International Journal of Legal and Comparative Jurisprudence Studies (LCJS)

Volume.5, Issue.1 pp: 1-17 Article 1
April (2024)

الأحكام الإجرائية للجرائم السيبرانية (دراسة مقارنة)

Procedural Provisions for Cybercrimes (Comparative Study)

ممدوح خليل البحر

Mamdooh Khalil Albaher

أستاذ القانون الجنائي- كلية الشرطة- أبوظبي

Professor of Criminal Law, Police College, Abu Dhabi

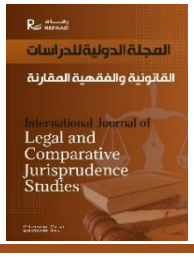
mamdooh.albaher@yahoo.com

Accepted قبول البحث	Revised مراجعة البحث	Received استلام البحث
2023/9/27	2023 /8/16	2023 /6/5

DOI: https://doi.org/10.31559/LCJS2024.5.1.1

رفـــاد REFAAD
www.refaad.com

International Journal of Legal and Comparative Jurisprudence Studies (LCJS)
المجلة الدولية للدراسات القانونية والفقهية المقارنة
Journal Homepage: https://www.refaad.com/Journal/Index/9
E-ISSN 2708-6607 | P-ISSN 2708-6593



الأحكام الإجرائية للجرائم السيبرانية (دراسة مقارنة)

Procedural Provisions for Cybercrimes (Comparative Study)

الملخص:

الأهداف: هدفت الدراسة إلى التعرف على الأحكام الإجرائية للجرائم السيبرانية في التشريع الإماراتي في القانون رقم 5 لسنة 2004 حول الأمن المعلوماتي والقانون رقم 5 لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات وتعديلاته. ومن أهم الأهداف التي تسعى الدراسة إلى تحقيقها: التعرف على مفهوم الجرائم السيبرانية وخصائصها، وبيان أهمية مرحلة التحقيق الجنائي في جمع الأدلة في مسرح الجريمة حيث تضمن التشريع الإماراتي نصوص قانونية إجرائية تكفل جمع الأدلة السيبرانية حيث يمكن الاستفادة من هذه النصوص والتوصل إلى توصيات مفيدة لطرق وإجراءات جمع الأدلة في الجرائم السيبرانية.

المنهجية: هناك أكثر من منهج تمت الاستفادة منها: المنهج الوصفي التحليلي لوصف الظاهرة موضوع الدراسة. والمنهج المقارن الذي يستدعى المقارنة مع بعض النظم القانونية العربية والأجنبية.

النتائج: من أهم النتائج التي توصلت الدراسة إليها أن الجريمة السيبرانية تشترط أساليب غير تقليديه وخاصتا جمع الأدلة والتفتيش والتحقيق. كما تتميز الجرائم السيبرانية بصعوبة إثباتها وسهولة اتلافها.

الخلاصة: نخلص من هذه الدراسة إلى ضرورة وجود تعاون إقليمي ودولي في مكافحة الجرائم السيبرانية وكذلك ضرورة وضع تشريعات جديدة على مستوى الوطني والإقليمي في مجال مكافحة هذا النوع من الجرائم. وأخيرًا، نوصي بضرورة إنشاء أقسام وإدارات في جميع مراكز الشرطة على مستوى دولة الإمارات يكون من اختصاصها متابعة ما يستجد من تطورات تقنية في مجال تكنولوجيا المعلومات والتقنية الحديثة للتعامل مع كافة الجرائم السيبرانية.

الكلمات المفتاحية: *الجريمة السيبرانية؛ شبكة الإنترنت؛ الدليل السيبراني؛ مسرح الجريمة السيبرانية؛ التفتيش في الجريمة السيبرانية.*

Abstract:

Objectives: The study aimed to identify the procedural provisions for cybercrimes in UAE legislation in Law No. 5 of 2004 regarding information security and Law No. 5 of 2012 regarding combating information technology crimes and its amendments. To achieve this goal, among the most important objectives that the study seeks to achieve are identifying the concept of cyber-crimes and their characteristics, and demonstrating the importance of the criminal investigation stage in collecting evidence at the crime scene, as UAE legislation includes procedural legal texts that guarantee the collection of cyber evidence as these texts can be benefited from and come up with useful recommendations for methods and procedures while collecting evidence in cyber-crimes.

Methods: There is more than one method that has been used: the descriptive and analytical approach to describe the phenomenon under the study. The comparative approach requires comparison with some Arab and foreign legal systems.

Results: One of the most important findings of the study is that cybercrime requires unconventional methods, especially evidence collection, inspection, and investigation. Cybercrimes are also difficult to prove and easy to destroy.

Conclusions: We conclude from this research that there is a need for regional and international cooperation in combating cybercrimes, as well as the need to develop new legislation at the national and regional levels in the field of combating this type of crime. Finally, we recommend the necessity of establishing sections and departments in all police stations across the UAE, whose specialization is to follow up on the latest technical developments in the field of information technology and modern technology to deal with all cybercrimes.

Keywords: *Cybercrime; the Internet; cyber evidence; cybercrime scene; cybercrime inspection.*

المقدمة:

إن مما يتصف به العصر الحالي، هو ازدياد وكثرة المعلومات بكافة وسائلها، والاعتماد عليها في الحياة اليومية وذلك منذ تطور شبكة الإنترنت والبريد الإلكتروني من خلال كثرة انتشار مواقعها على الشبكة العالمية، حيث أصبح الإنسان يتحول إلى الحياة الرقمية بعد دخولها إلى كافة مناحي الحياة سواء في وسائل التواصل مع الآخرين أو من خلال الاتصال مع الآلة.

وإزاء هذا التقدم العلمي الرهيب وظهور التقنية الرقمية تنبهت كثير من دول العالم ومنها دولة الإمارات العربية المتحدة إلى هذه الطفرة العلمية للتعامل مع متطلبات عصر الذكاء الاصطناعي في ظل الثورة الصناعية الرابعة والتي يقع فيها على كاهل أجهزة الشرطة والأمن المسؤولية الكبيرة للحفاظ على الأمن والنظام وبالتالي فقد اتجهت دول العالم إلى الاستفادة من هذه التقنية في كافة المجالات الأمنية والشرطية، حيث أدخلت التقنية الرقمية في نطاق الحكومة الذكية وفي التجارة الإلكترونية، كما أدخلت هذه التقنية في كافة التعاملات والابتعاد عن الإدارة التقليدية وهذا ما تقوم به الآن دولة الإمارات حيث استحدثت وزارة متخصصة للذكاء الاصطناعي وعلوم المستقبل حيث يمكن القول أن الذكاء الاصطناعي هو علم يهتم بصناعة آلات تقوم بتصرفات ذكية فهو عبارة عن جعل الآلة العادية تتصرف كالآلات التي تشاهد في أفلام الخيال العلمي، وبالتالي نستطيع أن نقول أن الذكاء الاصطناعي هو علم يهدف إلى جعل الحاسوب والآلات الأخرى تكتسب خاصية الذكاء وتكون لها القدرة على القيام بأشياء هي إلى وقت قريب كانت حصرًا على الإنسان، مثل التفكير والإبداع والتعلم وكذلك التخاطب.

وبكافة المجالات وبالأخص النطاق التكنولوجي، نرى أن فكرة الحكومة الإلكترونية التي تعتبر دولة الإمارات هي السباقة بين دول المنطقة في الأخذ بهذا التطور العلمي وتطبيقاته وتوج هذا التطور بإقامة مؤتمر سنوي لتطوير الحكومة الذكية، وبالتالي كان من الطبيعي أن تتجه دولة الإمارات إلى هذه التطورات ومنها إطلاق استراتيجية للذكاء الاصطناعي باعتباره التوجه العالمي الحديث حتى تبقى دولة الإمارات من الدول الحضارية وفي صدارة الدول الرائدة في الثورة التكنولوجية العالمية. وهذا يدفعنا إلى القول بأن دولة الإمارات تدير اقتصادها طبقًا لأحدث النظم التقنية، واستحداث أفكار أو نقل تجارب عالمية لكي تكون الدولة الأكثر استعدادًا للمستقبل، وهذا كله يهدف إلى تفعيل الابتكار في الإدارة للنهوض بمؤسسات الدولة على جميع المستويات، فالابتكار يعد من أهم القدرات التي يجب أن تحظى بالاهتمام والعناية والرعاية من قبل الدول، حيث أصبح الاهتمام بهذا العلم ضرورة تفرضها طبيعة العصر الحديث كونه له دور في جميع المجالات في الحياة العصرية. وعلى هذا الأساس نرى أن أهمية الحديث -على سبيل المثال- عن دور الذكاء الاصطناعي في نطاق العمل الشرطي، حيث أن الذكاء الاصطناعي يمكن أن يعمل على التنبؤ الأمني في الجرائم السيبرانية والتنبؤ الأمني يعتبر وسيلة عالية المستوى لمواجهة الجرائم الأكثر خطورة بل وحتى الوقاية منها (أبو النصر،2012، 18). ويمكن أن يحقق للأجهزة الأمنية والشرطية فوائد كثيرة ومن أهمها تحديد احتياجات الأجهزة الشرطية والأمنية المستقبلية والتسليح لوقاية المجتمع من الجرائم وخاصة السيبرانية الأكثر خطورة.

إشكالية الدراسة:

كان لظهور الجريمة السيبرانية عاملًا حاسمًا في قيام كثير من الدول بسن تشريعات جديدة او تعديل تشريعاتها القائمة لمواجهة هذا الخطر المتدفق لمواجهة الجريمة السيبرانية باعتبارها من أهم الجرائم المستحدثة تقرع في جنباتها أجراس الخطر لتنبه مجتمعات العصر الراهن لعظم حجم المخاطر الناجمة عنها التي تستهدف الاعتداء على المعطيات بدلالتها السيبرانية الواسعة، فسلاحها الحاسب الآلي وشبكة الإنترنت، ومقترفها مجرم ذكي له دراية كاملة في الأنظمة المعلوماتية والتقنيات التكنولوجية.

ولا تقف صعوبة اثبات الجرائم السيبرانية عند حد تعذر الوصول إلى الأدلة الكونية لأثباتها، لكن هذه الصعوبة تمتد إلى إجراءات الحصول على هذه الأدلة، وإذا كان من السهل على جهات التحري أن تتحرى عن الجرائم التقليدية عن طريق المشاهدة والتتبع والمساعدة، فأنه يصعب عليها القيام بهذه الإجراءات في شأن جرائم السيبرانية.

وتكمن إشكالية الدراسة في الإجابة على التساؤل التالي: **ما الطرق والأساليب الإجرائية المستخدمة في التعرف على الجرائم السيبرانية، وهل تخضع هذه الجريمة لقواعد إجرائية عامة أم قرر لها المشرع أحكامًا خاصة؟**

أهمية الدراسة:

تتجلى أهمية هذه الدراسة في أنه يتعرض لجانب مهم من قواعد قانون الإجراءات الجزائية والتي تتمثل في طرق جمع الأدلة في الجرائم السيبرانية حيث تتضمن إجراءات الضبط والمعاينة والتفتيش وغيرها من الإجراءات.

ويمكن إبراز أهمية الدراسة في النقاط التالية:

- تعد الجريمة السيبرانية نتاجًا وإفرازًا لتقنية المعلومات، فهي ترتبط وتقوم عليها، وقد أدى اتساع نطاق هذه الجرائم في المجتمع وازدياد ازدهار حجم ودور الشبكة المعلوماتية في القطاعات المختلفة إلى إعطاء الجرائم السيبرانية لونًا أو طابعًا قانونيًا خاصًا يميزها عن غيرها من الجرائم.
- أهمية موضوعهم الأدلة في الجرائم السيبرانية لإجل استظهار الدليل الجنائي وذلك كله في ضوء القواعد العامة للإجراءات الجزائية.

أهداف الدراسة:

تسعى الدراسة إلى تحقيق الأهداف التالية:

- التعرف على مفهوم الجريمة السيبرانية وخصائصها.
- بيان أهمية مرحلة الاستدلالات في جمع الأدلة في الجرائم السيبرانية.
- بيان أهم سمات مرتكبي الجرائم السيبرانية.
- بيان أهمية مرحلة التحقيق الجنائي في جمع الأدلة والتفتيش في الجرائم السيبرانية.

منهج الدراسة:

هناك أكثر من منهج تمت الاستفادة منها: المنهج الوصفي التحليلي لوصف الظاهرة موضوع الدراسة. والمنهج المقارن الذي يستدعي المقارنة مع بعض النظم القانونية العربية والأجنبية التي لها صلة مباشرة بموضوع جمع الأدلة في الجرائم السيبرانية وضمنت تشريعاتها بنصوص قانونية إجرائية تكفل جمع الأدلة السيبرانية وهذه النصوص القانونية يمكن الاستفادة منها في تشريعاتنا القانونية والتوصل إلى توصيات مفيدة لطرق وإجراءات جمع الأدلة والتفتيش في الجرائم السيبرانية.

أدوات الدراسة:

اعتمد الباحث على عدد من الأدوات البحثية ومن أهمها ما يلي:

- المراجع والمؤلفات القانونية التي تناولت الموضوع.
- الرسائل العلمية التي تناولت الموضوع أو أحد جوانبه.
- البحوث وأوراق العمل والمؤتمرات والندوات التي تناولت الموضوع أو أحد جوانبه.
- المواقع الإلكترونية التي تناولت الموضوع.

نطاق الدراسة:

- النطاق الزمني: التطور الإجرائي في القوانين والتشريعات الخاصة في الجرائم السيبرانية.
- النطاق المكاني: التركيز على دولة الامارات العربية المتحدة وبعض البلدان العربية وغير العربية أيضًا، التي اهتمت بالجرائم السيبرانية.
- النطاق الموضوعي: المعاينة والتفتيش في الجرائم السيبرانية.

خطة الدراسة:

قسمنا هذا الموضوع إلى مبحثين ومطلب تمهيدي وكما يلي:

مطلب تمهيدي: ماهية الجريمة السيبرانية.

المبحث الأول: إجراءات المعاينة في مسرح الجريمة السيبرانية.

المبحث الثاني: إجراءات التفتيش في الجريمة السيبرانية

مطلب تمهيدي: ماهية الجريمة السيبرانية

يمكن القول أن الجريمة السيبرانية تشكل تهديدًا كبيرًا وخطيرًا على المستوى العالمي في العصر الحديث. فهي عبارة عن مجموعة متنوعة من الأفعال الإجرامية التي تستخدم التكنولوجيا الرقمية والشبكات الإلكترونية في تنفيذها.

كما أن خطورة الجريمة السيبرانية تتمثل في الأضرار الجسيمة التي تلحق بالأفراد والمؤسسات والدول. وتؤدي إلى فقدان البيانات الحساسة، وتعريض الحق في الحياة الخاصة للخطر وتلحق ضررًا بالسمعة والثقة في الأنظمة الرقمية، كما أنها تعطل البنية التحتية للدول، وتكبد المشاريع الاقتصادية خسائر كبيرة. وتسبب في توقف الخدمات ذات الأهمية مثل النقل؛ المياه؛ الكهرباء، مما يؤثر بصورة أكبر على حياة الأفراد والمجتمعات.

وأن التصدي لهذه الجرائم، يقع على عاتق المؤسسات والأفراد بإتخاذ تدابير أمان قوية، والتعاون مع الجهات الرسمية والقوات الأمنية لمكافحة الجريمة السيبرانية، وزيادة الوعي بأهمية الأمن السيبراني.

فقد تطورت العلوم والمعارف ودخول التكنلوجيا الحديثة شتى مناحي الحياة، مما إدى إلى تطور الظاهرة الإرهابية تطورًا نوعيًا كبيرًا في أساليبها وصورها ووسائلها حيث بات الإرهابيون يستخدمون ما أنتجته ثورة الإنترنت وتكنولوجيا المعلومات لتحقيق أغراضهم الإرهابية، مما أفسح الطريق لظهور الجرائم السيبرانية إلى حيز الوجود.

ويمكننا تعريف الإجرام السيبراني: هو عبارة عن هجمه إلكترونية غرضها تهديد الحكومات والأفراد أو العدوان عليها، سعيًا لتحقيق أهداف سياسية أو دينية أو أيديولوجية، وتنتج عنها آثار تخريبية مدمرة. ويعرف الإجرام السيبراني كذلك بأنه: هجمات غير مشروعة، أو تهديدات بهجمات ضد الحاسبات

أو الشبكات أو المعلومات المخزنة إلكترونيًا، وتوجه من أجل الانتقام أو ابتزاز أو أجبار أو التأثير في الحكومات أو الشعوب أو المجتمع الدولي بأسره لتحقيق أهداف معينة.

واتساقًا مع هذه التعريفات سالفة الذكر يمكننا أن ننتهي إلى تعريف مصطلح الإجرام السيبراني إجرائيًا على أنه:

- نشاط أو فعل هجومي إجرامي متعمد.
- يقوم به فرد أو جماعة أو دولة.
- هو عمل يتم لأغراض سياسية أو دينية أو عرقية.
- يستخدم وسائل التكنولوجيا الحديثة.
- يوقع أضرارًا بالممتلكات العامة أو الخاصة.
- يهدف إلى أدخال الرعب أو الخوف أو الفزع لتحقيق غايات إرهابية.

والإجرام السيبراني بهذا المعنى هو ظاهرة عالمية تشكل إحدى صور الجرائم السيبرانية العابرة للحدود الوطنية تمس على نحو مباشر أمن الدول حيث تستخدم الجماعات الإرهابية الإنترنت لاختراق الحواسيب الآلية للمؤسسات والمرافق الحيوية العسكرية والاقتصادية والثقافية للدولة كالبنوك والبورصات العالمية والمطارات والموانئ وغيرها، والاطلاع على بياناتها المخزونة وتدميرها (عطية،2014، ص10).

خصائص الإجرام السيبراني:

يتسم الإجرام السيبراني بمجموعة من الخصائص الرئيسية التي تميزه عن مفهوم الإرهاب في صورته التقليدية ونشير إلى أهمها:

- جرائم ناعمة: بمعنى عدم استخدام العنف والاستعاضة عنه بأدوات التكنولوجيا الحديثة.
- سهولة الاتصال بين الجناة: وسهولة التنسيق عن بعد فيما بينهم لتنفيذ الجرائم السيبرانية.
- المهارات التقنية: وجود قدرة من المهارة والخبرة بتكنولوجيا المعلومات لدى المجرمين أفرادًا كانوا أم جماعات.
- سهولة التخفي: بمعنى تنوع أساليب العمل لدى العصابات الإجرامية وقدرتها الكبيرة على التخفي.
- جسامة الخسائر: تكون عادة الخسائر جسيمة من حيث الأرواح والممتلكات خاصة في الدول التي تعتمد على تكنولوجيا المعلومات.
- الطبيعة العابرة للحدود: يتميز الإجرام السيبراني بالطابع العابر للحدود حيث يتم التخطيط للجريمة السيبرانية بدولة ويتم التمويل بدولة أخرى، ويتم التنفيذ بدولة ثالثة.
- توافر القصد الجنائي العمدي في الجرائم السيبرانية: تتصف الجرائم السيبرانية بكونها جرائم عمدية ترتكب بعد تدبير وتخطيط مسبقين ولا تقع هذه الجريمة بصورة عفوية أو عن طريق الخطأ.
- وأخيرًا، صعوبة إثباتها لسرعة غياب الدليل بعد ارتكابها: من المعلوم انه المعلومات التي يحملها الإنترنت تكون على شكل رموز مخزنة على وسائط تخزين ممغنطة ولا تقرأ إلا بواسطة الحاسب الآلي وهو ما يجعل الدليل الكتابي أو المقروء أمرًا يصعب بقاءه أو اثباته لأنه الجاني مرتكب هذه الجريمة لا يترك ورائه أي أثر مادي خارجي، الأمر الذي يجعل من الصعب على المحققين اكتشاف الجريمة ومعرفة مرتكبها (حسن،2014، 8).

أسباب انتشار الإجرام السيبراني:

هناك أسباب ودوافع وراء انتشار الإجرام السيبراني وازدياد أنشطته في كافة دول العالم. وفي ما يتعلق بدوافع ارتكاب الجرائم السيبرانية فهي متنوعة ومن أهم أسباب ارتكابها قد تكون سياسية، اقتصادية، أيديولوجية أو شخصية أو انتقاميه ويرجع ذلك إلى جملة اعتبارات نشير إلى أهمها (المرسي،2017، 145):

- أسباب تقنية ترجع إلى ضعف بنية الشبكات المعلوماتية وعدم خصوصيتها وقابليتها للاختراق من خلال الثغرات الموجودة بها.
- صعوبة التعرف على الهوية الإلكترونية للمجرمين حيث يقوم بشن هجومهم (الإلكتروني) بهوية وشخصية وهميه يستتر ورائها للتخفي عن أعين رجال الأمن.
- هناك أسباب اقتصادية أيضًا ترتبط برخص التكلفة وسهولة الاستخدام حيث يكفي بالقيام بهجوم إلكتروني بتوفر حاسوب متطور متصل بشبكة معلوماتية متطورة فقط لا غير.
- أسباب قانونية وتنظيمية ترتبط بضعف البنية التشريعية على المستوى الوطني والدولي. التي تكفل المواجهة الحازمة للجرائم السيبرانية وفي إطار من الرقابة على الاتصالات عبر الإنترنت يضاف إلى ذلك نقص خبرة بعض الأجهزة الأمنية والمحققين وأجهزة الملاحقة المعنية بذلك.
- زيادة كثرة الاعتماد على تكنولوجيا المعلومات في كافة مناحي الحياة المعاصرة بسبب كفاءتها في معالجة البيانات، حيث أصبحت القاعدة التي يرتكز عليها عمل كثير من المرافق الحيوية للدولة مثل المطارات، البنوك، المستشفيات مما يجعلها هدفًا سهلًا للإجرام السيبراني.

دور التشريع الإماراتي في مكافحة الإجرام السيبراني:

اعتمدت دولة الإمارات العربية المتحدة قانون إنشاء وحماية شبكة الاتصالات الصادر عام 2002، والمرسوم بقانون الاتحادي رقم 3 لعام 2003 في شأن تنظيم قطاع الاتصالات وتعديلاته والقانون رقم 5 لعام 2004 حول الأمن المعلوماتي والقانون الاتحادي رقم 1 لعام 2006 بشأن المعاملات والتجارة الإلكترونية والمرسوم بقانون اتحادي رقم 3 لعام 2012 بشأن إنشاء الهيئة الوطنية للأمن الإلكتروني وتعديلاته والمرسوم بقانون اتحادي رقم 5 لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات والقانون الاتحادي رقم 12 لعام 2016 بتعديل مرسوم بقانون اتحادي رقم 5 لعام 2012 في شأن مكافحة جرائم تقنية (1) المعلومات. وقد جرمت المادة 2 (الفقرة 1 من المرسوم بقانون اتحادي رقم 5 لعام 2012 في شأن مكافحة جرائم تقنية المعلومات الدخول بدون تصريح أو بتجاوز حدود التصريح إلى موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات، أو وسيلة تقنية معلومات أو بالبقاء فيه بصورة غير مشروعة. كما فرضت ذات المادة عقوبة الحبس والغرامة التي لا تقل عن مائة ألف درهم ولا تزيد على ثلاثمائة ألف درهم أو بإحدى هاتين العقوبتين على هذا الفعل. وإذا ترتب على الفعل المذكور إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أي بيانات أو معلومات كانت العقوبة الحبس مدة لا تقل عن ستة أشهر، وغرامة لا تقل عن مائة وخمسين ألف درهم ولا تجاوز سبعمائة وخمسين ألف درهم أو بإحدى هاتين العقوبتين، وذلك وفقًا للفقرة 2 من ذات المادة (2) اليوم القوات كذلك، تعاقب المادة 4 من المرسوم بالسجن المؤقت والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز مليون وخمسمائة ألف درهم إذا كان هذا الدخول بقصد الحصول على بيانات حكومية، أو معلومات سرية خاصة بمنشأة مالية، أو تجارية أو اقتصادية. وإذا تعرضت هذه البيانات أو المعلومات للإلغاء أو الحذف أو الإتلاف أو التدمير أو الإفشاء أو التغيير أو النسخ أو النشر أو إعادة النشر، ارتفعت العقوبة إلى السجن مدة لا تقل عن خمس 5 سنوات والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تجاوز 2 مليون درهم وقد اعتبرت المادة 44 من المرسوم الجرائم التالية بالإضافة إلى الجرائم 1. تقديم معلومات غير صحيحة أو غير دقيقة أو مضللة إلى أي منظمات أو مؤسسات أو هيئات أو أي كيانات أخرى باستخدام الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات للإضرار بمصالح الدولة أو الإساءة إلى القوانين السارية في البلاد ويعاقب مرتكب أي من هذه الأفعال بعقوبة السجن المؤبد، كما يعاقب بالعقوبة ذاتها على الترويج للأفعال المذكورة أو 3. إنشاء أو إدارة موقع إلكتروني أو الإشراف عليه أو نشر معلومات على الشبكة المعلوماتية أو وسيلة تقنية معلومات بقصد التحريض على أفعال أو نشر أو بث معلومات أو أخبار أو رسوم كارتونية أو أي صور أخرى من شأنها تعريض المنصوص عليها في المادة 4 والمادة 29 جرائم ماسة بأمن الدولة إذا ارتكبت الحساب أو المصلحة دولة أجنبية أو أي جماعة إرهابية أو مجموعة أو جمعية أو منظمة أو هيئة غير مشروعة سمعتها أو هيبتها أو مكانتها (مادة 38).

وهكذا يمكن القول أن مكافحة الجريمة السيبرانية ذات أهمية قصوى في عصرنا الحاضر بسبب تزايد التفاعل بين البشر والتكنولوجيا الرقمية. وأن هذه الجرائم تشكل تهديدًا جسيمًا للأفراد والمؤسسات والمجتمعات والدول، وبالتالي ضرورة التصدي بشكل جدي وفعال. وفيما يلي أهم أسباب هذه الأهمية:

- توفير حماية للمعلومات الحساسة: وتتضمن الجريمة السيبرانية سرقة واختراق المعلومات الشخصية والمؤسساتية. وأن مكافحة هذه الجرائم تضمن حماية خصوصية للأفراد والمؤسسات والمعلومات الحساسة مثل المعلومات المالية والطبية والعسكرية.
- الحفاظ على الاقتصاد: تعتبر الهجمات السيبرانية التي تتسبب في تحمل الشركات والحكومات خسائر مالية جسيمة وتقلل من فرص النمو الاقتصادي. ان مكافحة الجريمة السيبرانية يساعد في الحفاظ على الاستقرار الاقتصادي.
- ضمان استدامة البنية التحتية: من المعلوم أن البنية التحتية الحيوية مثل (الكهرباء والمياه والنقل) تعتمد على الأنظمة السيبرانية وضد هجمات الجريمة السيبرانية ويمكن أن تسبب في تعطيل هذه الخدمات الحيوية، مما يؤثر على حياة الناس والاقتصاد.
- الأمن القومي: الجريمة السيبرانية يمكن أن تكون أداة للتجسس والتخريب والتأثير على العمليات الحكومية والأمن القومي. لذلك، يجب مكافحتها بفعالية لحماية الدولة والمجتمع.
- تهديد للصحة والسلامة: أن الجرائم السيبرانية يمكن أن تتشمل على الهجمات التي تقع على البنى التحتية مما يعرض حياة الأفراد للخطر.
- الحفاظ على الثقة: تعتبر الثقة في الأنظمة والخدمات الرقمية أمر ضروري وحيوي وأن الجرائم السيبرانية تهدد هذه الثقة، وتجعل المستخدمين يشعرون بالقلق بخصوص أمن معلوماتهم وخصوصياتهم.
- تحقيق العدالة: أن مكافحة الجريمة السيبرانية تساعد على تقديم العدالة ومعاقبة المجرمين السيبرانيين، مما يؤدي إلى إرسال رسالة بأن هذه الأنشطة لا يسمح بها المجتمع.

باختصار، فإن مكافحة الجريمة السيبرانية ضرورة في غاية الأهمية لأجل ضمان الأمن الرقمي واستدامة التنمية الاقتصادية والاجتماعية في عالم يعتمد بشكل متزايد على التكنولوجيا والإنترنت.

المبحث الأول: إجراءات معاينة مسرح الجريمة السيبرانية (الدليل السيبراني)

تمهيد:

تمثل قواعد الإثبات أهمية خاصة إذ إنه حق يتجرد من كل قيمة إذا لم يقم الدليل على الواقعة التي يستند إليها، فالدليل هو عصب الواقعة أو هو النتيجة التي تحققت باستعمال وسائل الإثبات المختلفة أي إنتاج الدليل.

ويقصد بهذا الإثبات، القواعد المتعلقة بالبحث عن الأدلة وإقامتها أمام القضاء وتقديرها من جانبه، فالإثبات هو مجموع الأسباب المنتجة لليقين، وبالتالي فإن الإثبات في المواد الجنائية ما هو إلا كافة الأدلة التي تؤكد وقوع الجريمة، وتحقق حالة اليقين لدى القاضي لإدانة المتهم، أو ترجح حالة الشك لديه فيقضي بالبراءة، أو هو كل ما يؤدي إلى إظهار الحقيقة (الصغير،2015، 475). ويعد كل من المعاينة والتفتيش أحد أهم وسائل جمع الأدلة في مسرح الجريمة السيبرانية.

المطلب الأول: مفهوم معاينة مسرح الجريمة السيبرانية

المعاينة وإن كانت واردة في جميع الجرائم إلا أن هناك بعض الجرائم التي تتضاءل فيها أهمية المعاينة من ذلك جريمة التزوير المعنوي وجريمة السب، فهذه الجرائم تعد المعاينة فيها ليست ذات جدوى، هذا من ناحية، ومن ناحية أخرى فإن معاينة الجريمة التقليدية والاطلاع على مسرح الجريمة فيها يكون ذا أهمية متمثلة في تصوير كيفية وقوع الجريمة وظروف وملابسات ارتكابها وتوفير الأدلة المادية التي يمكن تجميعها عن طريق هذه المعاينة، لكن هذه المعاينة لا تؤدي ذات الدور في كشف غموض الجريمة المعلوماتية وضبط الأشياء التي تفيد في إثبات وقوعها ونسبتها إلى مرتكبها (حجازي،2001، 60).

ويرجع السبب في تضاؤل أهمية المعاينة في الجريمة السيبرانية إلى أن الجريمة التقليدية تجري غالبًا على مسرح الجريمة وتخلف آثارًا مادية تترتب عليها الأدلة الجنائية، وهذا المسرح يعطي المجال أمام سلطة جمع الاستدلالات وسلطة التحقيق الابتدائي في الكشف عن غموض الجريمة والأدلة وذلك عن طريق المعاينة والتحفظ على الآثار المادية التي خلفتها الجريمة، لكن فكرة مسرح الجريمة في الجريمة السيبرانية يتضاءل دورها في الافصاح عن الحقائق المؤدية للأدلة المطلوبة وذلك لسببين:

الأول: أن الجريمة السيبرانية قلما تخلف آثارًا مادية.

الثاني: أن كثيرًا من الأشخاص يردون إلى مسرح الجريمة العادية خلال الفترة من وقت وقوع الجريمة وحتى اكتشافها أو التحقيق فيها وهي فترة قد تكون طويلة نسبيًا، الأمر الذي يعطي فرصة للجاني أو للآخرين أن يضروا أو يتلفوا أو يعبثوا بالآثار المادية للجريمة إن وجدت، الأمر الذي يورث الشك في دلالة الأدلة المستفادة من المعاينة (حجازي، مرجع سابق، 61).

وفي كل الأحوال فإنه عند تلقي البلاغ عن وقوع إحدى الجرائم السيبرانية وبعد التأكد من البيانات الضرورية في البلاغ يتم الانتقال إلى مسرح الجريمة لمعاينته، ومسرح الجريمة الإلكترونية يختلف كما قدمنا عن مسرح الجريمة التقليدية كالقتل والسرقة، والجريمة السيبرانية قد تكون جريمة مستمرة كما في حال الجرائم الاقتصادية -السرقة والاحتيال- وقد يكون مسرحها كالجرائم الأخرى كما في التزوير وإتلاف البرامج وتفجير المباني والمنشآت، ففي حالة الجريمة المستمرة ذات الأهداف الاقتصادية تكون المعاينة هدفها المداهمة وضبط الأدلة على الطبيعة، وفي الحالة الثانية وبعد وقوع الجريمة، فالأمر يتوقف على اعترافات المتهمين متى تم القبض عليهم وكذلك شهادة الشهود والقرائن.

وفي كل الأحوال يتعين مراعاة الإجراءات الآتية عند الانتقال إلى مسرح الجريمة السيبرانية (الصغير، 2012، ص111):

- ضرورة وجود معلومات مسبقة عن مكان الجريمة من حيث عدد الأجهزة المطلوب معاينتها وشبكاتها.
- وجود خريطة توضح الموقع الذي ستتم معاينته، وتفاصيل المبنى أو الطابق موضوع البلاغ، وعدد الأجهزة والخزائن والملفات ويحدد ذلك من خلال مصادر سرية لجهاز الأمن.
- تحديد الأجهزة المحتمل تورطها في الجريمة السيبرانية حتى يتم تحديد كيفية التعامل معها فنيًا قبل المعاينة، سواء من حيث الضبط أو التأمين أو حفظ الأوراق أو المستندات المتداولة.
- تأمين الأجهزة والمعدات التي سيتم الاستعانة بها في عملية المعاينة سواء كانت أجهزة أو برامج صلبة أو لينة.
- إعداد الفريق المتخصص الذي يتولى المعاينة من الخبراء التقنيين ورجال الضبط والأمن.
- إخطار الفريق الذي سيتولى المعاينة قبل تمامها بوقت كافٍ حتى يستعد من الناحية الفنية والعملية، وذلك لكي يضع الخطة المناسبة لضبط أدلة الجريمة الإلكترونية حال معاينتها.
- تحديد البيانات والمهام والاختصاصات المطلوبة من كل عضو من فريق المعاينة على حده، وذلك حتى لا تتداخل الاختصاصات.
- إعداد خطة المعاينة، موضحة بالرسومات مع تمام المراجعة التي تكفل تنفيذها على الوجه الأكمل.
- أن تتم هذه الإجراءات وفق مبدأ المشروعية وفي إطار ما تنص عليه القوانين الجنائية.

- تأمين عدم انقطاع التيار الكهربائي لأن معاينة الأجهزة وما بها من برامج وشبكات وأنظمة تشغيل لا جدوى منها في ظل عدم وجود التيار الكهربائي (حجازي، مرجع سابق، ص316).

وعند معاينة مسرح الجريمة، يرى جانب من الفقه الجنائي، ضرورة وضع عدة ضوابط في معاينة مسرح الجريمة المعلوماتية وهذه الضوابط هي (عبدالمطلب، ص22):

- تحديد أجهزة الحاسب الالي الموجودة في مكان المعاينة، وتحديد مواقعها بأسرع فرصة ممكنة وفي حالة وجود شبكة اتصالات يجب البحث عن خادم الملف وذلك لأجل تعطيل الاتصالات لمنع تخريب الأدلة الموجودة أو محوها، ويراعي تصوير الأجهزة الموجودة وخاصة الأجزاء الخلفية منها.
- ضرورة وضع حراسة كافية على مكان المعاينة، ومراقبة التحركات داخل مسرح الجريمة، بل ورصد الاتصالات الهاتفية من وإلى مكان مسرح الجريمة مع إبطال مفعول أجهزة الهاتف المتحرك التي قد تساعد -عن طريق تقنية معينة- في تدمير أدلة الجريمة الالكترونية متى تم توصيلها بالأجهزة محل المعاينة، وذلك ممكن من الناحية العملية.
- ملاحظة الطريقة المعد بها النظام المعلوماتي السيبراني والآثار التي يخلفها ومعرفة السجلات الالكترونية التي تزود بها شبكة المعلومات لمعرفة موقع الاتصال ونوع الجهاز المتصل عن طريق الدخول إلى النظام أو الموقع أو الدخول معه في حوار وبرتوكولات الاتصال عبر الإنترنت وإن تعلقت الجريمة بهذه الشبكة والتي تعرف اختصارًا (IP) (عبدالمطلب، 2021، ص21).
- يتعين كذلك ملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يمكن تحليل البيانات ومقارنتها والوصول منها إلى دليل عند عرض الأمر على القضاء (حجازي،2002،ص64).
- عدم نقل المواد المعلوماتية خارج مسرح الجريمة السيبرانية إلا بعد التأكد من خلو المحيط الخارجي للحاسب من مجالات القوى المغناطيسية- الممرات المغناطيسية- التي قد تتسبب في محو البيانات، ولن يتأتى ذلك إلا عن طريق خبراء الحاسب الآلي.
- ويرتبط بذلك أن الفريق الذي سيتولى المعاينة، ومن ثم ضبط وتحريز الأدلة -إن وجدت- لا بد وأن يضم اثنين أو أكثر من خبراء الحاسب الآلي، يتولون ضبط وإدخال المعلومات المضبوطة في الحاسب الآلي، وتصنيف الأدلة وتحريزها في صناديق، ووضع العلامات الدالة عليها، ويقوم هذا الفريق كذلك بنقل أجهزة الحاسب الآلي المضبوطة بعد تكملة إجراءات الرسم والتصوير على أن يراعى تنوع خبراء الحاسب الآلي ما بين محققين وآخرين مدربين على التعامل مع الأدلة وكذلك طرق تقييمها (رستم،ص104)، لأجل الحصول على دليل من هذه المعاينة المعلوماتية.
- التحفظ على محتويات سلة المهملات وما فيها من أوراق ممزقة وشرائط واقراص ممغنطة وغير سليمة أو محطمة ورفع البصمات التي قد تكون عليها، وكذلك التحفظ على مستندات الإدخال والمخرجات الورقية لجهاز الحاسب الآلي، قد تكون على صلة بالجريمة السيبرانية (رستم، مرجع سابق، ص104).
- ضرورة قصر المعاينة على الباحثين والمحققين الذين لديهم كفاءة علمية وخبرة فنية في مجال الحاسبات والشبكات واسترجاع المعلومات، وأن يكونوا قد تلقوا تدريبًا جيدًا على ذلك (حجازي، 2009، ص590).

ولكن من الأفضل أن يضم فريق المعاينة أشخاصًا من مأموري الضبط القضائي والمحققين للحصول على الادلة أو تحليل الأدلة القائمة وسؤال الشهود، ويضم كذلك آخرين للرسم والتصوير، وذلك لأجل عمل رسم كروكي لمسرح الجريمة السيبرانية، وتحديد مواقع الأجهزة والملفات والأشخاص، وكذلك أشخاصًا آخرين للتفتيش العملي - في مسرح الجريمة - شرط أن يتم ذلك وفقًا لقانون الإجراءات الجزائية ما لم يوجد قانون خاص يحكم إجراءات التفتيش في الجريمة الالكترونية، ثم أفرادًا هدفهم تأمين مسرح الجريمة الذي تجري معاينته، وضبط المخارج منه والمنافذ إليه (البشرى،2012، ص31).

ونخلص من ذلك إلى أن المعاينة في الجريمة السيبرانية لمسرح الجريمة قد لا تكون مجدية مثل المعاينة لمسرح الجريمة التقليدية، وأنه في حال القيام بها، متى كان مسرح الجريمة يسمح بذلك، فإن ضوابط واحتياطات القيام بها تختلف عن معاينة الجريمة التقليدية، وذلك لاختلاف الجريمة السيبرانية في طبيعتها من الجريمة التقليدية.

ويرى جانب من الفقه الجنائي المعلوماتي أن الفريق الذي سيتولى المعاينة كإجراء تحقيق في الجرائم الإلكترونية، عليه أن يقوم بإعداد خطة لهذا الغرض، هي خطة هجوم واضحة ومفهومة لدى أعضاء الفريق، جميعه على أن تكون الخطة موضحة بالرسومات وتتم مراجعتها مع أعضاء الفريق قبل بدء التحرك مع الأخذ في الاعتبار قاعد السرية والتي تعني الحالة، الرسالة، والتنفيذ، المداخل والمخارج، والاتصالات، وهي ملائمة للأجهزة الأمنية وأجهزة تنفيذ القوانين، فالحالة أو الوضع يعني معرفة حجم القضية التي تقوم بالتحقيق فيها، وعدد المتورطين فيها، أما الرسالة فهي تحديد الهدف من الغارة، والتنفيذ بمعنى كيفية أداء المهمة، أما المداخل والمخارج فإن معرفتها ضرورية وهي تختلف من جريمة إلى أخرى، وتحسب وفقًا لطريقة التحقيق، بينما يأتي عنصر الاتصالات لضمان السرية وسلامة التعاون وتبادل المعلومات أثناء الغارة (البشرى، مرجع سابق، ص368)، أو المعاينة.

المطلب الثاني: الشروط الواجب توافرها لصحة معاينة مسرح الجريمة السيبرانية

لكي تحقق المعاينة الأهداف المرجوة منها في كشف غموض الحادث والتوصل إلى الفاعل لابد من مراعاة الآتي:

- سرعة الانتقال إلى مكان وقوع الجريمة السيبرانية: فور تلقي البلاغ والتأكد من صحة وقوعه على مأمور الضبط القضائي أو عضو النيابة الانتقال بسرعة إلى مكان مسرح الجريمة السيبرانية ومعاينته، ففي سرعة الانتقال فوائد كبيرة منها، ضمان عدم تغيير شكل مسرح الجريمة عن الوضع والحالة التي تركها الجاني عليه، والاستماع إلى أقوال شهود الواقعة دفعة واحدة، وسماع ما يمكن الحصول منه على معلومات أو إيضاحات تفيد في كشف الحقيقة، وتتيح لمأمور الضبط القضائي مواجهة المتهم عند الإنكار بالأدلة المادية في مكان وقوع الجريمة إذا كان المتهم حاضرًا (بوحوش،2010، ص214).
- السيطرة على مكان وقوع الجريمة السيبرانية: بمجرد وصول المحقق لمكان الحادث لمعاينته أن يقوم بالسيطرة عليه وذلك باتباع الإجراءات التالية:
  - حصر الذين تواجدوا بداخل مسرح الجريمة بعد هروب الجاني واكتشاف الواقعة وتدوين كافة بياناتهم وصلتهم بالواقعة وأطرافها.
  - منع تواجد أحد بداخل مسرح الجريمة حتى لا يؤثر ذلك على الآثار والأدلة التي عثر عليها بقصد أو بدون قصد.
  - التأكد من عدم لمس أية آثار أو أدوات بداخل مسرح الجريمة.
  - التحفظ على ما له علاقة بالحادث من أمكنة وأشياء وأشخاص.
  - إخطار الخبير لرفع الآثار التي بمكان الحادث كل وفقًا لاختصاصه.

1. الترتيب والتسلسل في المعاينة:

ينبغي أن تجري المعاينة بصورة مرتبة وبتسلسل ولضمان تحقيق ذلك يجب على المحقق مراعاة اتباع الآتي:

- أن يحدد نقطة البدء في المعاينة وهي ذاتها نقطة الانتهاء أو بمعنى آخر ينتهي من المعاينة.
- أن يبدأ في المعاينة من الأكبر إلى الأصغر بمعنى أن المعاينة تبدأ من منطقة الحادثة إلى العقار محل الحادث إلى الشقة مسرح الجريمة إلى الهدف.
- ألا ينتقل من مكان لآخر إلا بعد تأكده تمامًا من معاينته وعدم تركه أية أشياء به ويعتبر كل جزء يقوم بمعاينته محددًا، وأن يدون ما شاهده من آثار أو الآلات في ذلك الجزء، وإذا وجد آثارًا معينة يضعها في مظروف ويدون عليها نوع الأشياء ومكان العثور عليها.

2. الدقة والعناية الفائقة:

وهذا الشرط يتفق مع الذي قبله، فإن التسلسل والترتيب في المعاينة بالتأكيد يصاحبه دقة وعناية فائقة، وتقتضي الدقة والعناية في مسرح الجريمة الالكترونية اتباع الخطوات التالية (حجازي، مرجع سابق،ص217):

- تحديد تاريخ ووقت الانتقال لإجراء المعاينة.
- إخطار الخبراء الذين يلزم الاستعانة بهم في مسرح الجريمة السيبرانية حسب نوعها ليتداخل كل منهم بوسائله وأساليبه الفنية حسب تخصصهم.
- وصف المنطقة التي بها مسرح الجريمة، ويتم فحصها بحثًا عن الآثار التي توضح كيفية ارتكابها من قبل الجاني، فمثلًا معاينة الأسلاك المتصلة بشبكة الإنترنت، أو معاينة الأسلاك المتصلة بالشبكة الداخلية للمنشأة.
- إذا كان مسرح الجريمة داخل مبنى فيلزم معاينة كافة منافذ الدخول والخروج لبيان مدى سيطرة المتهم على مسرح الجريمة، فإن ذلك يفيد فيما إذا كان محل الجريمة خاضعًا للسيطرة الكاملة للمتهم أم بإمكان أشخاص آخرين الوصول إليه، وبالتالي قد تكون أجهزة الكمبيوتر المستخدمة في ارتكاب الجريمة على المشاع مع آخرين.
- وصف المحتويات فيما هو مرتبط بالجريمة كأجهزة الكمبيوتر والماسح الضوئي والطابعة، والأسطوانات المدمجة وغير ذلك من الأدوات المستخدمة في ارتكاب الجرائم الإلكترونية (رستم، مرجع سابق، ص125).

3- تدوين المعاينة:

المعاينة إجراء من إجراءات التحقيق المهمة، لذا فإنه يسري عليها ما يسري على تلك الإجراءات من توثيق، فالمعاينة يتم تدوينها كتابةً ورسمًا وتصويرًا.

المطلب الثالث: خطوات معاينة مسرح الجريمة السيبرانية وقواعد تحريز الأدلة

سوف نتناول هذا المطلب في فرعين: الأول: خطوات معاينة مسرح الجريمة السيبرانية وفي الفرع الثاني: قواعد ضبط وتحريز الأدلة السيبرانية المتحصلة من مسرح الجريمة وذلك على التوالي.

الفرع الأول: خطوات معاينة مسرح الجريمة السيبرانية

معاينة مسرح الجريمة السيبرانية يقصد به "معاينة الآثار التي يتركها مستخدم الشبكة المعلوماتية أو الإنترنت وتشمل الرسائل المرسلة منه أو التي يستقبلها وكافة الاتصالات التي تمت من خلال الكمبيوتر والشبكة العالمية، وتتم معاينة مسرح الجريمة السيبرانية على مرحلتين:

المرحلة الأولى: إجراءات المعاينة:

تصوير الكمبيوتر وما قد يتصل به من أجهزة بدقة تامة وسائر ملحقاته والأجهزة الطرفية المتصلة به والمحتويات والأوضاع العامة بمكانه مع التركيز بوجه خاص على تصوير الأجزاء الخلفية للحاسب ويراعى هذا تسجيل وقت وتاريخ ومكان أخذ كل صورة (مصطفى، 2010، ص135).

- العناية الفائقة بمعرفة الطريقة التي تم إعداد النظام والآثار الإلكترونية وخاصة السجلات الإلكترونية التي تقوم بتزويد الشبكات المعلوماتية لأجل معرفة مكان الاتصال ونوع الجهاز المستخدم الذي تم من خلاله الولوج إلى النظام أو الموقع.
- مع ملاحظه وإثبات حالة التوصيلات والكابلات المتصلة بجميع مكونات النظام لأجل إجراء عملية المقارنة والتحليل عندما يعرض الأمر لاحقًا على القضاء.
- عدم نقل أي معلومات من مسرح الجريمة قبل إجراء اختبارات للتأكد من خلو المحيط الخارجي لموقع الكمبيوتر من أي مجالات لقوى مغناطيسية يمكن أن تتسبب في محو أو إتلاف البيانات المسجلة.
- الاحاطة بمستندات الإدخال والتحفظ عليها وكذلك المخرجات الورقية لجهاز الكمبيوتر الذي له علاقة بالجريمة لرفع ومضاهاة الأدلة الموجودة فيه من بصمات وغيرها.
- رسم مخطط مفصل للإدارة التي حصلت الجريمة بها معززًا بكشف تفصيلي بالأشخاص المسئولين بها ودور كل شخص منهم.

التحفظ عما قد يوجد بسلة المهملات من الأوراق الملقاة أو الممزقة أو أوراق الكربون المستعملة والأشرطة والأقراص الممغنطة غير السليمة وفحصها ورفع البصمات التي قد تكون لها صلة بالجريمة المرتكبة (مصطفى، مرجع سابق، ص135).

المرحلة الثانية: إجراءات التحفظ:

عندما يصل الفريق إلى مكان الجريمة السيبرانية، ضرورة التأمين وكذلك السيطرة على مسرح الجريمة والبدء في العمل على النحو التالي:

- السيطرة على المناطق المحيطة بمسرح الجريمة وذلك عن طريق إغلاق الطرق والمداخل.
- ضرورة سيطرة رجال الشرطة على المكان الذي تتم به المعاينة من خلال إقامة عدد من نقاط الحراسة كافية لمراقبة التحركات في داخل الدائرة ورصد المكالمات الهاتفية من وإلى مسرح الجريمة مع إبطال أجهزة الهاتف الجوال.
- تأمين موقع ارتكاب الجريمة والسيطرة على جميع أركانه ومنافذه والتحفظ على الأشخاص الموجودين.
- تحديد أجهزة الحاسب الآلي الموجودة في المكان وتحديد مواقعها بأسرع فرصة ممكنة وفي حالة وجود شبكات اتصالات يجب البحث عن خادم الملف File Server لتعطيل حركة الاتصالات.
- يوضع حرس على كافة الأجهزة لأجل ان لا يتمكن أيًا من المتهمين من إتلاف المعلومات من على البعد أو من خلال جهاز آخر داخل المبنى.
- اختيار مكان لمقابلة المتهمين والشهود على أن يكون المكان بعيدًا عن أجهزة الكمبيوتر.
- التحفظ على البيانات محل الجريمة، وكذلك الأدوات التي استخدمت في ارتكابها أو الآثار المتخلفة عنها وتفيد في كشف الحقيقة ويتم استخراج نسخة من المعلومات المضبوطة على الوسائط الخاصة بالجهة التي تتولى التحقيق، مع بقائها تحت تصرفها حتى انتهاء المحكمة من إجراءاتها، ويذهب آخرون إلى ضرورة حفظ صورة أخرى لدى المحضرين المتواجدين في المحكمة، خوفًا من التلف أو ضياع النسخة الأصلية المتواجدة تحت تصرف جهة التحقيق أو المحاكمة (مصطفى، مرجع سابق، ص135).

الفرع الثاني: قواعد ضبط وتحريز الأدلة السيبرانية المتحصلة من مسرح الجريمة

يتمثل الدليل الإلكتروني في الجرائم السيبرانية بصورة عامة في ذبذبات أو نبضات إلكترونية مسجلة على وسائط أو دعائم مادية، وإذا لم يكن المحقق مؤهلًا ومدربًا على التعامل معها ومدركًا لطبيعة النظام الإلكتروني، فقد يغفل أو يهمل دليلًا إلكترونيًا، أو قد يتسبب في إتلافه، وإفساد دلالته، لذا كان تأمين ضبط تلك الأدلة أمرًا مقتضيًا لا مناص منه، وحيال ذلك يمكن اتخاذ بعض الإجراءات الخاصة للحفاظ عليها وصيانتها من العبث ومن أبرزها:

- ضبط وتحريز الدعائم الأصلية للبيانات وعدم الاكتفاء بضبط النسخ، فالدعائم الأصلية هامة جدًا عند عرض الأدلة على المحكمة.
- مراعاة ظروف الحرارة والرطوبة المناسبتين لتخزين الأحراز الإلكترونية.
- التزام القواعد الفنية المتعلقة بنقل الأحراز الإلكترونية والتحوط من المرور بها أو تخزينها على مقربة من محطة إرسال لاسلكي وعدم وضعها في أماكن متربة أو قاعدة لتأثير الأتربة والغبار عليها.
- ضرورة العمل على تأمين البرامج التي تم ضبطها قبل البدء بتشغيلها فنيًا وعمل نسخ احتياطية منها سليمة وكاملة.
- ضرورة أن نميز بين الأدلة الإلكترونية عن غيرها بوضع علامة واضحة مادية خاصة به من قبل جميع من كانت في حيازتهم (إبراهيم، مرجع سابق، ص177).

ونخلص مما سبق، لكي يؤتي إجراء المعاينة ثماره عند القيام به بمعرفة رجال الضبط القضائي والسلطات الأمنية، ضرورة تعليم هؤلاء مبادئ وعلوم الحاسب الآلي وكيفية التعامل مع هذه الأجهزة التي لا غنى عنها في ضبط الجرائم الإلكترونية، بل أصبحت وسيلة ربط قوية وسريعة ما بين وحدات الأمن وبعضها البعض في السيطرة على الموقف الأمني وضبط الجريمة وتحليل عناصرها والحصول على أدلتها.

وقبل أن نختتم هذا الفرع يبقى التساؤل هل يجوز معاقبة الموظفين على إفشاء أسرار المواطنين التي يطلعوا عليها بحكم وظائفهم عبر أجهزة الحاسب أو شبكاته؟

لقد اختلف الفقه المقارن في الإجابة عن هذا التساؤل بين مؤيد ومعارض، ويمكن بلورة هذا الخلاف في اتجاهين رئيسيين هما(هلالي، 2010، ص52):

الاتجاه الأول:

يذهب أصحابه إلى أن نلك ليس من واجب الشاهد، وفقًا للالتزامات التقليدية للشهادة، ففي لوكسمبورغ في بلجيكا ليس الشاهد مجبرًا على التعاون في كل ما يعرفه عند سؤاله أمام المحكمة، وبالتالي من الصعب إجبار المتهم على ان يقدم أية بيانات يجهلها، ولم يدخلها بنفسه هو في ذاكرة الحاسوب حتى وإن كان باستطاعته الوصول إليها نظرًا لمعلوميته بكلمات المرور السرية، وفي حالة تعاون الشاهد على هذا النحو، فإن دوره يكون أقرب إلى الخبرة منه إلى الشهادة، وفي ألمانيا تذهب غالبية الفقه إلى عدم التزام الشاهد بطبع البيانات المخزنة في ذاكرة الحاسوب، على أساس أن الالتزام بأداء الشهادة لا يشمل هذه المهمة، وفي التشريع التركي لا يجوز أبدًا إكراه الشاهد لغرض حمله على الإفصاح عن كلمات المرور السرية، أو كشف الشفرات الخاصة بتشغيل البرامج المتنوعة.

الاتجاه الثاني:

يرى البعض أنه يجب على الشاهد أن يقوم بطباعة ملفات البيانات أو الافصاح عن كلمة المرور أو الشفرة الخاصة بكافة البرامج على اختلاف أنواعها. وهذا ما يراه جانب من الفقهاء الفرنسيين في غياب النص التشريعي يكون الشاهد مكلفًا بالكشف عن كلمات المرور السرية التي يعرفها وشفرات تشغيل البرامج (رستم، 2005، ص117)، ما عدا حالات المحافظة على سر المهنة، فإنه يكون في حل من الالتزام بأداء الشهادة، وفي التشريع الهولندي، يسمح قانون الحاسوب لسلطات التحقيق أن تصدر الأمر للقائم على تشغيل النظام بتقديم كافة المعلومات اللازمة لاختراقه والوصول إلى داخله، كالإفصاح عن كلمات المرور السرية، والشفرات الخاصة في تشغيل البرامج المختلفة أو حل رموز البيانات المشفرة (Soto& Knitt, 2000, p.153).

وفي إطار مشروعية الأدلة السيبرانية نجد أن قانون الإجراءات الجنائية الفرنسي لم يتضمن أي نصوص تتعلق بمبدأ الأمانة أو النزاهة في البحث عن الحقيقة، إلا أن الفقه والقضاء كانا بجانب هذا المبدأ سواء في مجال التنقيب عن الجرائم التقليدية أو في مجال التنقيب في جرائم الحاسوب والإنترنت، كأن يستخدم اعضاء الضبطية القضائية طرقًا معلوماتية في أعمال التنصت على المحادثات الهاتفية، ويشير رأي فقهي فرنسي إلى أن القضاء قد قبل استخدام الوسائل العلمية الحديثة في البحث والتنقيب عن الجرائم تحت تحفظ، وهو أن يتم الحصول على الأدلة الجنائية ومن بينها الأدلة المتحصلة من الإنترنت، بطريقة شرعية ونزيهة، ونفس الشيء نجده في سويسرا وبلجيكا(عوض، 2007،ص85)، وفي بريطانيا، قامت الشرطة بتركيب جهاز تنصت على خط هاتف احدى الشاكيات بناء على موافقتها، وقد أجرت الشاكية عدة مكالمات هاتفية مع الطرف الاخر الذي كانت الشرطة تشك في ارتكابه الجريمة، وقد تم تسجيل المكالمات التي تضمنت موضوعات تدين المتهم، لكن القاضي قام باستبعاد هذه التسجيلات على أساس أنها تمت من خلال حيلة خداعية (بلال، 2009، ص16)، أما في التشريع الهولندي فإذا كانت بيانات الحاسب المسجلة في ملفات الشرطة غير قانونية، فذلك يؤدي إلى نتيجة مؤداها اهمية محو هذه البيانات وعدم استخدامها كدليل جنائي بسبب استبعاد الأدلة غير القانونية(بلال، مرجع، ص17).

وفي اليابان، اصدرت محكمة مقاطعة (KOFV) حكمًا أقرت فيه مشروعية التنصت للبحث عن الدليل، حيث ضرورة التحريات، وإمكانية استخدام الإجراءات في التحريات تكون مأخوذة بعين الاعتبار؛ لكن الفقه الياباني ينظر الى الأدلة الجنائية التي يتم الحصول عليها بطرق وحيل غير مشروعة يجب أن تكون مستبعدة وان كانت تقليدية، أو أدلة حاسب آلي، أو أدلة إنترنت (أحمد، 2008، ص137).

ومن الطرق الغير مشروعة التي تستطيع أن تستخدم في الحصول على الأدلة الناتجة عن الإجرام المعلوماتي: الإكراه المادي والإكراه المعنوي في مقابلة المتهم المعلوماتي لأجل فك شفرة نظام من النظم المعلوماتية، أو الوصول إلى دائرة حل التشفير، أو الوصول إلى ملفات البيانات المخزنة، أو التحريض على ارتكاب جرائم الإرهاب الإلكتروني من قبل أعضاء الضبطية القضائية، كالتحريض على الغش أو التزوير المعلوماتي أو التجسس المعلوماتي، والاستخدام غير المصرح به للحاسب، والتنصت، والمراقبة الالكترونية عن بعد (الصغير، مرجع سابق، ص111).

ومن الطرق التي تعتبر غير مشروعة أيضًا استخدام التدليس أو الغش أو الخداع في الحصول على الأدلة الرقمية (الصغير، مرجع سابق، ص112)، ولقد صادقت لجنة الوزراء التابعة للمجلس الأوروبي في 1981/1/28م على اتفاقية خاصة بحماية الأشخاص في مواجهة مخاطر المعالجة الآلية للبيانات ذات الطبيعة الشخصية، ومن المحاور المهمة التي تناولتها الاتفاقية ضرورة أن تكون البيانات المضبوطة صحيحة وكاملة ودقيقة ومستمدة بطرق مشروعة، ومدة حفظها محدودة بالسنة، وضرورة عدم إفشائها وكذلك عدم استعمالها الا في الأغراض المخصصة لأجل استعمالها، وكذلك يحق للشخص المعني في التعرف والاطلاع على المعلومات المسجلة والتي تتعلق بذلك الشخص، وله حق تصحيحها وتعديلها وابداء رأيه في مناقشتها ومحوها إذا كانت باطلة. ولقد جاء بقانون الشرطة والإثبات الجنائي البريطاني الصادر لعام 1984م، بضرورة تحديد الشروط المتطلب توافرها ووجودها في مخرجات الحاسوب حتى تقبل أمام المحكمة، واشتمل هذا القانون على عدة توجهات في كيفية تقدير قيم أو وزن البيان المستخرج عن طريق الحاسوب، فأوصت

المادة (11) منه (Bevan & Lidstone, 2005, p.497)، بمراعاة كل الظروف عند تقييم البيانات الصادرة عن الحاسوب المقبولة في الإثبات طبقاً للمادة (69) من القانون نفسه، وبوجه خاص ضرورة النظر في موضوع (المعاصرة) ما إذا كانت المعلومات المتعلقة بقرار قد تم رفد الحاسوب بها في وقت معاصر (أي ملازم) لهذا الأمر أم لا، وأيضًا مسألة ما إذا كان أي أحد من المتصلين على أي نحو بإخراج البيانات من الحاسوب لديه دافع بإخفاء الوقائع أو تشويهها، وقد نصت المادة (69) من قانون الشرطة والإثبات الإنجليزي على ثلاثة شروط أساسية لقبول الدليل الرقمي أمام القضاء الجنائي، هي:

- يجب ألا يوجد أساس معقول للاعتقاد أن البيان غير صحيح أو غير دقيق، بسبب الاستعمال غير الملائم للظروف، أو للغرض الذي يستخدم من أجله الحاسب الآلي.
- يجب التأكد من أن جميع المكونات المادية للحاسب كانت تعمل بدقة، وعلى نحو متوافق كما ينبغي.
- يجب أن تخضع الشروط المحددة (التي تدخل في متطلبات القبول) المتعلقة بالموضوع لتقدير المحكمة المختصة.

المبحث الثاني: إجراءات التفتيش في الجريمة السيبرانية

تفرض الطبيعة المعنوية للمعلومات قواعد خاصة للتفتيش، لأن قواعد التفتيش التقليدية قد قننت لضبط الأشياء المادية، فضبط المعلومات يختلف عن ضبط الأشياء المادية كالمخدرات والأسلحة ونحو ذلك، مما يوجب إيجاد وسائل تقنية خاصة بالمعلومات للحفاظ عليها من كل عبث يمكن أن يلحق بها (يوسف، ص85).

المطلب الأول: محل التفتيش في الجريمة السيبرانية وإجراءات الضبط

أكد المجلس الأوربي سنة 1995 في مجال مكافحة الجرائم السيبرانية في التوصية رقم 13 (95) R على أنه يتعين مراجعة القوانين في مجال الإجراءات الجنائية، للسماح باعتراض الرسائل الإلكترونية وتجميع البيانات المتعلقة بتداول المعلومات في حالة التحقيقات المتعلقة بجريمة من الجرائم الخطيرة الماسة بسرية أو بسلامة الاتصالات أو بأنظمة الكمبيوتر، وأن يسمح القانون لسلطات التحقيق والاستدلال أن يتزودوا بالوسائل الحديثة التي تمكنهم من تجميع المعلومات الضرورية لتحرياتهم وتحقيقاتهم، وأن يتم التحفظ على هذه المعلومات وصيانتها بطريقة مناسبة، ولذلك أصبحت التشريعات الحديثة تجيز تفتيش الأجهزة الإلكترونية لضبط المعلومات المتواجدة فيها والتي تفيد في كشف الحقيقة (أبو الوفا، 2009، ص81).

وطبقًا للمادة (19/)1 من اتفاقية بودابست (بودابست، 2001)، تلتزم الدول الأطراف بتخويل السلطات المختصة، صلاحية التفتيش والولوج إلى البيانات المعلوماتية التي تم احتواؤها، سواء في داخل النظام المعلوماتي أو على دعامة مستقلة، وكذلك تفتيش المكونات المتصلة بالنظام، كما في حالة الحاسب الآلي المحمول والطابعة وأجهزة التخزين المتصلة، وإذا كانت البيانات مخزنة ماديًا في نظام آخر أو في جهاز تخزين آخر، فإنه يمكن الوصول إليها وضبطها من خلال النظام المعلوماتي مع النظم المعلوماتية الأخرى.

وطبقًا للفقرة الثانية من المادة 19 من اتفاقية بودابست فإن للجهات المختصة سلطة توسيع نطاق التفتيش، ليشمل نطاقًا معلوماتيًا آخر أو جزءًا منه، بناء على أسباب معقولة تدعو للاعتقاد بأن البيانات المطلوب ضبطها مخزنة في هذا النظام المعلوماتي.

كما تنص المادة (4/19) من هذه الاتفاقية، على أن لكل دولة طرف من حقها أن تسن من القوانين ما هو ضروري، لتمكين السلطات المختصة أن تقوم بالتفتيش أو الدخول إلى:

- نظام الكمبيوتر أو جزء منه أو المعلومات المخزنة به.
- الوسائط التي يتم تضمين معلومات الكمبيوتر بها، مادامت مخزنة في إقليمها.

نطاق الضبط المعلوماتي:

طبقًا للفقرة الثالثة من المادة (19) من اتفاقية بودابست فإن الضبط يشمل الأجزاء المادية للحاسب الآلي ودعامات التخزين المعلوماتية، خاصة عندما لا يمكن الحصول على نسخة من البيانات أو المعلومات، وكذلك ضبط البرامج الضرورية من أجل الولوج إلى البيانات وضبطها (أبو وفا، مرجع سابق، ص82).

إجراءات ضبط وتفتيش أنظمة الحاسوب والشبكات:

لابد من إصدار إذن من النيابة العامة تجيز تفتيش أنظمة الحاسوب، شريطة أن يتضمن الإذن تحديد النظام محل التفتيش بدقة وعنوان شخص المتهم واسمه وصفته، وتحديد وسائل التفتيش والجهاز الذي سيقوم به، والأشياء التي يتم البحث عنها ومنحهم الصلاحية لدخول نظام الحاسوب وضبط ما يحتويه من بيانات ومعلومات. وعلى الأجهزة التي تقوم بالضبط معرفة كيفية التعامل مع الأدلة بطريقة فنية صحيحة لتلافي إتلافها أو محوها والمحافظة عليها، كما ينبغي تشجيع المجني عليهم في الجرائم السيبرانية بصفة عامة والجرائم التي تقع على بيانات الحاسوب على وجه الخصوص، بالإبلاغ عن هذه الجرائم مع تقرير العقوبات الرادعة للأشخاص الذين يعملون على نشر هذه الجرائم بقصد هز الثقة في الجهات المجني عليها، واتباع القواعد الفنية اللازمة عند تحرير البيانات المضبوطة وتأمينها من الاتلاف (الحلبي، 2017، ص177)، ومن هذه القواعد الفنية ما يلي:

- أخذ نسخة احتياطية عن الجهاز والعمل عليها لضمان عدم المساس بالدليل الأصلي، والتعامل مع النظام من قبل أشخاص متخصصين بعلوم الحاسب.
- عدم تنفيذ البرامج على حاسوب مسرح الجريمة خوفًا من اتلاف الأدلة الموجودة عليه أو محو الذاكرة أو الملفات، وعدم السماح للمشتبه به بالتعامل مع حاسوب مسرح الجريمة.
- إعداد نسخة احتياطية عن وسائط تخزين المعلومات الموجودة في مسرح الجريمة.
- توثيق جميع أنشطة التحقيق في محضر كمحاضر الشرطة كل ما يفعله المحقق بالوقت والتاريخ ومعرفة ماهية المعلومات المحفوظة واستخدام التشفير وعمل نسخة احتياطية آمنة.
- تخزين دليل الحاسوب في أماكن آمنة غير معرضة للمجالات الكهرومغناطيسية والكهرباء الساكنة والغبار(الحلبي، 2017، ص178).

المطلب الثاني: شروط إذن التفتيش في الجريمة السيبرانية

من المستقر عليه في التشريعات المقارنة عدم جواز تفتيش جهاز الكمبيوتر إلا بناءً على إذن وفقًا للأصل العام، ويلزم توافر شروط معينة لصحة الإذن بالتفتيش، وهي: 1/ أن يكون هناك اتهام موجه بالفعل، 2/ أن تكون الجريمة على درجة معينة من الخطورة، 3/ وشرط جدية التحريات، 4/ وشرط التحديد في الإذن. حيث يعتبر تنفيذ الإذن مخلًا بشرط التحديد، إذا قام رجل الضبط القضائي بضبط الجهاز مع أن الإذن كان لضبط المعلومات، بينما لا يعتبر الإذن مخلًا بشرط التحديد أن ينص على ضبط وتفتيش جهاز الكمبيوتر والدسكات الممغنطة، وكل البرامج التي يمكن أن تحتوي على أدلة تفيد في كشف الحقيقة. ولذا يكفي لصحة الإذن بالتفتيش والضبط في الجريمة السيبرانية أن يقتصر هذا الإذن على ذكر ضبط جهاز الكمبيوتر الخاص بالمتهم، دون تحديد أكثر من ذلك، ولما كان الإذن الصادر بتفتيش المنزل يمتد إلى ملحقاته، فإنه إذا صدر إذن بتفتيش جهاز كمبيوتر، فإن هذا التفتيش يمتد إلى الديسكات والأقراص الممغنطة والطابعة باعتبارها من ملحقات الجهاز، بشرط أن تكون متواجدة على مقربة من هذا الجهاز محل التفيش، ويجوز أن يشمل الإذن بالتفيش البحث عن معلومات في الكمبيوتر تتعلق بجريمة من الجرائم، ويستوي أن تكون هذه المعلومات في أي شكل كان، سواء إلكترونيًا أو مغناطيسيًا في صورة ديسك أو اسطوانة أو مسجلة على الهارد ديسك أو في شكل أوراق تم طبعها بناء على ذلك (عطا الله، 2007، ص384).

التفتيش في النظم الإلكترونية في بعض التشريعات:

يتنازع الفقه المقارن في اتجاهان، بصدد مدى اعتبار النفاذ أو الولوج إلى النظم الإلكترونية نوعًا من التفتيش، وذلك كما يلي:

الاتجاه الأول: من الدول التي قامت بسن تشريعات جزائية حديثة قادرة على مواجهة التقنية الإجرامية التي صاحبت ظهور الحاسب الآلي وشبكة الإنترنت وأفردت جانبًا كبيرًا من تلك القوانين والتشريعات لبحث مسألة التفتيش والضبط هي المملكة المتحدة وذلك من خلال قانون إساءة استخدام الحاسب الآلي، إذ نص على إجراءات تفتيش نظم الحاسب الآلي في جرائم الولوج غير المصرح به على أنظمة الحاسب الآلي، والتعديل غير المصرح به على أنظمة الحاسب الآلي بدون إذن، طالما كان هدف الولوج ارتكاب أفعال غير مشروعة عن قصد. أما إذا كان الولوج مجردًا، دون نية لارتكاب أفعال غير مشروعة، فإن التفتيش ممكن ولو بدون إذن قضائي (رستم، مرجع سابق، ص67).

وإلى جانب المملكة المتحدة، هناك الولايات المتحدة الأمريكية، وذلك من خلال القوانين الإجرائية الفيدرالية بشأن جرائم الكمبيوتر، إذ نظمت إجراء التفتيش والضبط في بيئة الحاسب الآلي في القسم 42USC 2000، وكذلك فرنسا من خلال الاتفاقية الأوروبية لجرائم الإنترنت وذلك في المادة (19) من اتفاقية بودابست المشار إليها سابقًا (Misuse, 2009, p.46).

الاتجاه الثاني: ويستند أنصار هذا الاتجاه إلى عمومية نصوص التفتيش للتوسع في تفسيرها من أجل مد حكمها إلى البيانات المخزنة آليًا في الأنظمة الإلكترونية، ونموذج هذا الاتجاه يمكن رصده في محيط الفقه الكندي، عندما توسع في تفسير نص المادة (487) عقوبات كندي إلى حد يسمح بتفتيش وضبط بيانات الحاسب غير المحسوسة، وإن كان في الحقيقة وحتى الآن يتم ضبط الركيزة أو الوعاء المادي للبيانات كالأقراص والأسطوانات الممغنطة. ومن التشريعات أيضًا التي نصت صراحة على أن التفتيش يتم بالنسبة لجميع أنظمة الحاسب الآلي، ومثال ذلك قانون إساءة استخدام الحاسب الالي في إنجلترا الصادر في سنة 1990م حيث نص على أن إجراءات التفتيش تشمل أنظمة الحاسب الآلي (Grabosky, 2006, p.112).

وهناك تشريعات أخرى قد أجازت تفتيش أي شيء أو اتخاذ أي إجراء يكون لازمًا لجمع أدلة الجريمة، وعلى ضوء ذلك، فإن تفتيش المكونات المعنوية للحاسبات الآلية يدخل في عداد الأشياء التي جاء النص عليها بصورة عامة دون تقييد؛ وكمثال لهذه التشريعات: المادة (251) من قانون الإجراءات الجنائي اليوناني التي تجيز لسلطة التحقيق أن تتخذ أي إجراء أو شيء يكون لازمًا لجمع الدليل، ويفسر الفقه اليوناني عبار (أي شيء) بأنها تشمل جميع بيانات الحاسب الآلي، سواء كانت هذه البيانات مخزنة في حاملتها أو كانت معالجة آليًا في الذاكر الداخلية (Misha, 2011, p.214).

وفي مقام الموائمة بين الاتجاهين، يري البعض أن التشكك في الطبيعة المادية للبيانات الإلكترونية على النحو الذي حدا بالاتجاهين السابقين إلى محاولة إزالته أو تجنبه قد لا يكون له ما يسوغه، ذلك أن تمييزًا مهمًا لأسباب تكنولوجية وقانونية يجب أن يقام -كما يرى بعض الفقهاء- بين المعلومات من جهة، والبيانات المعالجة إلكترونيًا من جهة ثانية. فأولهما ليس شيئًا ماديًا وإنما هو عملية أو علاقة، تقوم بين ذهن بشري وبعض أنواع المثيرات، وهي مع تجسدها ماديًا في وعاء أو ركيزة تحتويها تنتقل إلى الغير بواسطتها من طبيعة معنوية مؤكدة ومن ثم فلا سبيل لأن يرد عليها تفتيش أو ضبط. أما البيانات المعالجة

إلكترونيًا فهي نبضات أو ذبذبات إلكترونية وإشارات أو موجات كهرومغناطيسية قابلة لأن تسجل وتخزن على وسائط معينة، ويمكن نقلها وبثها وحجبها واستغلالها وإعادة إنتاجها، كما يمكن كذلك تقديرها كميًا من حيث المبدأ وقياسها، فهي ليست إذًا شيئًا معنويًا كالحقوق والآراء والأفكار، بل هي شيء له في العالم الخارجي المحسوس وجود مادي، أي أنها على ما وصفتها بحق محكمة جنح بروكسل، أشياء محسوسة ومادية ومن ثم يصدق قانونًا أن يرد التفتيش والضبط عليها. وعلى هذا الأساس، يعتبر تفتيش نظام المعلومات الحاسب ووسائط وأوعية حفظ وتخزين البيانات المعالجة إلكترونيًا، إجراء يندرج ضمن التفتيش بمعناه القانوني، وبالتالي يخضع لأحكامه، ومنها الشروط الواجب توافرها فيه، مع نوع من الخصوصية تتماشى مع نوع الجريمة المراد جمع الأدلة بشأنها وكذا البيئة التي يتعامل معها مأمور الضبط القضائي القائم بذلك الإجراء (رستم، مرجع سابق،ص69).

جواز تفتيش جهاز الكمبيوتر بدون إذن في حالات استثنائية:

يجوز التفتيش دون إذن في حالات استثنائية، وعندئذ يكون التفتيش صحيحًا، ومن هذه الاستثناءات في مجال المعلومات في كثير من التشريعات ما يلي: 1- الرضاء، 2- التفتيش على إثر الضبط الصحيح 3- حالة الضرورة 4 – حالة التلبس عند وجود الكمبيوتر خارج السكن 5 - التفتيش في حالة ضبط الأشياء المطلوبة 6- تفتيش شبكة الإنترنت.

التزام مزودي الخدمات بتقديم المساعدة اللازمة لإتمام التفتيش والضبط:

تتجه التشريعات إلى إلزام مزودي الخدمات بالتعاون مع سلطات التحقيق ورجال الضبط القضائي لإتمام عملية الضبط والتفتيش بنجاح، لأنه بدون هذا التعاون ستبقى السلطات المختصة بالتفتيش والضبط فترة طويلة من الوقت في المواقع المراد تفتيشها عبر النظام المعلوماتي، وهذا يمثل عبئًا اقتصاديًا بالنسبة للشركات، وكذلك للمشتركين الذين يجدون أنفسهم في حالة استحالة الوصول إلى البيانات أثناء عملية التفتيش. وطبقًا لنص التوصية رقم (13/95) الصادرة عن المجلس الأوربي، فإنه يتعين أن يفرض التزام على مزودي الخدمات الذين يقدمون خدمات الاتصالات اللاسلكية للجمهور، إما من خلال شبكة عامة، وإما من خلال شبكة خاصة، أن يقدموا لسلطة التحقيق المعلومات اللازمة لتحديد هوية مستعمل الشبكة (أبو الوفا، مرجع سابق،ص83)، كما فرضت الاتفاقية الأوربية لجرائم الإنترنت (اتفاقية بودابست) التزمًا على مزودي الخدمات بالتعاون مع جهات التحقيق، فقد نصت المادة (20) من القسم الخامس، على أن الدول الأعضاء من حقها أن تلزم مزود الخدمات - في حدود ما تسمح به وسائله الفنية المتاحة - أن يقوم بتجميع أو تسجيل البيانات بالوسائل الفنية المناسبة، وأن يتعاون وأن يساعد السلطة المختصة في تجميع وتسجيل البيانات المتعلقة بحركة التداول والتي تجري بطريق الكمبيوتر. كما أن هذا التعاون يكون واجبًا في مرحلة المحاكمة، فيجوز للمحكمة أن تصدر أمرًا لمزود الخدمات أن يقدم المعلومات اللازمة لتحديد هوية المشتركين في الاتصالات الالكترونية، أو الذين قاموا بإنشاء موقع معين على الإنترنت، وذلك في المواد المدنية والجنائية. وتلزم الاتفاقية مزودي الخدمات بأن يحتفظوا بسرية الإجراءات القانونية التي تتخذها السلطات المختصة. والمعلومات التي يمكن إلزام مزودي الخدمات بتقديمها، هي المعلومات الضرورية التي تسمح بتطبيق إجراء التفتيش والضبط بنجاح، وايجاد طريقة مشابهة للدخول والحصول على البيانات، كأن يعلق الاتصال بكلمة مرور أو إجراء أمني آخر. وقد تناولت الفقرة الخامسة من المادة (19) من اتفاقية بودابست، مدى إمكانية إخطار الأطراف المعنية بإجراء التفتيش المعلوماتي، حيث يعد هذا الإخطار عنصرًا جوهريًا في اجراء التفتيش، لأنه يسمح بإقامة تفرقة بين البحث عن بيانات معلوماتية مخزنة تدخل في إطار التفتيش، والذي لا يُعد إجراءً سريًا، ولذلك فإن الرأي الراجح هو عدم الالتزام بالإخطار، وبين اعتراض البيانات في فترد نقلها، والذي يُعد إجراءً سريًا (عطا الله، مرجع سابق،ص386)، وتجميع البيانات المتعلقة بالمرور يعد إجراءً مهمًا للتنقيب والتحري والبحث عن الجرائم، فتجميع بيانات المرور المتعلقة بالاتصالات المعلوماتية، وخاصة في حالة البث غير المشروع للمواد الإباحية، بالدخول غير القانوني لنظام معلوماتي، وإعاقة حسن سير أداء وظيفة نظام معلوماتي، أو الاعتداء على سلامه البيانات يمكن من خلالها، يكون من الضروري لكشف هذه الجرائم، تحديد ما إذا كانت الجريمة مرتكبة من خلال شبكة الإنترنت، وتتبع مسار الاتصالات بين الضحية وفاعل الجريمة، كما تسمح هذه التقنية للتنقيب والتحري بعمل مقارنات بين ساعة وتاريخ ومصدر اتصالات المشتبه فيه وساعة التدخلات غير القانونية في نظم الضحايا، وهوية الضحايا الآخرين، وتحديد المساهمين الآخرين في ارتكاب الجريمة

المطلب الثالث: قواعد تحريز المضبوطات في الجرائم السيبرانية وتأمينها فنيًا

يجب على سلطات التفتيش والضبط في الجرائم السيبرانية المحافظة على البيانات المنسوخة أو المرفوعة، وذلك بالتحفظ عليها في الحالة التي تم العثور عليها لحظة الضبط، وذلك بمراعاة ما يلي:

أولًا: ضبط الدعائم الأصلية للبيانات وعدم الاقتصار على ضبط نسخها:

يجب أن يرد الضبط على الدعائم الأصلية للبيانات، لأن الاكتفاء بضبط نسخ من دعائم البينات المطلوبة وترك دعائمها الأصلية لدى من يحوزها، من شأنه صعوبة إثبات صحة وسلامة النسخة المتحصل عليها، مما يضر بسير التحقيق الجنائي، حيث لن تتمكن السلطات المختصة من استخراج نسخ منها، كي تتمكن من استمرار نشاطها (أبو الوفا، مرجع سابق،ص85).

ثانيًا: مراعاة ظروف الحرارة والرطوبة المناسبة لتخزين الأحراز المعلوماتية:

يراعى في تخزين الاقراص والأشرطة الممغنطة المحرزة، أن تتراوح درجة الحرارة داخلها بين 4-34 درجة مئوية، وأن تكون نسبة الرطوبة بين 20% إلى 80% وبذلك يمكن أن تصل مدة التخزين لهذه الأقراص والأشرطة إلى ثلاث سنوات.

ثالثًا: تأمين نقل الأحراز المعلوماتية وحملها:

كي لا تتعرض الأحراز المعلوماتية أثناء نقلها أو حملها لصدمات متفاوتة قد تؤدي إلى اتلاف كلي أو جزئي لمحتوياتها، فإنه يجب التحرز من المرور بها أو تخزينها على مقربة من محطة إرسال لاسلكي، وكذلك عدم وضعها في أماكن مترية لتأثرها بالغبار والأتربة.

رابعًا: تأمين البرامج المضبوطة قبل تشغيلها:

وذلك بعمل نسخ سليمة وكاملة منها، كتأمين فني لها قبل تلفها.

خامسًا: أحكام التسلسل الإجرائي للضبط:

وذلك ببيان تسلسل الإجراءات التي مرت بها البيانات المعلوماتية المضبوطة منذ ضبطها حتى عرضها على القضاء، بذكر اسم من تولى إعداد وتجهيز دعائم البيانات (الأشرطة الممغنطة والأقراص وغيرها) وكذلك من تولى عملية التسجيل...إلخ (أبو الوفا، مرجع سابق،ص85).

سادسًا: تمييز المادة المضبوطة:

ويكون ذلك بوضع علامة مادية مميزة من قبل من كانت في حيازته، فعند نقل البيانات المخزنة داخل الحاسب الآلي إلى أقراص أو أشرطة ممغنطة، يجب على المحقق ومشغل النظام أن يسجل كل منهما اسمه وبياناته التعريفية، على كل من اسطوانة الحاسب والأقراص أو الأشرطة ذاتها، ووضعها في علب مغلقة وتحريزها.

وطبقًا لنص المادة (116) من الكتاب الثاني من اتفاقية بودابست، فإنه لكل دولة طرف في الاتفاقية أن تتخذ ما تراه مناسبًا للحفاظ على المعلومات على وجه الاستعجال، إذا كان يُخشى فقدان تلك المعلومات أو العبث بها، كما أن لها أن تتخذ من الوسائل ما يُلزم الشخص الذي لديه البيانات المخزنة المطلوبة في حيازته أو تحت سيطرته أن يحافظ عليها، وأن يتخذ كل ما من شأنه المحافظة على سلامتها للفترة الضرورية من الوقت، بما لا يزيد على 90 يومًا، لكي يُمكن السلطات المختصة من تقديمها، وللدولة أن تحدد الميعاد بإجراء جديد (م 16 /2 من الكتاب الثاني) من اتفاقية بودابست، ويتم اتخاذ هذه الإجراءات التحفظية حتى ولو أسهم واحد أو اكثر من مزودي الخدمات في نقل تلك الاتصالات (م 17 من الكتاب الثاني). وطبقًا للمادة (19) من القسم الرابع من هذه الاتفاقية، فإنه من سلطة كل دولة طرف في الاتفاقية أن تتخذ الإجراءات التالية: أن تضبط نظام الكمبيوتر أو جزءًا منه أو المعلومات المخزنة على أي وسيط من وسائط التخزين الخاصة بالكمبيوتر، وأن نحافظ على سلامة تلك المعلومات المخزنة. وقد نصت المادة (1/17) من قانون الأمن الداخلي الفرنسي رقم 239 لسنة 2003، على الإجراءات الواجب اتباعها عند قيام رجال الضبط القضائي بتفتيش النظام المعلوماتي، وأخذ نسخ بالبيانات في أحراز مختومة بالشمع الأحمر، ويلزم بعد ذلك ضرورة مراعاة الجهات القائمة على إجراءات الضبط والتحقيق والمحاكمة، وأن تتوافر في الخبير الذي تستعين به في تعاملها مع الجرائم المعلوماتية، الإمكانيات والقدرات العلمية والفنية في مجال التخصص الدقيق لموضوع الخبرة، بحصوله على درجة علمية في هذا التخصص الدقيق، وأن تتوافر لديه الممارسة العملية التي تسمح له باكتساب كفاءة فنية عالية (أبو الوفا، مرجع سابق،ص87).

المطلب الرابع: مدى تمتع الدليل السيبراني بالحجية أمام القضاء الجزائي

إن مجـرد الحصول على الدليل السيبراني (الرقمي) وتقديمه للقضاء لا يكفي لاعتماده كدليل للإدانة، إذ الطبيعة الفنية الخاصة للدليل الرقمي تمكن من العبث بمضمونه على نحـو يحرف الحقيقة دون أن يكون في قدرة غير المتخصص إدراك ذلك العبث (فرج، مرجع سابق،ص77)، فضلًا عن ذلك فإن نسبة الخطأ في إجراءات الحصول على دليل صادق في الإخبار عن الحقيقة تبدو عالية في مثل هذا النوع من الأدلة السيبرانية، ولذلك تثور فكرة الشك في مصداقيتها كأدلة للإثبات الجنائي، فهل من شأن ذلك استبعاد الدليل الرقمي (السيبراني) من دائرة أدلة الإثبات الجنائي لتعارضه وقرينة البراءة؟ (حجازي، مرجع سابق،ص82).

في ظل النظم القانونية التي تعتمد النظام اللاتيني في الإثبات، فإن القاضي يملك سلطة واسعة في تقييم الدليل من حيث قيمته التضليلية فللقاضي قبول الدليل أو رفضه وهو يعتمد في ذلك على مدى اقتناعه الشخصي وقناعته الوجدانية بذلك الدليل.

ثم إن سلطة القاضي الجزائي في تقدير الدليل لا يمكن أن نتوسع في شأنها بحيث يقال إن هذه السلطة تمتد لتشمل الأدلة العلمية، فالقاضي بثقافته القانونية لا يمكنه إدراك الحقائق المتعلقة بأصالة الدليل السيبراني، فضلًا عن ذلك فإن هذا الدليل يتمتع من حيث قوته التدليلية بقيمة ثبوتية قد تصل إلى حد اليقين، فهذا هو شأن الأدلة السيبرانية عمومًا، فالدليل السيبراني من حيث تدليله على الواقع توافر فيه شروط اليقين، مما لا يمكن معه القبول بممارسة القاضي لسلطته في التأكد من ثبوت تلك الوقائع التي يعبر عنها ذلك الدليل، ولكن هذا لا يناقض ما سبق أن قدمناه من أن الدليل السيبراني هو موضع شك من حيث سلامته من العبث من ناحية وصحة الإجراءات المتبعة في الحصول عليه من ناحية اخرى، حيث يشكك في سلامة الدليل السيبراني من ناحيتين:

الناحية الأولى: الدليل السيبراني من الممكن خضوعه للعبث للخروج به على نحو يخالف الحقيقة، ومن ثم فقد يقدم هذا الدليل معبرًا عن واقعة معينة صنع أساساً لأجل التعبير عنها خلافًا للحقيقة، وذلك دون أن يكون في استطاعة غير المتخصص إدراك ذلك العبث، على نحو يمكن معه القول إن ذلك قد أصبح هو الشأن في النظر لسائر الأدلة السيبرانية التي قد تقدم للقضاء، فالتقنية الحديثة تمكن من العبث بالدليل السيبراني بسهولة ويسر بحيث يظهر وكأنه نسخة أصلية في تعبيرها عن الحقيقة (فرج، مرجع سابق،ص78).

الناحية الثانية: وإن كانت نسبة الخطأ الفني في الحصول على الدليل السيبراني نادرة للغاية، إلا أنها تظل ممكنة، ويرجع الخطأ في الحصول على الدليل السيبراني لسببين (عبدالمطلب، مرجع سابق،ص253):

الأول: الخطأ في استخدام الأداة المناسبة في الحصول على الدليل السيبراني، ويرجع ذلك للخلل في الشفرة المستخدمة أو بسبب استخدام مواصفات خاطئة.

الثاني: الخطأ في استخلاص الدليل، ويرجع ذلك إلى اتخاذ قرارات لاستخدام أداة تقل نسبة صوابها عن 100% ويحدث هذا غالبًا بسبب وسائل اختزال البيانات أو بسبب معالجة البيانات بطريقة تختلف عن الطريقة الأصلية التي تم تقييمها.

ومن ذلك فإننا نخلص إلى أن الشك في الدليل السيبراني (الرقمي) لا يتعلق بمضمونه كدليل، وإنما بعوامل مستقلة عنه، ولكنها تؤثر في مصداقيته، ولكن هل يمكن التثبت من سلامة الدليل السيبراني من حيث العيوب؟ وبكلمة أوضح هل من الممكن أن يضفى على الدليل الرقمي اليقين من خلال إخضاعه للتقييم الفني الذي يمكن من تفادي تلك العيوب التي تشوبه وما موقف القاضي الجزائي من هذا الدليل إذا ما خضع لمثل ذلك التقييم؟

مثلما يخضع هذا النوع من الأدلة لقواعد معينة تحكم طرق الحصول عليه، فإنه كذلك يخضع لقواعد أخرى للحكم على قيمته التدليلية، وذلك يرجع للطبيعية الفنية لهذا الدليل، وبناء عليه فهناك وسائل فنية من طبيعة هذا الدليل تمكن من فحصه للتأكد من سلامته وصحة الإجراءات المتبعة في الحصول عليه، وسوف نحاول فيما يلي تناول بعض هذه الوسائل(عبدالمطلب، مرجع سابق،ص254).

أهم الوسائل والطرق في تقييم الدليل السيبراني:

سوف نتناول وسائل تقييم الدليل السيبراني من خلال مدى سلامته من العبث، ثم وسائل تقييمه من خلال مدى سلامة الإجراءات المتبعة للحصول عليه من الناحية الفنية وذلك على النحو التالي:

أولًا: تقييم الدليل من خلال مدى سلامته من العبث:

يمكن التأكد من سلامة الدليل السيبراني من العبث بعدة وسائل نذكر منها:

- يلعب علم الكمبيوتر دورًا مهمًا في تقديم المعلومات الفنية التي تساهم في فهم مضمون الدليل السيبراني(عبدالمطلب، 2000)، وهذه الوسائل يستعان بها في كشف مدى التلاعب بمضمون هذا الدليل، وتعد وسيلة التحليل التناظري الرقمي من الوسائل المهمة للكشف عن مدى دقة ومصداقية الدليل السيبراني، ومن خلالها تتم مقارنة الدليل الرقمي المقدم للقضاء بالأصل المدرج بالآدلة السيبرانية (الرقمية)، ومن خلال ذلك يتم التأكد من مدى وقوع عبث في النسخة المستخرجة أم لا(أبو الوفا، مرجع سابق،ص84).
- وحتى في حالة عدم الحصول على النسخة الأصلية للدليل السيبراني أو في حالة أن العبث قد وقع على النسخة الأصلية، ففي هذه الحالة بالإمكان التأكد من سلامة الدليل السيبراني من التبديل أو العبث من خلال استخدام عمليات حسابية خاصة تسمى بالخوارزميات (بيومي، مرجع سابق، ص91).
- وهناك نوع من الأدلة السيبرانية يسمى بالدليل المحايد، وهو دليل ليس له علاقة بموضوع الجريمة إلا أنه يساهم في التأكد من مدى سلامة الدليل السيبراني المقصود من حيث عدم حصول تعديل أو تغيير في النظام (الكمبيوتري).

فمن خلال هذه الطرق يمكن التأكد من سلامة الدليل السيبراني ومدى تطابقه مع الواقع.

ثانيًا: تقييم الدليل السيبراني من حيث السلامة الفنية للإجراءات المستخدمة في الحصول على الدليل السيبراني:

عادة تتبع عدد من الإجراءات الفنية للحصول على الدليل السيبراني، وهذه الإجراءات من الممكن أن يعتريها خطأ ويحصل الشكك في سلامة نتائجها، وبناء على ذلك يمكن في في هذه الحالة اعتماد ما يعرف باختبارات (داو بورت) (عبدالمطلب، مرجع سابق،ص248)، كوسيلة للتأكد من سلامة الإجراءات المتبعة في الحصول على الدليل السيبراني المطابق للقانون لقبوله كدليل إثبات، وفيما يلي أهم الطرق التي تتبع للتأكد من سلامة ودقة هذه الإجراءات من الناحية الفنية (إبراهيم ، مرجع سابق،ص229):

أ- ضرورة إخضاع الأداة المستخدمة لعدة تجارب للتأكد من دقتها في إعطاء النتائج ويتحقق ذلك بإتباع اختبارين أساسيين هما:

- اختبار السلبيات الزائفة: ومفاد هذا الاختبار أن تخضع الأداة المستخدمة في الحصول على الدليل السيبراني لاختبار يبين مدى قدرة هذه الأداة على عرض كافة البيانات المتعلقة بالدليل السيبراني، من دون إغفال بيانات مهمة عنه.
- اختبار الايجابيات الزائفة: وهو خضوع الأداة المستخدمة في الحصول على الدليل السيبراني لاختبار فني دقيق نستطيع من خلاله التأكد من أن هذه الأداة لا تعرض بيانات اضافية أخرى. وهكذا يتم من خلال هذين الاختبارين التأكد من أن الأداة المستخدمة قد عرضت كل البيانات المتعلقة بالدليل السيبراني وفي الوقت نفسه لم تضف إليها أي بيان آخر، وهذا الأمر يعزز مصداقية النتائج التي يتم الحصول عليها من خلال تلك الأداة في إثبات الواقع.

ب- الاعتماد على الأدوات التي أثبتت البحوث العلمية كفاءتها في تقديم نتائج أفضل:

حيث تدلل المقالات والبحوث المنشورة في الدوريات في مجال تقنية المعلومات على الوسائل السليمة التي يجب اتباعها لأجل الحصول على الدليل السيبراني، وفي نفس الوقت تثبت تلك الدراسات الأدوات المشكوك في كفاءتها، وهذا يساعد على تحديد مصداقية المخرجات التي تم الحصول عليها من تلك الأدوات(حجازي، مرجع سابق،ص38).

وهكذا يتضح لنا أنه من المستطاع الوقوف على سلامة الدليل السيبراني، فإذا توافرت في الدليل السيبراني الشروط العامة لما يمكن أن يمثل أساسًا لتوافر الثقة فيه، فإنه قد يبدو من غير المقبول أن يعيد القاضي تقييم هذا الدليل وطرحه من جديد على بساط البحث، فالدليل السيبراني بوصفه دليلًا علميًا فإن دلالته قاطعة بشأن تلك الواقعة (فرج، مرجع سابق،ص79).

وهكذا يتضح أن الخبرة تحتل في هذا المجال دورًا مهمًا في التثبت والتأكد من صلاحية هذا الدليل كأساس لتكوين عقيدة القاضي، فبحث مصداقية هذا الدليل هي من صميم فن الخبير لا القاضي.

وبالتالي يجب عدم الخلط بين الشكوك التي تشوب الدليل الرقمي بسبب إمكانية العبث به أو لوجود خطأ في الحصول عليه وبين القيمة الإقناعية لهذا الدليل، فالحالة الأولى لا يملك القاضي الفصل فيها لأنها مسألة فنية، فالقول فيها هو قول أهل الخبرة، فإن سلم الدليل السيبراني من العبث والخطأ، فإنه لن يكون للقاضي سوى القبول بهذا الدليل ولا يمكنه التشكيك في قيمته التدليلية لكونه وبحكم طبيعته الفنية يمثل إخبارًا صادقًا عن الواقع (احمد، مرجع سابق،ص295)، ما لم يثبت عدم صلة الدليل بالجريمة المراد إثباتها.

الخاتمة:

من خلال هذه الدراسة عن الأحكام الإجرائية للجرائم السيبرانية في التشريع الإماراتي والمقارن نستطيع أن نبين أهم النتائج والتوصيات وكما يلي:

النتائج:

هنالك عدة نتائج ونستطيع أن نختار أهمها:

- تشترط الجريمة السيبرانية أساليب غير تقليدية فيجمع الأدلة والتحقيق الابتدائي لاكتشاف الدليل وذلك من قبل فنيين مختصين.
- تتميز الجرائم السيبرانية بصعوبة إثباتها ومتابعة مرتكبيها وسهولة أتلاف أدلتها.
- لا يوجد تشريع للإجراءات الجنائية للجرائم الإلكترونية في الأمارات حيث تطبق القواعد العامة في قانون الإجراءات الجزائية الإماراتي على الجرائم الإلكترونية.
- من الصعوبات التي تحول دون الحصول على الأدلة السيبرانية، هو تعذر أجراء التفتيش لضبط هذه الجرائم عندما يكون الحاسب الألي متصلًا بحاسبات أخرى خارج الدولة، ويكون تفتيش هذه الحاسبات ضروريًا لكشف عما تشتمله هذه الجرائم.

التوصيات:

هنالك عدة توصيات ونستطيع أن نختار أهمها:

- ضرورة تدريب أجهزة العدالة الجنائية حتى يكون في استطاعتها التعامل مع هذا النمط المستحدث من الجرائم بما يكفل لهم القدرة الفنية والتحقيقية لممارسة أعمالهم بكفاءة وجداره.
- من الضروري القيام بدراسات مقارنة حول طرق جمع الأدلة في الجرائم السيبرانية.
- يجب أن تكون هناك ضوابط واضحة وصالحة للتعامل مع الجرائم السيبرانية والممارسات غير الأخلاقية/ وبما يحد ويقيد من خطورة هذه الأفعال لأجل ردع مرتكبيها.
- يجب إنشاء قاعدة بيانات للجرائم السيبرانية من حيث أنواعها وأساليبها للرجوع إليها عند الحاجة.
- ضرورة وضع تشريع عقابي يتعامل مع الجرائم السيبرانية وقايةً، وتحقيقًا وضبطًا.
- ضرورة تشديد الرقابة على المنشورات والمطبوعات التي ترد إلى البلاد من الخارج خشية تسلل المواد المحظورة والتي تستغل في ارتكاب الجرائم السيبرانية.
- ضرورة وضع تشريعات جديدة على المستوى الوطني والإقليمي في مجال مكافحة الجرائم السيبرانية.
- عند الحاجة والضرورة الملحة يجب الاستفادة من مرتكبي الجرائم السيبرانية للعمل كمساعدين لمأموري الضبط القضائي.
- وأخيرًا نشدد على أهمية وجود تعاون إقليمي ودولي في مجال مكافحة الجرائم السيبرانية التي تتم باستخدام أجهزة الكمبيوتر أو عبر الشبكة العنكبوتية.

المراجع:

إبراهيم، خالد ممدوح. (د.ت). *فن التحقيق الجنائي في الجرائم الإلكترونية*.

أبو النصر، مدحت محمد. (2012). *التفكير الابتكاري والإبداعي طريقك الى التميز والنجاح*.

أبو الوفا، محمد أبو الوفا. (2009). *المواجهة الإجرائية للجرائم المعلوماتية*. بحث مقدم إلى كلية القانون قسم القانون العام، جامعة الإمارات.

أحمد، هلالي عبدالإله. (2008). *حجية المخرجات الكمبيوترية في المواد الجنائية: دراسة مقارنة*. الطبعة الثالثة، دار النهضة العربية.

البشرى، محمد الأمين. (2005). *التحقيق في جرائم الحاسب الآلي*. بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات، ص6.

البشرى، محمد الأمين. (د.ت). *الجرائم الإلكترونية (التحقيق والإدعاء والمحاكمة)*. أكاديمية شرطة دبي.

بلال، أحمد عوض (2003). *قاعدة استبعاد الأدلة بطرق غير مشروعة في الإجراءات الجنائية المقارنة*. دار النهضة العربية.

بوحوش، عطية. (2018). *حجية الدليل الرقمي في إثبات الجرائم السيبرانية*. رسالة ماجستير، طرابلس، ليبيا.

بيومي حجازي، عبدالفتاح. (2019). *الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية: دراسة مقارنة في ضوء القواعد العامة للإجراءات الجنائية*. الطبعة الأولى.

بيومي، عبدالفتاح. (2002). *الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت: دراسة متعمقة في الجرائم السيبرانية*. دار الكتب القانونية، المحلة الكبرى، مصر.

حسين، سامي جلال. (2015). *التفتيش في الجرائم المعلوماتية*. دار الكتب القانونية.

الحلبي، خالد عياد. (2017). *إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت*. دار الثقافة والنشر للتوزيع.

رستم، هشام محمد فريد. (2006). *الجوانب الإجرائية للجرائم المعلوماتية*. مكتبة الأت الحديثة.

رستم، هشام محمد فريد. (د.ت). *العقوبات ومخاطر تقنية المعلومات*.

الشوا، محمد سامي. (1998). *ثورة المعلومات وانعكاساتها على قانون العقوبات*. الطبعة الثانية، دار النهضة العربية.

الصغير، جميل عبدالباقي. (2012). *أدلة الاثبات الجنائي والتكنولوجيا الحديثة*. دار النهضة العربية.

عبد المطلب، ممدوح. (2005). *أدلة الصور الرقمية في الجرائم عبر الكمبيوتر*. شرطة دبي.

عبدالمطلب، ممدوح عبدالحميد. (د.ت). *الجريمة عبر الإنترنت*. مكتبة الحقوق.

عبدالمطلب، ممدوح. (2006). *البحث والتحقيق الرقمي في جرائم الكمبيوتر والإنترنت*. دار الكتب القانونية.

العتيبي، خالد بن مرزوق. (د.ت). *الجوانب الإجرائية في الشروع في جرائم المعلوماتية*.

عوض، رمزي رياض. (2007). *مشروعية الدليل الجنائي في مرحلة المحاكمة وما قبلها: دراسة تحليلية تأصيلية مقارنة*. دار النهضة العربية.

فرج، أمير. (د.ت). *الأثبات الجنائي للجريمة الإلكترونية والاختصاص القضائي*.

مصطفى، أحمد محمود. (2010). *جرائم الحاسبات الآلية في التشريع المصري: دراسة مقارنة*. دار النهضة العربية.

هلالي، عبدالإله أحمد. (2010). *التزام الشاهد بالكلام في الجرائم المعلوماتية: دراسة مقارنة*. النسر الذهبي.

Bevan, N., & Lidstone, K. (2005). *A Guide to the Police and Criminal Evidence Act (2nd ed.)*. Bulterworthe.

Council of Europe activities related to Information Technology, Data Protection, and computer crime. (2006). Better Information and Communication Technology Law, 5(3), 177.

Fafinski, S. (2009). *Computer Misuse: Response, regulation and the law*. Willan Publishing.

Glenny, M. (2011). *Cyberthieves - Cybercops and You*. Alfred A. Knopf.

Grabosky, P. (2006). *Electronic Crime*. Prentice Hall.

Knittel, J., & Soto, M. (2000). *The Danger of Computer Hacking*. The Rosen Publishing Group.