمد ضبط الجريمة وإثباتها على جمع أدلة الإثبات المعترف بحجيتها القانونية من خلال مجموعة من الوسائل والإجراءات الرئيسية والتي تتمثل في :(المعاينة – التفتيش – الخبرة – ضبط الأشياء محل الجريمة) ، تليها طرق أخرى يتم اللجوء إليها في مراحل تحقيق لاحقة مثل (الاستجواب –المواجهة – سماع الشهود) .

(١) الكوكيز: هي عبارة عن ملفات نصية، تودعها المواقع التي تتم زيارتها على القرص الصلب في الجهاز، بحيث تحتوي هذه الملفات على مجموعة من المعلومات التي تتيح للموقع استعادتها عند الحاجة، تحديداً عند الزيارة المقبلة لهذا الموقع.

*** مدى حجية الدليل الرقمي في الإثبات الجنائي ؟**

الدليل الرقمي : هو دليل إلكتروني على شكل نبضات مغناطيسية أو كهربائية، يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات خاصة، وللقاضي الجنائي مطلق الحرية في تقدير الدليل المقدم له وله الأخذ به أو لا. (١)

وتتعدد أنواع المخرجات الإلكترونية ، فقد تكون ورقية - Electronic receipt ، أو غير ورقية في صورة معلومات مسجلة على الشبكة أو على أقراص مرنة Floppy Disk ، أو صلبة Hard Disk ، ويصعب في المحررات الإلكترونية التمييز بين أصلها ونسخها .

*** أشكال الدليل الرقمي:**

١ - أدلة رقمية خاصة بأجهزة الحاسب .

٢ - أدلة رقمية خاصة بشبكة "الإنترنت".

٣ - أدلة خاصة ببروتوكولات تبادل ونقل المعلومات (TPC /IP /HTTP).

٤ - قسمت وزارة العدل الأمريكية ٢٠٠٢ الدليل الرقمي إلى :

- السجلات المحفوظة في الحاسب الآلي ، كالبريد الإلكتروني ، وملفات معالجة الكلمات Winword .

- السجلات التي تم إنشاؤها وإعدادها بواسطة الحاسب،مثل files.

---

(١) عبد المطلب ، ممدوح عبد الحميد (٢٠٠٦) ، مرجع سابق ، ص ٨٩.

- السجلات التي تم حفظ جزء منها بالإدخال وجزء تم إنشاؤه عن طريق الحاسب الآلي، مثل Excel. [1]

* خصائص الدليل الرقمي:

١- دليل يتكون من بيانات ومعلومات إلكترونية غير مرئية يتطلب الوصول إليها استخدام الحاسب الآلي كـ Hardware واستعمال برامج Software معينة.

٣- دليل علمي، يتطلب وجوده توافر مجال تقني للتعامل معه.

٤- دليل ذو طبيعة خاصة من التقنية يتكون من نبضات رقمية .

٥- يصعب التخلص منه ، ولكن من السهل تغيير تكوينه .

٦- محو أو إزالة الدليل الرقمي من الحاسب - يعتبر دليل إدانة في حد ذاته في مواجهة المجرم المعلوماتي، لكون عملية المحو يتم تسجيلها بالحاسب، ومن ثم يمكن تحويله كدليل للإدانة.

٧- تمتاز بعض الأدلة الرقمية بسعة تخزينية عالية.

٨- مصطلح الدليل الرقمي مصطلح شامل يتضمن كافة الأشكال المتوفرة حالياً والتي قد تتوفر في المستقبل.

* من أمثلة الدليل الرقمي :

- ورق الطباعة من الحاسب.

---

(١) فرغلي ، عبد الناصر محمد محمود ، المسماري ، محمد عبيد سيف سعيد .(٢٠٠٧) . "الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية"، دراسة تطبيقية مقارنة، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية، الرياض، ص.١٥

- الأجهزة الإلكترونية مثل (الهاتف النقال – الحاسبات – الموديوم) .
- وسائل التخزين (الثابتة – المدمجة CD الفلاش USB الأشرطة الممغنطة ...).
- برامج نظم التشغيل .
- بروتوكولات الإنترنت (TPC /IP).

* من شروط حجية الدليل الرقمي في الإثبات :

١. يجب أن يكون الدليل الإلكتروني يقيني غير قابل للظن أو الترجيح .[١]

٢. التأكد من سلامة الدليل الإلكتروني المقدم من العبث به ، ويستطيع الخبير التقني وجهات التحقيق المدربة من إدراك حقيقة كون الدليل سليم أم لا من خلال التناظر بين الدليل المقدم بالأصل المدرج بالآلة الرقمية – أو من خلال عمليات حسابية خاصة تسمى الخوارزمات – أو مقارنته بدليل محايد (دليل مثل) للتأكد من مطابقة الدليل المقدم للمواصفات.

٣. مناقشة الدليل الإلكتروني علنياً للتحقق من سلامته ، وهنا تثور المشكلة بالنسبة لقاضي التحقيق لكون تلك الأدلة غير مرئية ، لا يمكن قراءتها أو استخراجها إلا باستعمال أجهزة إلكترونية ، والأمر وارد للتلاعب بالمعلومات المسجلة بمسحها أو استبدالها.

ومن ناحية أخرى ، يتطلب مواجهة الجرائم الإلكترونية وجود نظام قانوني متكامل يحدد آليات ضبط المعاملات و التجارة الإلكترونية وإضفاء الحجية القانونية

(١) حطب ، ياسر محمد الكومي. (٢٠١٤) . الحماية الجنائية والأمنية للتوقيع الإلكتروني ، منشأة المعارف، الإسكندرية ، ص ٣٠٥

على المستندات الإلكترونية شأنها شأن المستندات الورقية ، حتى يتاح للقاضي الجنائي الاعتماد عليها و اتخاذها دليلاً جنائياً ، كغيره من الأدلة. (١)

الفرع الثاني

المشكلات المتعلقة بالتفتيش والمعاينة والخبرة

حثت اتفاقية بودابست م(٢٣) على تعاون الدول الأطراف في المسائل الجنائية على أوسع نطاق فيما يخص إجراءات التحقيق والمتابعة و جمع الأدلة الخاصة بالجرائم الإلكترونية .

و تعتبر إجراءات التحقيق كالتفتيش والخبرة والمعاينة ، من أكبر التحديات التي تواجه عملية الإثبات في الجرائم الإلكترونية .

أولاً: التفتيش في البيئة الإلكترونية:

التفتيش : هو البحث عن أشياء تفيد الكشف عن الحقائق في جريمة ما ، ويجوز أن يكون محله منزل أو مكتب أو مقر للمجرم ، أو شخص المجرم ذاته .

و التفتيش في البيئة الإلكترونية : ينصب على جهاز الحاسب الآلي المتصل بالشبكة المعلوماتية المخصص لاستقبال البيانات وتخزينها أو إعادة إرسالها، ومعالجة واستخراج النتائج المطلوبة .

---

(١) ومن القوانين التي منحت المستند الإلكتروني حجية في الإثبات مثلها مثل المحرر الورقي: قانون التجارة و المعاملات الإلكترونية التونسي سنة ٢٠٠٠ ، وكذلك قانون إمارة دبي للتجارة الإلكترونية سنة ٢٠٠٢ ، وقانون نظم التوقيع الإلكتروني المصري سنة ٢٠٠٤ ، و القانون العربي النموذجي ٢٠٠٣ ، وأيضاً لجنة الأمم المتحدة للقانون التجاري الدولي United Nation (Commission on International Trade Law (UNCITRAL سنة ٢٠٠٠ .

يخضع التفتيش في إجراءاته للضوابط التي يحددها قانون الإجراءات الجنائية المختص وما إذا كان الفعل المُرتكب محل حماية جنائية من عدمه ، ولتحقيق الغاية من التفتيش لابد من وجود دلائل أو قرائن في أجهزة الحاسب الآلي وملحقاته المادية أو المعنوية خاصة بمُرتكب الجريمة ، تفيد في كشف الادلة والحقائق ، وما يحتمل أن يكون قد استعمل في ارتكابها أو نتج عنها أو وقعت عليه. (١).

وقد ثار جدل فقهي حول مدى إمكانية تفتيش وضبط البيانات المخزنة أو المعالجة إلكترونياً وانقسموا في ذلك لاتجاهين :

- الاتجاه الأول : (الفرنسي)، و يميل إلى عدم صلاحية إجراء التفتيش والضبط على برامج وبيانات الحاسب الآلي باعتباره وسيلة للإثبات المادي . (٢)
- والاتجاه الثاني : يرى أن المعلومات ذات الطبيعة المعنوية رغم كونها مجرد نبضات إلكترونية ، إلا أنها قابلة للتخزين -على CD مثلاً - وبالتالي فهي ليست شيئًا معنويًا كالحقوق والآراء والأفكار بل أشياء لها وجود ملموس في العالم الخارجي ، ومن ثم يصح أن يرد عليها التفتيش والضبط .

ومن ثم يتم التفتيش على المكونات المعنوية باعتبارها محتوى لمعلومات وبيانات وحوار وكلمات سر يمكن تصفحها وتحليلها لاستظهار الدليل المعلوماتي ، وفي حالة الاتصال بشبكات معلومات دولية ، واستخدام أنظمة تقنية خارج إقليم الدولة المتواجدين على إقليمها لارتكاب الجريمة ، هنا : لا يجوز لسلطات تحقيق الدولة التي

(١) بكري ، بكري يوسف .(٢٠١٠)، " التفتيش عن المعلومات في وسائل التقنية الحديثة " ، دار الفكر الجامعي، الإسكندرية، ص ص ٦٧-٨٠

(٢) حجازي ، عبد الفتاح بيومي حجازي (٢٠٠٧) . مرجع سابق ذكره ص ٣٨٠.

ارتكبت الجريمة على إقليمها ، أو أضرت بأحد رعاياها أو بمصالحها الأساسية أن تباشر التفتيش أو غيره من إجراءات التحقيق خارج حدودها الإقليمية [١] .

ولا يفترض أن يكون الأمر بالتفتيش عاماً ، وإنما يجب أن يكون محدد الهدف منه تحديدًا دقيقًا ، وأن يتم وصف الأشياء المطلوب ضبطها بصورة تفصيلية ، دون إطلاق يد السلطة التقديرية لرجل الشرطة الذي سيقوم بتنفيذه ، ويلزم أن يكون عضو جهة التحقيق ملمّاً بالجوانب الفنية للحاسب واستخداماته حتى لا تكون القرارات القضائية في يد البعض وسيلة لاصطناع الأدلة أو التسلط أوالاستبداد ، إذ يمكن عن طريق الوسائل العلمية والتقنية الحديثة العبث بالبيانات الموجودة على الحاسب ومحوها [٢] .

(١) وفى هذا الشأن قضت إحدي المحاكم الألمانية في جريمة غش ارتكبت في ألمانيا بأن الحصول على البيانات الخاصة بهذه الجريمة والمخزنة بشبكات اتصال موجودة في سويسرا لا يتحقق إلا بطلب المساعدة من الحكومة السويسرية ، وفى واقعة نشر فيروس(Love bug) عام ٢٠٠٠ الذي تسبب في إتلاف المعلومات في أجهزة الحاسب الآلي، فعندما اكتشف الخبراء الأمريكيون بان هذا الفيروس أرسل من الفليبين فإن تفتيش منزل المشتبه فيه تقتضي تعاون السلطات الفليبينية والحصول على إذن من قاضي التحقيق بالفليبين.

(٢) أصدر القضاء الأمريكي حكماً بتعويض شركة ستيف جاكسون التي تقوم بأعمال النشر ، وكانت تصدر جريدة إلكترونية وتخضع للحماية المقررة بموجب قانون حماية الخصوصية وقانون حماية الاتصالات الإلكترونية ، اللذان لا يجيزان القبض والتفتيش في حق السري الأمريكي بتفتيش الشركة وضبط أجهزة للحاسب الآلي وملحقاتها ومجموعة من البرامج وطابعات ليزر وكمية من الأسطوانات وملفات خاصة بجريدة إلكترونية ، وكذلك آلة حاسبة شخصية ، ووضعت الأختام على المضبوطات فترتب على هذا الإجراء تعرض الشركة لأزمة مالية كبيرة في الوقت الذي لم توجه أية تهمة لصاحب الشركة أو لأي من العاملين معه ، بل في النهاية تبين أن التفتيش لم يكن متعلقًا به أو بعمله ، وأن أحد العاملين بالشركة - والذي لم توجه له تهمة - كان الهدف من الإجراء ، وكانت المعلومات المطلوب ضبطها موجودة بمنزله ، المطردي ، مفتاح بو بكر . (٢٠١٢) ، مرجع سابق.

ومن جانبنا نرى جواز أن يتضمن التفتيش في الجرائم الإلكترونية كل ما يتعلق بالمحل الإلكتروني للجريمة ، ويختلف الأمر فقط حسب درجة استعداد وتطور جهات التحقيق لاستيعاب هذا النوع من الجرائم، وعليه يتصور بالنسبة لنا:

- تفتيش المكونات المادية للأجهزة المستخدمة في الجريمة.
- تفتيش البرامج وقواعد التشغيل البيانات التي ساعدت على فك الشفرات.
- وقد يصل الأمر إلى تفتيش شبكات المعلومات المتصلة بالحاسب الآلي لمعرفة هل كانت تسمح بالولوج للمواقع التي تم اختراقها من عدمه ، أم تم استخدام سيرفر Server بدولة أخرى للتمكن من هذا الأمر.

وقد نصت بودابست م ٣٢ : على امكانية الدخول بغرض التفتيش والضبط لأجهزة حاسب أو شبكات تتبع دولة أخرى بدون إذنها في حالتين: الأولى إذا تعلق التفتيش بمعلومات متاحة للعامة ، والثانية إذا رضى المالك حائز هذه البيانات بهذا التفتيش.

و لصحة إجراء التفتيش وتوافقه مع إجراءات التحقيق الجنائى الوطنية عدد من متطلبات:

١. أن يكون التفتيش بسبب وقوع جريمة قانونية تحمل وصف جناية أو جنحة.
٢. وجود اتهام لشخص أو أكثر بالمساهمة في تلك الجريمة الإلكترونية.
٣. وجود أدلة مادية قوية تفيد في كشف الجريمة.
٤. أن تقوم به السلطة المختصة بالتحقيق الجنائي في حضور الشخص صاحب المحل موضوع التفتيش (نظام الاجراءات الجزائية السعودي م ٤٦) ، فيجب أن يُحاط بضمانات حتى لا يتحول لتعدي على الحياة الخاصة .

٥. تحرير محضر بالتفتيش لكونه عمل من أعمال التحقيق فيتطلب إثبات ما تم فيه من إجراءات ونتائج.

٦. أخذ كافة الضمانات التي تضمن سلامة البيانات محل التفتيش وعدم تعرضها للتلف ، وأولها أن يتم من خلال سلطات تحقيق على دراية بالوسائل المادية والإلكترونية محل التفتيش في تلك الجرائم.

ثانياً: المعاينة الإلكترونية:

عرف الدكتور فتحي سرور عملية المعاينة بأنها : " إثبات مباشر ومادي لحالة شيء أو شخص معين ويكون ذلك من خلال الرؤية أو الفحص المباشر للشيء أو الشخص بواسطة مباشر الإجراء " (١)

فالمعاينة : إجراء من إجراءات التحقيق تتم بتكليف رسمي من جهة التحقيق المختصة حيث ينتقل المحقق إلى مسرح الجريمة لمشاهدة آثارالجريمة بنفسه ، لرفع الآثار وجمع كل ما قد يفيد في كشف الحقيقة ، سواء تتعلق بأشخاص أو أشياء موجودة بمكان الجريمة ، وتخضع الأدلة الناتجة من المعاينة لتقدير القاضي . (٢)

وفي مجال الجرائم الإلكترونية : تتطلب المعاينة انتقال مُحقق متخصص في مجالات التقنية بتكليف رسمي للتفتيش عن البيانات و استخراج المعلومات وفحص الملفات والبرامج والمراسلات وفك وتتبع الشفرات والرموز ، وعمل كل ما من شأنها المساعدة في التحقيق .

---

(١) سرور ، أحمد فتحي. (١٩٨١) . الوسيط في قانون الإجراءات الجنائية ، دار النهضة العربية ، القاهرة .ص ٢٨٧

(٢) العازمي ، فهد عبد الله العبيد. (٢٠١٢). الإجراءات الجنائية المعلوماتية ، رسالة لنيل درجة درجة الدكتوراه في القانون، كلية الحقوق، جامعة القاهرة. ص ٢٦٦

*** هل تجوز المعاينة فى الفضاء الإلكترونى ؟؟**

يعتبر الفضاء السيبراني العقبة الأساسية أمام معاينة الجريمة الإلكترونية إلا أنه وبرغم كل الصعوبات يتعين قيام المعاينة الإلكترونية ، مع الأخذ في الاعتبار :

- **الانتقال المادي لمسرح الجريمة متى كان محل المعاينة مكونات مادية إلكترونية مستخدمة في الجريمة (كالأجهزة – والشبكات – والريسيرفات ... الخ) ومن ثم التحفظ على كل ما يُعد دليل مادي.**
- **وإذا وقعت الجريمة على معلومات ذات طبيعة إلكترونية ، هنا يكون الانتقال افتراضياً أو إلكترونياً ، بالولوج لمسرح الجريمة بواسطة شبكة الإنترنت لفحص مسار الإنترنت و فحص الخادم ... الخ.**

وهناك مجموعة من تدابير التحفظية على المحقق اتباعها كي تساعده في أداء مهمته على أكمل وجه ، منها:

- **التحري المسبق عن مسرح الجريمة وجمع المعلومات والبيانات حول نوع وعدد ومواقع الأجهزة التي تم استخدامها.**
- **توفير الوسائل والإمكانات اللازمة من أجهزة وبرامج وأدوات يمكن الاستعانة بها في الفحص والضبط ، وحفظ الأدلة.** [1]
- **التأكد من خلو محيط مسرح الجريمة الخارجي من أية مجالات مغناطيسية قد تتسبب في محو أو إتلاف البيانات المسجلة أو التشويش على عملية المعاينة ذاتها.**

---

(١) حطب ، ياسر محمد الكومي. (٢٠١٤) . مرجع سابق ، ص ٢٤٥

- تتبع أثر الاتصالات المرتبطة بأجهزة المجني عليه ، والوصول إلى الملفات التاريخية التي تبين لحظات الاتصالات (البداية والنهاية لتحديد ساعة التنفيذ)، و من أين صدرت تلك الاتصالات؟ ومن الذي قام بإجراؤها ، مع ضرورة الإلمام بالحالات التي تستوجب التحفظ على أجهزة الحاسب أو الاكتفاء بنسخ نسخة من المعلومات المتوفرة عليه ... الخ.

ومن المهم أن يكون المحقق المعاين لمسرح الجريمة الإلكترونية ملماً بمهارات عالية من التقنية ، مثل القدرة على استخدام برامج mpTime sta وهي البرامج التي يمكن عن طريقها تحديد الزمن الذي تم فيه السلوك الإجرامي، لأن ذلك لا يكون متاحاً في جميع الأنظمة المعلوماتية .

ثالثاً: الخبرة بالتقنية:

الخبرة : هي أحد أهم وسائل جمع الأدلة ، التي قد يلجأ إليها المُحقق عند وجود وقائع مادية يصعب تحليلها وفهما إلا بعد عرضها على خبير متخصص فيها (كخبير من الطب الشرعي / الذي يتم اللجوء إليه لتحديد الصفة التشريحية في جرائم القتل لمعرفة سبب الوفاة) ، ويكون الخبير في حكم الشاهد من حيث الحُجية أو القوة في الإثبات.

ويرجع صعوبة ضبط وإثبات الجرائم الإلكترونية ، إلى كونها ترتكب في مسرح جريمة افتراضي Cyberspace يختلف كليًا عن مسرح الجريمة التقليدية ، ومن ثم لا يتصور القواعد العامة التقليدية لانتداب الخبراء لتفقد آثار الجناة .[١]

(١) ثنيان ، ناصر آل ثنيان ، (٢٠١٢) " إثبات الجريمة الإلكترونية – دراسة تأصيلية تطبيقية " ، رسالة ماجستير ، جامعة نايف العربية للعلوم الأمنية ، كلية الدراسات العليا ، قسم العدالة الجنائية، ص ٢٤ وما بعدها.

ورغم ذلك تلعب الخبرة الفنية دور كبير في إثبات الجريمة الإلكترونية وجمع أدلتها، و التحفظ عليها فالخبير التقني المتخصص بمثابة المعاون الذكي للمحقق في كشف الغموض المرتبط بأدلة الجريمة الإلكترونية محل التحقيق. (١)، ونجاح هذا الأمر يتطلب انتداب خبراء ذو مواصفات ومهارات عالية في هذا المجال التقني ليمكن المحقق من: القدرة على تحليل البيانات الخاصة بأنظمة الـ hard ware &Soft ، وفك الشفرات Cryptanalysis skills واستعادة البيانات الملغاه ، والادراك الكامل لآلية عمل الشبكات المعلوماتية ،وكذلك وكافة البرامج والتطبيقات الإلكترونية اللازمة، حتى يتمكن من تحديد الأماكن المحتملة للأدلة ، ونوع البرامج المستخدمة في الجريمة ، ونقل الأدلة إلى أوعية أخرى دون تلف لأغراض التحقيق دون أن يؤدي إلى محو أثرها أو تلفها .

وغياب الخبرة الفنية عالية التقنية قد يتسبب في عجز سلطات التحقيق والاستدلال عن كشف الحقائق وجمع الأدلة ، لذلك يجب أن تتوفر في الخبير المنتدب الضوابط القانونية المعول بها عند ندب الخبراء لأغراض التحقيق: (٢)

- يكون الخبير من ضمن جدول الخبراء التي تعدها المجالس القضائية المتخصصة .
- أداء اليمين القانونية .

(١) الفيل ، علي عدنان (٢٠١٢) ، " إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية " ، المكتب الجامعي الحديث بغداد ، ، ص ٢٧

(٢) العازمي ، فهد عبد الله العبيد. (٢٠١٢)، مرجع سالف ذكره ، ص ٦٤٠ ،

- مع توفير الأجهزة والوسائل والبرامج وأنظمة كشف الاختراق ، وبرامج مراجعة واسترجاع العمليات التي تعينه على أداء دوره التقني وإنجاز خبرته على أكمل وجه .[١]

وقد حثت اتفاقية بودابست ١٦م الدول على تطبيق أنظمة فنية لحماية البيانات المخزنة وإلتزام العاملين في أي نظام معلوماتي بحفظ كل العمليات المنطقية التي تجري على الأجهزة لمدة لا تقل على ٩٠ يومًا ، وهذا يتطلب توفير برنامج وطني متكامل لرفع مستوى كفاءة العمل بهذه التقنية للتمكن من ملاحقة تلك الجرائم.

الفرع الثالث

المشكلات المتعلقة بسلطات التحري والملاحقة

تضمنت اتفاقية بودابست في (المواد ١٨/١٩/٢٠) مجموعة من الإجراءات التي يجب أن تعتمدها السلطة التشريعية بكل دولة طرف للتمكن من الحصول على الأدلة وضبطها ، ومن أهم هذه الإجراءات الإجراءات الممهدة لجمع الأدلة :-[٢]

وهي نوع من المراقبة والمتابعة من السلطة المختصة يتولى القيام بها مقدمو خدمات الحاسب الآلي والإنترنت ، وتنقسم إلى نوعين :

(١) الشهري ، حسن بن أحمد .(مارس ٢٠١٢)، " نظم المعلومات وتكاملها مع النظم الخبيرة "، مجلة الفكر الشرطي، عدد ٨٢ ، صادر عن مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، الإمارات العربية المتحدة، ، ص.ص ٦٧ ٦٨

(٢) بغدادي ، أدهم باسم نمر (٢٠١٨) ، " وسائل البحث والتحري عن الجرائم الإلكترونية " ، أطروحة مقدمة لنيل درجة الماجستير في القانون العام بكلية الدراسات العليا ، جامعة النجاح الوطنية ، فلسطين ، ص ٧٢ وما بعدها

١. النوع الأول: إجراءات التحفظ على مضمون البيانات وإلزام مقدمو الخدمات من أفراد وشركات بحفظ البيانات المخزنة بالحواسيب والإنترنت لفترة زمنية معينة ، وإلزامهم بتمكين السلطة المختصة بالاطلاع والتحقيق في شأن تلك البيانات المحفوظة.

٢. النوع الثاني : التحفظ السريع على محفوظات خط سير البيانات (إرسال/استقبال/نقل) و إلزام مقدمي الخدمات بمساعدة جهة التحقيق للتعرف على مُرتكب الجريمة الإلكترونية والمساهمين معه في ارتكابها ، (م/١٧بودابست) .

* صعوبات جمع الأدلة والاستدلال في الجرائم الإلكترونية : [١]

يصعب اكتشاف الجرائم الإلكترونية و إثباتها لـــ:

- نتيجة الذكاء الذي يتمتع به المجرم المعلوماتي الذي يكون لديه المهارة في محو أي آثار تدل عليه ، ومن ثم صعوبة اكتشافهم وإدانتهم. [٢]
- صعوبة تتعلق بالجانب الفني لعمليات البحث والتحقيق في تلك الجرائم لقصور في الإلمام بالمعرفة و التقنيات الحديثة لدى القائمين بعمليات البحث والتحقيق. [٣]

(١) الغافري ، حسين بن سعدي. (٢٠٠٩) .السياسة الجنائية في مواجهة جرائم الإنترنت، دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق، جامعة عين شمس، القاهرة. ص ١٢٠.

(٢) عباس ،عمرو حسين .(إبريل ٢٠٠٨) ، " أدلة الإثبات الجنائي والجرائم الإلكترونية" بحث مقدم إلى المؤتمر الإقليمي الثاني حول تحديات تطبيق الملكية الفكية في الوطن العربي،المنظم من طرف دولة مصر بمقر جامعة الدول العربية خلال الفترة ٢٦-٢٧/٤/ ٢٠٠٨ .

(٣) جمال ، براهيمي .(٢٠١٨) . " التحقيق الجنائي في الجرائم الإلكترونية " جامعة مولود معمري، كلية الحقوق والعلوم السياسية – قسم الحقوق ، ص ص ١٥٢-١٦٠

لذلك أوصى المجلس الأوروبي ١٩٩٩ إلى ضرورة تدريب الشرطة و أجهزة العدالة بما يواكب التطور المتلاحق لتقنية المعلومات ، لذلك تعقد المنظمة الدولية للشرطة الدولية العديد من الدورات التدريبية لمُحققي جرائم الحاسب الآلي لتدريبهم على أعلى مستوى. (١)

الفرع الرابع

المشكلات المتعلقة بالاختصاص والقانون الواجب التطبيق

يحدد الاختصاص المكاني للقانون الجنائي الوطني أربعة مبادئ رئيسية: مبدأ الإقليمية، الشخصية ، العينية و العالمية ، وتأخذ معظم التشريعات الجنائية بمبدأ الإقليمية كأصل عام ثم تكمله بالمبادئ الأخرى .

و يقصد بمبدأ الإقليمية : تطبيق القانون الوطني علي كل جريمة ترتكب في إقليم الدولة، سواء أكان الجاني وطنيًا أم أجنبيًا، وسواء أكان المجني عليه فيها وطنيًا أم أجنبيًا، وفي بيئة الجرائم الرقمية يكفي اعتبار مجرد مكالمة هاتفية مع شخص في دولة أخرى مبررًا لاعتبار الجريمة قد وقعت بالفعل فوق إقليم الدولة!.

ويقصد بمبدأ العينية : سريان القانون الوطني على جرائم معينة تقع في خارج البلاد بغض النظر عن جنسية الفاعل في تلك الجرائم بسبب تعلقها بمصالح جوهرية للدولة ، وهو ما أخذ به القانون المصري (م/٣) بسريانه " على كل من ارتكب خارج جمهورية مصر العربية من غير المصريين جريمة من الجرائم المنصوص عليها من هذا القانون، متى كان الفعل معاقبًا عليه في الدولة التي وقع فيها تحت أي وصف قانوني".

---

(١) العجمي ،عبد الله دغش ، (٢٠١٤) ، مرجع سابق، ص ٨٤

ويقصد بمبدأ العالمية : سريان القانون الوطني على الجرائم التي تتعلق بتقنية المعلومات والتي تقع خارج البلاد حتى وإن كان الفاعل أجنبي وهو ما يسمي بالاختصاص السلبي.

ومن المتعارف عليه أن مبدأ الشخصية في قانون العقوبات له وجهان: وجه سلبي : يقصد به تطبيق القانون على كل جريمة يكون المجني عليه وطنيًا ولو كان المُرتكب أجنبيًا ولو ارتكب الجريمة خارج إقليمها ، ووجه إيجابي: يُقصد به تطبيق القانون الوطني على كل من يحمل جنسية الدولة ولو ارتكب الجريمة على أجنبي خارج إقليمها (وهو المعمول به في أغلب التشريعات الوطنية). (١)

و الأمرلا يخلو من ظهورصعوبات، تفضي إلى إثارة تنازع في الاختصاص إما إيجابي بين أكثر من تشريع وطني ، أو سلبي يخرج معه اختصاص أي من الدول بملاحقة الجاني. (٢)

وقد ثار جدل حول الأحقية في ملاحقة المعلومات المخزنة خارج إقليم الدولة أو البيانات التي تم معالجتها إلكترونياً خارج الإقليم ، وهنا ظهر رأيان:

١- الأول : يرى إنه من غير المشروع أن تقوم سلطات الدولة بالتدخل وتفتيش النظم المعلوماتية الموجودة في إقليم دولة أخرى ، لكشف أوضبط أدلة تتعلق بجريمة وقعت على أراضيها وذلك استنادًا إلى مبدأ إقليمية القانون .

٢- الثاني ، يرى أنه من الممكن توافق الآراء دولياً بالسماح بتنفيذ إجراءات الملاحقة والتفتيش وغيرها لكشف وضبط أدلة خارج الإقليم ، حال توافر

(١) المرجع السابق، ص ٨٦
(٢) المرجع السابق ، ص ٨٦

ظروف معينة يتم تحديدها ، كإشعار الدولة المراد تفتيش البيانات والمعلومات المخزنة بنظمها المعلوماتية [1]، ولذلك كانت الحاجة مُلحة لإبرام اتفاقيات تنظم وقت وكيفية اتخاذ مثل هذه الإجراءات.

وقد أتاحت وسائل الاتصال عبر الإنترنت و الأقمار الصناعية المتطورة، فرصًا هائلة للخروج على مبدأ الإقليمية ، فتم الأخذ بمبدأ العينية ليتمكن القانون الوطني من ملاحقة الجرائم التي تقع خارج البلاد (مصر) ، وكذلك طبق البعض مبدأ العالمية ليتمكن القانون الوطني من ملاحقة الجناة الأجانب في أي مكان طالما كان المجني عليهم يحمل جنسية القانون الوطني (بلجيكا) ، ومن ثم يكون الحق في تسليم المجرمين ومحاكمتهم. [٢]

كيفية التغلب على التنازع الإيجابي للاختصاص :

النهج الأول : إعطاء الأولوية لأي من الدول المتنازعة وفقًا لأحد معايير الاختصاص الأكثر جدوى لضمان ملاحقة الجريمة ، وهنا يبدو مبدأ الإقليمية هو الأكثر قبولًا ، حيث أن الدولة التي يقع فيها الجزء الأكبر من النشاط الإجرائي تكون هي الأرجح في ملاحقة الجريمة ومحاكمة فاعليها.

---

(١) وعلى هذه الكيفية أصدر المجلس الأوروبي في ١١ سبتمبر ١٩٩٥ توصية من بين عدة توصيات تناولت مشاكل الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات ، جاء فيها بأن تفترض إجراءات التحقيق مد الإجراءات إلى أنظمة حاسب آلي أخر قد تكون موجودة خارج الدولة وتفترض التدخل السريع ، وحتى لا يمثل مثل هذا الأمر اعتداء على سيادة الدولة أو القانون الدولي ، وجب وضع قاعدة قانونية صريحة تسمح بمثل هذا الإجراء ،

(٢) الحصاوي ، مروي السيد.(٢٠١٩). مبدأ العالمية في القانون الجنائي، رسالة دكتوراه، كلية الحقوق، جامعة المنصورة ، ص ١٠٢

ويأتي في المرتبة الثانية مبدأ العالمية من حيث الملائمة بالنسبة للدول التي يقع فيها النشاط الإجرامي يليه مبدأ الشخصية في شقه الإيجابي ، بحيث ينعقد الاختصاص بنظر الجريمة للدولة التي يحمل جنسيتها مُرتكب هذه الجريمة ، فإن تعددت جنسياته ، فيكون من حق الدول التي يحمل جنسياتها حتى لا يأخذ البعض من اكتساب جنسية جديدة سبيلاً للإفلات من الملاحقة ، كما يمكن اللجوء إلى هذا المعيار تفاديًا لإفلات المُتهم من الملاحقة حين لا يتيسر ملاحقته وفقًا لأي من المعاييرالأربعة السابقة.

النهج الثاني يتمثل في تأكيد الملاحقة الجنائية عند كل حالة يخشى فيها لسبب إجرائي أو آخر إفلات مُرتكب الجريمة من المحاكمة ، ومثال ذلك : حين تقع الجريمة في إقليم دولة معينة ويتم إلقاء القبض على المُتهم في دولة أخرى يكون مُتمتعًا بجنسيتهًا ، هنا يُثار التنازع في الاختصاص وفقا لـ : مبدأ الإقليمية الذي يمنح الاختصاص لدولة مكان وقوع الجريمة ، ومبدأ العالمية الذي يعطي الاختصاص بملاحقة الجريمة لدولة مكان القبض على المُتهم ، ويبيح لها في الوقت نفسه التنصل لأنها غير مجبرة على تسليم رعاياها .

ونرى إمكانية حل هذه المعضلة من خلال : بـ

- الاعتراف بمبدأ المحاكمة أو التسليم كلما أمكن .
- الاعتراف بإمكانية إحالة الدعوى الجنائية عن الجريمة الواقعة من دولة إلى أخرى .
- التأكيد على ضرورة تبادل كافة أشكال المساعدة القانونية بين الدول.

- اللجوء إلى الإنابة القضائية ، ويتم ذلك وفقًا لقانون الدولة المطلوب منها مباشرة هذه الإجراءات ، وليس طبقًا لقانون الدولة التي تم إنابتها في القيام بالإجراءات .

* التعاون الدولي في المسائل الجنائية وفقاً لاتفاقية بودابست :

لم يعد الإنتربول وحده وسيلة التعاون الجنائي بين الدول ، بل أصبح لزاماً على الدول أن تستخدم بروتوكولات موحدة لنظم تخزين المعلومات وحمايتها ، لذلك بات تطوير البنية التحتية الرقمية والمعلوماتية ضرورة مُلحة لأي دولة ومطلباً أساسياً لمواجهة الانتهاكات الإلكترونية الإجرامية ، وقد تبنت بودابست صور وأشكال وحدود التعاون الدولي في الجرائم الإلكترونية، حيث:

- حثت اتفاقية بودابست م/ ٢٣ على : التعاون الدولي على أوسع نطاق في المسائل الجنائية الخاصة فيما يخص إجراءات التحقيق والتحري وجمع الأدلة ، وبالترتيبات المتفق عليها في ضوء التشريعات التي تتعلق بالجرائم الجنائية ذات الصلة بهذا النوع من الجرائم.

- وحثت م/ ٣٠ أيضاًعلى : الكشف والمساعدة على الفور عن بيانات الحركة المحفوظة (وفقاً للمادة ٢٩) والمتعلقة بالاتصال محل التجريم ، لتحديد هوية مزود الخدمة والمسار الذي تم من خلاله ذلك الاتصال ، وأجاز نص المادة ؛ للدولة المطلوب منها المساعدة - حجب بيانات الحركة- المطلوب منها الافصاح عنها – متى رأت أنها تتعلق بجريمة سياسية أو اعتبرت ما ستقدمه من معلومات من شأنه إلحاق الضرر بسيادتها وأمنها ، أو نظامها العام .

- وأجازت م /٣ : لدولة التحقيق أن تطلب من دولة طرف أخرى البحث في بيانات، النفاذ إليها، مصادرتها، تأمينها ...إلخ متى كانت مُخزنة بواسطة نظام إلكتروني يوجد داخل أراضي الدولة الطرف المطلوب منها المساعدة.

ورغم ذلك لازال هناك العديد من التحديات والصعوبات التى تعترض التعاون الدولى بين الدول فى تلك الجرائم منها :-

- عدم وجود اتفاق عام بين الدول على مفهوم الجرائم .
- عدم وجود توافق بين قوانين الإجراءات الجنائية للدول بشان التحقيق في تلك الجرائم .
- النقص الظاهر في مجال الخبرة لدي الشرطة و جهات الإدعاء و القضاء .[١]

ومن جانبنا نرى أن نجاح التعاون بين الدول بالسماح لتفعيل الإنابة القضائية:

لاستكمال وإتمام إجراءات التحقيق والمُلاحقة الجنائية (كسماع شهادة مُتهم مُقيم بالخارج عن طريق الإنابة القضائية)[٢] ، سيكون من شأنه تسهيل إتمام الإجراءات الجنائية بين الدول بما يكفل تقديم المُتهمين للمحاكمة وتحقيق الردع الجنائي المطلوب لمكافحة تلك الجرائم.

(١) عوض ، محمد محي الدين .(٢٠١١) ، " مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات " دار الفكر العربي ، ط١ ، القاهرة ص.ص ٣٢٦-٣٢٧

(٢) مهدي ، عبد الرؤوف . (١٩٩٦). شرح القواعد العامة للإجراءات الجنائية ، دار النهضة العربية ، الاسكندرية، ص ١٠٢.

المبحث الخامس

التدابير الواجب اتباعها لمواجهة الجرائم الإلكترونية

هناك من الإجراءات والتدابير التي يجب اتخاذها على كافة المستويات الوطنية والدولية للحماية من خطر الجرائم الإلكترونية ومكافحة مخاطرها ، من خلال اتخاذ خطوات جادة في توفير الحماية الأمنية والقانونية اللازمة.

المطلب الأول

تدابير وإجراءات الحماية الأمنية

تشمل الحماية الأمنية ثلاث نقاط هامة تتعلق بأمن المعلومات ومهدداتها و إجراءات الحماية المُمكنة لها .

١. <u>حماية أمن المعلومات</u>:

- الاهتمام الأمني بالمعلومات المُخزنة بحواسب المؤسسات كالبنوك والبورصة والوزارات .
- تخصيص تغطية مالية كافية لتوفير برامج حماية النظم المعلوماتية والإلكترونية لضمان الحفاظ عليها و جاهزيتها للاستخدام عند تلف ،مع ضمان السرية الكاملة لها.

- الحماية الأمنية للنظم الذاتية الخاصة للأفراد لضمان عدم الإساءة للحريات الخاصة بإفشائها والتلاعب بها.

ونقترح إنشاء وحدة طوارئ إلكترونية بالهيئات الوطنية المتخصصة لرصد التطور في حالات الهجمات الإلكترونية المستحدثة ، والعمل على دراسة ما يستجد من أساليب وتقنيات بخصوصها في محاولة لإيجاد حلول أمنية تحمي المنصات الموجودة من مخاطر الاختراق الأمني.

٢. التصدي لمهددات أمن المعلومات : منها :

- مهددات ناتجة عن كوارث طبيعية .
- مهددات بشرية غير مقصودة كسوء استعمال كلمة السر، أو تصفح موقع خبيث دون علم بحقيقة أمره.
- أخطرها : مهددات المتسللون (الكراكز) والمخترقون (الهاكرز) للمواقع والأجهزة باستخدام الثغرات الأمنية أو ثغرات بروتوكولات الاتصالات لها عدة أنواع منها : الفيروسات/الدودة / الباب السري [١] ، وما يُستجد من برامج أخرى يبتكرها الذكاء الإجرامي الإلكتروني.

٣. اتباع الإجراءات الأمنية الوقائية اللازمة :

- إستخدام برنامج الـ fire well ، (وهي عبارة عن برنامج يوجد حاجز بين الشبكة الداخلية الإنترنت و خادم شبكة الإنترنت Server) يقوم بفحص

(١) الفيروسات تتمكن من إفراغ الملفات من محتوياتها ، و الباب السري : يسمح بالدخول دون المرورباجهزة أو برامج الحماية ، أما الدودة فهو برنامج يؤدي إلى تخريب الملفات التي يدخلها .

المعلومات الداخلة و الخارجة والسماح لها بالمرور في حالة مطابقتها للمواصفات، إلا أنه لا يمنع من تعطيل بعض المعلومات و إحداث عُطب لها.

- استخدام عمليات التشفير.
- تفعيل التوقيع الرقمي .
- إستخدام أنظمة برامج الحماية ضد الفيروسات ، ووضع حلول للثغرات الأمنية.
- وضع سياسة أمنية لشبكة المعلومات تتماشى مع توصيات بودابست.
- الإحتفاظ بالمعلومات الحساسة على نسخ احتياطية بعيداً عن الشبكة.
- توعية الأفراد وإرشادهم دائماً لاتباع إجراءات السلامة فيما يتعلق بأمن معلوماتهم مثل :

. عدم فتح الرسائل مجهولة الهوية أو استخدام برامج غير اصلية ومجهولة المصدر.

. الحيطة والحظر من الإعلانات الخداعة.

. الحرص على الحفاظ على سرية المعلومات الخاصة جدًا ، وعدم الكشف عن كلمة السرنهائياً وتغييرها بشكل مستمر واختيار كلمات سر صعبة .

. تجنب تخزين الصور الخاصة على مواقع التواصل الاجتماعي و أجهزة الحاسب.

. استمرارية تحديث برامج الحماية الخاصة مثل ، MCafee، Norton.

. عدم ترك جهاز الحاسب مفتوحاً ، وعدم ترك الجهاز متصلاً بشبكة الإنترنت حال عدم الاستخدام.

. الحيطة والحذر من إعلانات الخداعة .

جميع تلك الإجراءات الأمنية إجراءات وقاية ، لا تحمي حماية مطلقة ولكن تُساهم في رصد وتحجيم المحاولات الإجرانية ، إلا أن خير سبيل حقيقي لمكافحة تلك الجرائم ، هو تنظيمها في إطار تشريعي وجزائي رادع . [١]

المطلب الثاني

التدابير التشريعية

تحدثنا القاعدة الشرعية الأصيلة: " لا جريمة ولا عقوبة إلا بنص " ـ لذا تعتبر الحلول التشريعية أحد أهم التدابير الوقائية التي تتخدها الدول ، وهناك حلول تشريعية مؤقته وأخرى دائمة :

١. فمن الحلول المؤقتة (القرارات التنظيمية):

- إصدار السلطة المختصة بعض المراسيم التنظيمية (كفرض تدابير احترازية على أنشطة مقاهي الإنترنت ، للوقاية من استغلالها أداة لتنفيذ تلك الجرائم) .
- التدخل لمنع الولوج إلى المواقع المُخلة بالحياء أو المُحرضة للعنف أو التطرف حماية للنظام العام بالدولة.
- دعم الدولة لبرامج الحماية ضد الفيروسات بأسعار في المُتناول ، لتشجيع على استخدامها.

(١) رشاد ، إسراء جبريل. (٢٠١٦) .الجرائم الإلكترونية " الأهداف – الأسباب – طرق الجريمة ومعالجتها" ، بحث منشور بالمركز الديمقراطي العربي ، ٩ اغسطس ، متاح على: https://democraticac.de/?p=٣٥٤٢٦

- التوعية المجتمعية والقانونية والتعريف بمدى خطورة الجرائم الإلكترونية.
- تدريب المحققين و رجال شرطة و قضاة على دراية عالية بالتقنية المعلوماتية وجرائم الإنترنت.
- فرض غرامات مالية وعقوبات تصل لإغلاق المنشأة التي تقدم خدمة الإنترنت للجمهور حال عدم إلتزامها بضوابط أمن المعلومات والمواقع المحظور الدخول عليها .

٢. من الحلول الدائمة (إصدار تشريع متخصص):

يجب مكافحة هذا النوع من الجرائم من خلال تشريع خاص يُنظمها ، يتوافق مع الإحداثيات العصرية والاتفاقيات الدولية المبرمة في هذا الشأن ، ويدعم التعاون الدولي بين كافة الأطراف المعنية بالجريمة ، ويكون قادرعلى تغطية كافة الجوانب المتعلقة بتلك الجرائم وإشكالياتها وتحدياتها، ومنها :

- أن يتضمن نطاق الحماية الجنائية الاعتراف بالأدلة الرقمية ومن ثم التوسع في حماية كل ما هو رقمي (العقد الإلكتروني و التوقيع الإلكتروني .... وما يستجد بالعالم الافتراضي).
- مواكبة احداثيات ومستجدات التجارة الإلكترونية وكل ما يرتبط بها من التسويق الإلكتروني و الدفع الإلكتروني ، وجميعها مجالات خصبة للاحتيال يجب تغطيتها.
- تعيين وسائل الإثبات ، وتبني المعاينة و الخبرة كأساليب للتحقيق في إثبات الجريمة الإلكترونية .
- إضافة التعديلات اللازمة على قانون الإجراءات الجزائية ، وقانون حقوق المؤلف وكافة القوانين ذات الصلة ، حتى لا تخلو من الحماية الجنائية للحقوق الإلكترونية .

- ضمان مساءلة كل من تعدى على مصلحة إلكترونية ذات حماية أياً كان نوع الشخص : طبيعي، أو معنوي ، مؤسسي ، مختلط .
- إدماج نصوص جرائم الإنترنت بفصل مستقل في قانون العقوبات الوطني.

- **ومن أساليب مكافحة الجرائم الإلكترونية:**

- التدريب التقني المستمرلرجال الشرطة والقضاء لتمكنهم من كشف تلك الجرائم وإيجاد السُبل الأدق في مواجهتها.
- حث الدول على التعاون فيما بينها خاصة في مجال تبادل المعلومات والإنابة القضائية سواء كان فيما يخص إجراءات التحقيق ، أوتسليم المجرمين .
- حث الدول على فرض عقوبات صارمة على المُرتكبين نظراً للخطورة الجسيمة لتلك الجرائم والتي قد تمس الأمن القومي.
- الاعتماد على أحدث التقنيات للتمكن من سرعة الكشف والاستدلال عن هوية مُرتكبي تلك الجرائم .
- الإسراع في إبلاغ الجهات الأمنية المعنية فور التعرض لاحتيال إلكتروني.
- توقيع الدول على معاهدات مكافحة الجرائم الإلكترونية والإلتزام بضوابطها لسهولة التعاون المشترك.
- إنشاء وحدات مختصة في التحقيق في جرائم الكمبيوتر في المحاكم والشرطة.
- تفعيل المشاركة الدولية والعربية لمواجة ومكافحة الجرائم المستحدثة منها أولاً بأول.

الخاتمة:

يعتبر الإنترنت سبباً رئيسياً في جعل الجرائم الإلكترونية عابرة للحدود والقارات حيث ترتكب الجريمة في دولة وتتحقق نتائجها في دولة أخرى، لذا يتطلب الأمر وجود تعاون دولي مشترك و مثمر لمواجهة التحديات الخاصة بتلك الجرائم ، والتصدي لأهم العقبات التي تقف حجر عثرة أمام هذا التعاون الدولي المنشود ، والتي منها:-

- **عدم وجود مفهوم محدد ومشترك بين الدول لماهية الجريمة الإلكترونية.**
- **عدم وجود مفهوم عام حول التعريف النظامي للنشاط الإجرامي المتعلق بالجرائم الإلكترونية.**
- **اختلاف آليات التصدي لتلك الجرائم وذلك لاختلاف فلسفة النظم القانونية المختلفة حول العالم.**
- **ضعف التنسيق بين أنظمة وقوانين الإجراءات الجنائية للدول المختلفة فيما يتعلق بالتحري والتحقيق في الجرائم الإلكترونية.**
- **نقص الخبرة لدي الجهزة الشرطية والقضائية في مجال المعلومات حول تلك الجرائم.**
- **تعقد المشاكل القانونية والفنية الخاصة بتنفيذ إجراء معلوماتي معين خارج حدود الدولة، أوضبط معلومة مخزنة فيه أو الأمر بتسلمها.**
- **عدم وجود معاهدات للمعاونة الثنائية أو الجماعية بين الدول التي تسمح بالتعاون الدولي الكفء لمواجهة المتطلبات الخاصة بتلك الجرائم أوسرعة إجراء التحريات فيه.**

- احتياج الأنظمة الجزائية الوطنية في التطور والتحسين التشريعي المستمر لمواكبة التطورات الهائلة والسريعة التي يصل إليها المجرمون المعلوماتيون في ارتكاب تلك الجرائم.
- صعوبة حصرهذا النوع من الجرائم نتيجة للتطور الهائل و السريع و المستمر دائماً.
- صعوبة إثبات الجريمة الإلكترونية ، لصعوبة حفظ الأدلة ،وصعوبة ملاحقة المجرمين المعلوماتيين لكونهم لا يتركون أثراً مادياً ورائهم .
- المحاكمة في الجرائم الإلكترونية هو ذاته المتبع في الجرائم العادية ولكن تختلف اختلاف أنواع الأدلة، لكونها عادة ما تكون ذات معطيات إلكترونية.

وكان من أولويات طرحنا البحثي تخصيص مبحث مستقل لإلقاء الضوء على أهم التدابير اللازمة لمواجهة الجرائم الإلكترونية بينما من خلال هذه الخاتمة الموجزة نأمل إلقاء الضوء على مجموعة من التوصيات التي من شأنها تدعم نجاح التدابير الخاصة بمكافحة الجرائم الإلكترونية ، <u>لذلك نوصي</u> :

- <u>على المستوى الوطني:</u>

- اتخاذ المؤسسات الوطنية العربية المختلفة كافة التدابير اللازمة لحماية أمن معلوماتها من الاختراق والسرقة بمراجعة سياساتها الأمنية بشكل دوري لضمان توافقها مع المعايير العالمية لأمن المعلومات.
- نشر الثقافة القانونية الكافية للحماية من الوقوع فريسة في براثن هذا النوع من الجرائم وتشجيع كافة صور التعاون الدولي في هذا الشأن ، والتركيز على الشباب الجامعي في هذه التوعية.

- استخدام أحدث التقنيات والوسائل للكشف عن هوية مُرتكبي الجرائم .
- ضرورة تعاون الجهات الأمنية والقضائية مع جهات وشركات خاصة متخصصة للاستعانة بخبراتها عالية التقنية في الكشف عن تلك الجرائم ، وتقنين الخبرة بالنسبة لتلك الشركات حتى تكون كافة .
- توفير برنامج وطني متكامل لرفع كفاء المحققين في هذه التقنية للتمكن من ملاحقة تلك الجرائم تماشياً مع ما نصت عليه بودابست.
- الاستعانة بالانتربول للاستفادة من خبراتهم في مجال الجرائم الإلكترونية العابرة للحدود.
- دعم جهات التحقيق بتوفير موسوعة قانونية وقضائية شاملة على كافة التجارب المناظرة للاستفادة بها كمرجعيات وسوابق في تحليل ومراجعة هذا النوع من الجرائم .
- تفعيل رقابة وطنية عُليا على المُصنفات الإلكترونية المتداولة حماية للنظام والأمن الوطني العام من تلك المعلومات الخادعة والكاذبة التي يتم ترويجها بوسائل إلكترونية ، بهدف التربح من وراء تدمير القيم المجتمعية وبث الأفكار الشاذة عليه لإفساده أو احباطه ، أو توجيه إلكترونياً لسياسات ضارة أمنياً.

محبطة

- <u>على المستوى العربي و الدولي:</u>

- نأمل إعادة النظر وإصدار التشريعات اللازمة لمن لم يُصدر تشريع متخصص لمكافحة تلك الجرائم حتى الآن ويلحق التجريم لقانون العقوبات العام

(الجزائر) ، وتحديث نظم مكافحة الجرائم الإلكترونية بشكل دوري لتفادي النقص أوالعجز في النص(السعودية ، عُمان) ،وتحديث التشريعات العربية (مصر ، فلسطين)،وذلك كي تتمكن التشريعات الوطنية من مواجهة ومواكبة التحديات المتتابعة لعصر الرقمنة الذي يشهده العالم والآخذ في التطور المستمر والسريع ، وذلك لضمان وتحقيق الحماية الجنائية اللازمة لأمن المعلومات ، ومن ثم تحقيق الردع وتدارك ضعف النص التشريعي الذي قد يؤدي إلى الانفلات من العقوبة .

- التركيز على أن يكون هناك اهتمام وتضامن عربي متكامل من خلال عقد اتفاقية تعاون عربية في مكافحة الجرائم الإلكترونية والمعلوماتية ، يعقد لها لجنة دائمة تنعقد سنوياً بجامعة الدول العربية ، بهدف بحث سُبل التعاون فيما بين الدول العربية في مكافحة تلك الجرائم ، والاستفادة من خبرات بعضهم البعض وتيسير تبادل المعلومات عبر الانتربول وكذلك تفعيل الإنابة القضائية العربية ، وتقديم العون العربي المشترك للدول التي تحتاج مساعدة لدعم أمنها المعلوماتي وتقريب الفوارق التكنولوجية قدر الإمكان .
- تشجيع التعاون الرقمي بين الدول العربية في كافة المجالات .
- ضرورة التعاون الدولي لضمان فرض عقوبات كبيرة ورادعة على مُرتكبي هذه الجرائم.

المراجع والمصادر

١. أحمد ، هلالي عبد الله. (٢٠٠٧) . الجوانب الموضوعية والاجرائية للجرائم المعلوماتية على ضوء اتفاقية بودابست الموقعة ٢٣ نوفمبر ٢٠٠١ ، دار النهضة العربية، الطبعة الأولى ، القاهرة .

٢. أيوب ، بولين. (٢٠٠٩) . الحماية القانونية للحياة الشخصية في مجال المعلوماتية ، منشورات الحلبي الحقوقية ، بيروت.

٣. بغدادي ، أدهم باسم نمر. (٢٠١٨) . وسائل البحث والتحري عن الجرائم الإلكترونية ، أطروحة مقدمة لنيل درجة الماجستير في القانون العام بكلية الدراسات العليا . جامعة النجاح الوطنية . فلسطين

٤. بكري ،بكري يوسف .(٢٠١٠). التفتيش عن المعلومات في وسائل التقنية الحديثة ، دار الفكر الجامعي. الإسكندرية.

٥. ثنيان ، ناصر آل ثنيان. (٢٠١٢) . إثبات الجريمة الإلكترونية – دراسة تأصيلية تطبيقية ، رسالة ماجستير جامعة نايف العربية للعلوم الأمنية. كلية الدراسات العليا ، قسم العدالة الجنائية، الرياض.

٦. جمال ، براهيمي. (٢٠١٨) . التحقيق الجنائي في الجرائم الإلكترونية ، جامعة مولود معمري ، كلية الحقوق والعلوم السياسية – قسم الحقوق ، الجزائر.

٧. حجازي ، عبد الفتاح بيومي. (٢٠٠٧) . صراع الكمبيوتر والإنترنت في القانون العربي النموذجي ، دار الفكر الجامعي ، القاهرة .

٨. حسني ، محمود نجيب .(١٩٧١) " النظرية العامة للقصد الجنائي " ، دار النهضة العربية ، ط٢ .

٩. حسين ، محمد عبد الطاهر. (٢٠٠٠) . المسئولية القانونية في مجال شبكات الإنترنت ، دار النهضة العربية ، القاهرة .

١٠.الحسيني، عبد الحسن ، القاموس الموسوعي في المعلومات والاتصالات والمعلوماتية القانونية ، مكتبة صادر ، الطبعة الأولى ، بيروت ٢٠٠٤ .

١١.الحصاوي ، مروي السيد.(٢٠١٩). مبدأ العالمية في القانون الجنائي، رسالة دكتوراه، كلية الحقوق، جامعة المنصورة.

١٢.حطب ، ياسر محمد الكومي. (٢٠١٤) . الحماية الجنائية والأمنية للتوقيع الإلكتروني ، منشأة المعارف، الإسكندرية.

١٣.الخن ، طارق. (٢٠١٨) . جرائم المعلوماتية ، الجامعة الافتراضية السورية ، متاح على: https://pedia.svuonline.org

١٤. ربايعة ، عبد اللطيف محمود. (٢٠١٦) . الجرائم الإلكترونية -التجريم والملاحقة والإثبات ، ورقة عمل مقدمة إلى المؤتمر الأول للجرائم الإلكترونية في فلسطين ، جامعة النجاح الوطنية ، ١٧ ابريل/نيسان، نابلس .

١٥.رشاد ، إسراء جبريل. (٢٠١٦) .الجرائم الإلكترونية " الأهداف – الأسباب – طرق الجريمة ومعالجتها" ، بحث منشور بالمركز الديمقراطي العربي ، ٩ اغسطس ، متاح على: https://democraticac.de/?p=35426

١٦.سرور ، أحمد فتحي. (١٩٨١) . الوسيط في قانون الإجراءات الجنائية ، دار النهضة العربية ، القاهرة .

١٧.الشناوي ، محمد. (٢٠٠٨) . جرائم النصب المستحدثة ، دار الكتب القانونية ، المحلة الكبرى ، القاهرة .

١٨.الشهري ، حسن بن أحمد. (مارس ٢٠١٢) . نظم المعلومات وتكاملها مع النظم الخبيرة ، مجلة الفكر الشرطي، عدد ٨٢ ، صادر عن : مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، الإمارات العربية المتحدة.

١٩.الشوا ، محمد سامي. (١٩٩٤). ثورة المعلومات وانعكاساتها على قانون العقوبات ، دار النهضة العربية ، القاهرة.

٢٠.العازمي ، فهد عبد الله العبيد. (٢٠١٢). الإجراءات الجنائية المعلوماتية ، رسالة لنيل درجة درجة الدكتوراه في القانون، كلية الحقوق، جامعة القاهرة.

٢١.عباس ، عمرو حسين. (ابريل ٢٠٠٨). أدلة الإثبات الجنائي والجرائم الإلكترونية ، بحث مقدم إلى المؤتمر الإقليمي الثاني حول تحديات تطبيق الملكية الفكية في الوطن العربي،المنظم من طرف دولة مصر بمقر جامعة الدول العربية خلال الفترة ٢٦-٢٧ إبريل ، القاهرة.

٢٢.عبد المطلب ، ممدوح عبد الحميد. (٢٠٠٦) .البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية ، القاهرة.

٢٣.العجمي ، عبد الله دغش. (٢٠١٤). المشكلات العملية والقانونية للجرائم الإلكترونية – دراسة مقارنة ، أطروحة لاستكمال رسالة الماجستير في القانون العام ، جامعة الشرق الأوسط ، الأردن .

٢٤.عطا الله ، شيماء عبد الغني.(٢٠٠٧). الحماية الجنائية للتعاملات الإلكترونية ، دار الجامعة الجديدة ، الاسكندرية.

٢٥.العفيفي ، يوسف خليل يوسف. (٢٠١٣). الجريمة الإلكترونية في التشريع الفلسطيني ،رسالة لاستكمال متطلبات الحصول على درجة الماجستير في القانون العام ، كلية الشريعة والقانون، بالجامعة الإسلامية ، غزة.

٢٦.عوض ، محمد محي الدين.(٢٠١١) . مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات ، دار الفكر العربي ، ط١ ، القاهرة .

٢٧.الغافري ، حسين بن سعدي. (٢٠٠٩) .السياسة الجنائية في مواجهة جرائم الإنترنت، دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق، جامعة عين شمس، القاهرة.

٢٨.فرغلي ، عبد الناصر محمد محمود ، المسماري ، محمد عبيد سيف سعيد .(٢٠٠٧) . "الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية"، دراسة تطبيقية مقارنة، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية، الرياض.

٢٩.الفيل ، علي عدنان. (٢٠١٢). إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية ، المكتب الجامعي الحديث ، بغداد.

٣٠.قايد ، أسامة عبد الله. (١٩٩٤) . الحماية الجنائية للحياة الخاصة وبنوك المعلومات ، دار النهضة العربية ، القاهرة.

٣١.قطب ، محمد علي ، (بدون سنة نشر) ، "الجرائم المعلوماتية وطرق مواجهتها " ، الأكاديمية الملكية للشرطة- وزارة الداخلية

٣٢.قورة ، نائلة عادل محمد فريد. (٢٠٠٥) .جرائم الحاسب الآلي الاقتصادية ، الطبعة الأولى ، منشورات الحلبي الحقوقية ، بيروت .

٣٣.الكثيري ، متعب بن هندي بن حمد. (٢٠١٩). المسئولية الجنائية للشخص المعنوي عن جرائم المعلوماتية في النظام السعودي : دراسة مقارنة بالقانون المصري ، رسالة ماجستير ، كلية العدالة الجنائية ،جامعة نايف العربية للعلوم الأمنية ، الرياض.

٣٤.لبشير ، سيدي محمد. (٢٠١٠) .دور الدليل الرقمي في إثبات الجرائم المعلوماتية، دراسة تحليلية تطبيقية ، بيان المسئولية رسالة ماجستير في العلوم الشرطية تخصص التحقيق والبحث الجنائي، كلية الدراسات العليا ،جامعة نايف العربية للعلوم الأمنية، الرياض.

٣٥.المطردي ، مفتاح بو بكر. (سبتمبر ٢٠١٢). الجريمة الإلكترونية والتغلب على تحدياتها ، ورقة مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية المنعقد في ٢٣-٢٥ سبتمبر ، السودان.

٣٦.مهدي ، عبد الرؤوف . (١٩٩٦). شرح القواعد العامة للإجراءات الجنائية ، دار النهضة العربية ، الاسكندرية.

٣٧.يونس ، بن عمر (٢٠٠٤) الجرائم الناشئة عن استخدام الإنترنت ، الطبعة الأولى ، دار النهضة العربية ، القاهرة.

- مصادر أجنبية:

1. UNODC United Nations Office on Drugs and Crime (2013).Comprehensive Study on Cybercrime. United nations

- **اتفاقيات وقوانين تم الإشارة إليها:**

- قانون العقوبات الفرنسي ١٩٨٨
- اتفاقية بودابست الصادرة عن المجلس الأوروبي عام ٢٠٠١
- نظام مكافحة الجرائم المعلوماتية السعودي ٢٠٠٧
- قانون مكافحة جرائم تقنية المعلومات المصري ٢٠١٨
- القانون العربي النموذجي ٢٠٠٣
- وثيقة الرياض لنظام القانون الموحد لمكافحة جرائم التقنية بدول مجلس التعاون الخليجي ٢٠١٣
- دليل الأمن السيبراني للبلدان النامية ، الاتحاد الدولي للاتصالات ITU ، طبعة ٢٠٠٧ : int.itu.www