التفتيش الجنائي على نظم الحاسوب والانترنت

دراسة مقارنة (مصر والسعودية)

"Criminal Inspection of Computer and Internet Systems AComparative Study (Egypt and Saudi Arabia)"

د. نهاد نادي عمر

nehadnady8@gmail.com

إلى الذين كانوا عونا لنا في بحثنا ونوراً يضئ الظلمة التي كانت تقف أحياناً في طريقنا.

إلى من زرعوا التفاؤل في دربنا وقدموا لنا المساعدات والتسهيلات والأفكار والمعلومات

ربما دون أن يشعروا بدورهم، فلهم منا كل الشكر والتقدير

إلى كل من دعا لي بالخير

أهديكم ذلك العمل المتواضع

شكر وتقدير

بسم الله الرحمن الرحيم

" قَالُوا سُبْحَانَكَ لَا عِلْمَ لَنَا إِلَّا مَا عَلَّمْتَنَا إِنَّكَ أَنتَ الْعَلِيمُ الْحَكِيمُ "

صدق الله العظيم

نحمد الله عز وجل الذي وفقنا في إتمام هذا البحث العلمي، والذي أعطانا الصحة والعافية والعزيمة

على استكماله .

فنتقدم بجزيل الشكر والتقدير لكل من ساعدني على تقديم هذا الموضوع المهم وجميع الأساتذة الكرام لما قدموا لي من توجيهات ومعلومات ذات قيمة عملت على المساهمة في كتابة وإثراء موضوع دراستنا في الكثير من الجوانب المختلفة دون نسيان أي فرد وخالص الشكر لكل من مديرين ومعلمين ومتعلمين داخل الجامعة

كما نتقدم بالشكر الجزيل لأساتذة علم النفس المحترمين، وقيامهم بتفضيل مناقشة هذه الرسالة والاستفادة من خبراتها العلمية، ووضع اللمسات المنهجية والإرشادات المتميزة التي جعلت هذا البحث بهذه الصورة الرائعة.

وفي الختام أتقدم بالشكر والتقدير لكل من مد لي يد العون والمساعدة أثناء تطبيق هذه الدراسة، فجزا الله الجميع خير الجزاء.

الحمد لله وبالله التوفيق

الباحث

المستخلص:

تعد الحوسبة والانترنت من التقنيات الحديثة التي أحدثت تحولًا جذريًا في الحياة اليومية والأعمال التجارية، ولكنها أيضًا أتاحت فرصًا جديدة لارتكاب الجرائم المعلوماتية لذا، أصبح التفتيش الجنائي على نظم الحاسوب والانترنت ضرورة لمكافحة هذه الجرائم والحفاظ على الأمن السيبراني.

تهدف هذه الدراسة إلى إجراء تحليل مقارن بين مصر والسعودية فيما يتعلق بالتفتيش الجنائي على نظم الحاسوب والانترنت وتم تقييم التشريعات والقوانين المحلية المتعلقة بالتفتيش الجنائي، وكذلك الإجراءات والسياسات المتبعة في كل بلد وتم أيضًا تحليل الدور الذي تلعبه الجهات المعنية في تنفيذ التفتيش الجنائي وتطوير القدرات المتعلقة.

بالإضافة إلى ذلك، تم مناقشة التحديات التي تواجه كل بلد في مجال التفتيش الجنائي، بما في ذلك الجوانب القانونية والتقنية والمؤسسية وسلط الضوء على الجوانب الإيجابية والسلبية في كل بلد وتوجيه التوصيات لتعزيز فعالية التفتيش الجنائي.

من خلال هذه الدراسة حصلنا على نتائج مهمة تساهم في تحسين التفتيش الجنائي على نظم الحاسوب والانترنت في كل من مصر والسعودية. كما ستساهم النتائج في تعزيز التعاون بين البلدين في مجال مكافحة الجرائم المعلوماتية .

كلمات مفتاحية للبحث: التفتيش الجنائي، نظم الحاسوب، الإنترنت

Abstract:

Computing and the internet are modern technologies that have brought about a radical transformation in daily life and business. However, they have also opened up new opportunities for committing cybercrimes. Therefore, criminal investigation of computer and internet systems has become necessary to combat these crimes and maintain cybersecurity.

This study aims to conduct a comparative analysis between Egypt and Saudi Arabia regarding criminal investigation of computer and internet systems. It evaluates the legislation and local laws related to criminal investigation, as well as the procedures and policies followed in each country. Furthermore, it analyzes the role played by relevant authorities in implementing criminal investigations and developing related capabilities.

In addition, the challenges faced by each country in the field of criminal investigation are discussed, including legal, technical, and institutional aspects. The positive and negative aspects in each country are highlighted, and recommendations are provided to enhance the effectiveness of criminal investigation.

Through this study, important results have been obtained that contribute to improving criminal investigation of computer and internet systems in both Egypt and Saudi Arabia. The results will also contribute to enhancing cooperation between the two countries in combating cybercrimes.

Keywords:

Criminal Inspection- Computer Systems- The Internet

مقدمة

تُسعى الدولة القانونية إلى تحقيق توازن بين حق المجتمع في معاقبة مرتكبي جرائم الحاسوب والإنترنت وبين حماية حقوق الإنسان في إجراءات المحاكمة الجنائية. ومن بين هذه الإجراءات، يأتي التفتيش كوسيلة تتعلق بحرية الأفراد وخصوصياتهم وحقوقهم المنزلية، ويجمع بين استخدام السلطة وتقييد الحرية. وفي الوقت الحالي، تواجه الأجهزة الأمنية في مصروالسعودية عدداً من الجرائم التي تتعلق بالحاسوب والإنترنت، لذا فمن الضروري أن نتعامل مع هذه المشكلات ونستعد لمواجهتها من خلال التشريعات.

وتأتي هذه الدراسة لتسليط الضوء على أحد هذه المشكلات وهو "التفتيش على نظم الحاسوب والإنترنت"، التي تنشأ نتيجة استخدام التكنولوجيا المعلوماتية في الجريمة. تهدف الدراسة إلى تطوير أساليب تتوافق مع طبيعة هذه التكنولوجيا للتصدي لهذه المشكلة، وتحقيق توازن بين متطلبات أنشطة الجهات القضائية فيما يتعلق بالخصوصية. وتستفيد الدراسة من الاستنتاجات والجهود والخبرات التي تم توفيرها في مجال الفقه المقارن في بحث هذه المشكلات، بما في ذلك التفتيش على نظم الحاسوب والإنترنت في السنوات الأخيرة، والخبرات المتنوعة في المجال التشريعي. وتعد هذه الدراسة مساعدة للمشرع الأردني إذا رغب في التعامل مع هذه المشكلات.

تطبيق النصوص التقليدية على جرائم الحاسوب والإنترنت يثير مشاكل في مسألة الإثبات، حيث يصعب في كثير من الأحيان العثور على أدلة مادية للجرائم المعلوماتية. ويمكن أن يتم اكتشاف الجرائم بشكل عرضي، ويعد محو

الدليل أمراً سهلاً في زمن قصير.[1] تشكل صعوبة كبيرة في التفتيش على نظم الحاسوب والإنترنت. بالإضافة إلى ذلك، تشكل تشفير البيانات المطلوب تفتيشها وضبطها مشكلة حقيقية تواجه سلطات التحقيق المعتمدة على التفتيش. وهذا يثير تساؤلات في مجال الفقه الجنائي حول إمكانية إجبار المشتبه فيهم على فك تشفير برامجهم أو نظمهم.[2] يتبين من هذا أن قانون أصول المحاكمات الجزائية قد يكون غير كاف في مواجهة هذه المشكلات والتساؤلات، وبالتالي قد يكون هناك حاجة لتعديل النصوص القانونية أو تشريع قوانين جديدة لمعالجة هذه المسائل[3].

بالإضافة إلى ذلك، ينبغي الدخول في اتفاقيات دولية وتفعيلها لمكافحة الجريمة المعلوماتية التي تعبر الحدود عبر شبكة الإنترنت. تعد هذه الدراسة محاولة لسد الفجوة في هذا النوع من الدراسات، وتواكب التطور التكنولوجي والعلمي والحاجة إلى معالجة المشكلات التي نشأت نتيجة لذلك. وقد قام الباحث بمقارنة التشريعات العربية والتشريعات الغربية في مجال التدابير الإجرائية المتعلقة بالجريمة المعلوماتية، حيث يشهد التشريع الإجرائي في بعض الدول الأوروبية.[4]

[1] د.م.ي. باجا نوف ود. يوم غرو شيفري- شرح الإجراءات الجنائية السوفيتية - ترجمة صالح العبيدي - جامعة بغداد – بغداد – ١٩٩٠م.

[2] د.حسني الجندي - الدفع ببطلان التفتيش في ضوء أحكام محكمة النقض دراسة تحليلية تأصيلية - دار النهضة العربية - القاهرة – ١٩٨٨/١٩٨٩م.

[3] د. حامد راشد - أحكام تفتيش المسكن في التشريعات الإجرائية العربية - دراسة مقارنة - ط ١ - دار النهضة العربية - القاهرة – ١٩٩٨م.

[4] د.جميل عبد الباقي الصغير - القانون الجنائي والتكنولوجيا الحديثة - الكتاب الأول - الجرائم الناشئة عن استخدام الحاسب الآلي – ط١ – دار النهضة العربية - القاهرة – ١٩٩٢م.

تم عقد المؤتمر الدولي الخامس للجمعية الدولية لقانون العقوبات في عام 1994، استناداً إلى التحضيرات التي بدأت في عام 1992. تم توصية المؤتمر بتحديد سلطات إجراء التفتيش والضبط في بيئة تكنولوجيا المعلومات، وخاصة فيما يتعلق بضبط الأموال غير المحسوسة وتفتيش نظم الحاسوب المتصلة ببعضها البعض (شبكات الحاسوب). تلاتها توصية رقم ر-٩٥-١٣ التي أصدرها المجلس الأوروبي في 11 سبتمبر 1995 بشأن مشكلات الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات، وتناولت مسألة التفتيش والضبط. يتم مناقشة بنود هذه التوصيتين خلال هذه الدراسة[1].

على الصعيد الإقليمي العربي، تم طرح مشروع القانون العربي النموذجي الموحد لمكافحة سوء استخدام تكنولوجيا المعلومات والاتصالات عن مجلس وزراء الداخلية العرب - الأمانة العامة في عام 2002. [2]تضمنت المادة 26 من هذا المشروع ضمانات لحماية سرية البيانات الأخرى المخزنة وعدم المساس بحقوق الأشخاص الأخرى غير المتعلقة بالبرامج والبيانات المخزنة. لم يتم حتى الآن قبول هذا المشروع من قبل الدول العربية، بما في ذلك الأردن، ولم تصدر أي تشريعات خاصة بجرائم الحاسوب والإنترنت أو الإجراءات الواجب اتخاذها لمواجهة هذه الجرائم، على الرغم من وجود

[1] أحمد أسامة حسنية، التفتيش في الجرائم الإلكترونية في التشريع الفلسطيني، دراسة تحليلية مقارنة بالتشريع العُماني، 2016

[2] هلالي عبد الإله أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، سنة 1997

تشريعات تتعلق بحماية الملكية الفكرية والصناعية التي تتضمن البرمجيات كجزء من المصنفات المحمية بالقانون

تأتي هذه الدراسة، المعنونة بـــ "التفتيش الجنائي على نظم الحاسوب والإنترنت: دراسة مقارنة"، كمحاولة لتسليط الضوء على إحدى هذه المشكلات المتعلقة بأنظمة الحاسوب والإنترنت. فالتقنية المعلوماتية تطرح قضايا جنائية متنوعة، ومن هنا تتطلب التحديات المرتبطة بتلك التقنية تبني أساليب ملائمة تتوافق مع طبيعتها الفريدة، مع الحفاظ في الوقت ذاته على توازن يلبي احتياجات أجهزة القضاء في ضمان الخصوصية. وفي هذا السياق، يستفيد الباحثون في هذا المجال من الخبرات والجهود التي تم توجيهها في الفقه المقارن لبحث هذه المشكلات، بما في ذلك التفتيش على نظم الحاسوب والإنترنت خلال السنوات الأخيرة.[1]

تعتبر الحواسيب والإنترنت من التكنولوجيات الحديثة التي أحدثت تحولاً جذرياً في طرق التواصل والتعامل مع المعلومات. ومع التطور المستمر في هذه التقنيات، ظهرت تحديات جديدة تتعلق بالجرائم المعلوماتية التي تستهدف أنظمة الحواسيب وشبكة الإنترنت. وتعد عمليات التفتيش الجنائي على نظم الحاسوب والإنترنت أحد الأدوات الهامة التي تساهم في الكشف عن جرائم الإنترنت ومتابعة المشتبه فيهم وجمع الأدلة القانونية.

[1] عربوز فاطمة الزهراء، التفتيش الالكتروني كإجراء للتحقيق في الجرائم المعلوماتية، مجلة جيل الأبحاث القانونية المعمقة، العدد 34

تهدف هذه الرسالة إلى إجراء دراسة مقارنة بين مصر والسعودية في مجال التفتيش الجنائي على نظم الحاسوب والإنترنت. وتسعى الرسالة إلى تحليل ومقارنة الأطر القانونية والإجرائية المتبعة في البلدين، بما في ذلك التشريعات والسياسات ذات الصلة وآليات التفتيش والضبط في هذا النطاق. كما تهدف الرسالة إلى تحديد التحديات والصعوبات التي تواجه عمليات التفتيش الجنائي على نظم الحاسوب والإنترنت في كل من مصر والسعودية، وتقديم توصيات واقتراحات قانونية تسهم في تعزيز فعالية هذه العمليات وتحسين نتائجها.

وتعتمد هذه الرسالة على منهجية بحثية متعددة، تشمل دراسة المصادر القانونية والقضائية ذات الصلة واستقصاء الدراسات والأبحاث السابقة في مجال التفتيش الجنائي على نظم الحاسوب والإنترنت في مصر والسعودية، وإجراء مقابلات مع الخبراء والمتخصصين في هذا المجال. ستتم دراسة وتحليل القوانين واللوائح المعمول بها في كل من مصر والسعودية، ومقارنتها من حيث التشريعات المعمول بها وآليات التفتيش والضبط المتبعة.

سيتم التركيز في هذه الرسالة على عناصر محددة مثل تعريف التفتيش الجنائي على نظم الحاسوب والإنترنت، والإجراءات المتبعة في جمع الأدلة الرقمية وتحليلها، وآليات التحقق من صحة الأدلة الرقمية، وحماية حقوق الأفراد أثناء عمليات التفتيش، والعقوبات القانونية المترتبة على ارتكاب الجرائم المعلوماتية.

من خلال هذه الدراسة المقارنة، ستساهم الرسالة في توفير فهم أعمق للتشريعات والسياسات المتبعة في مجال التفتيش الجنائي على نظم الحاسوب والإنترنت في مصر والسعودية. كما ستساعد الرسالة في تحديد الممارسات الجيدة والعوائق التي تواجه تنفيذ التفتيش الجنائي، وتقديم توصيات قانونية وسياسية لتعزيز الفعالية والكفاءة في هذا المجال.

التفتيش الجنائي على نظم الحاسوب والإنترنت هو أحد الأدوات الحاسمة في مكافحة الجرائم المعلوماتية، ولكنه يشكل تحديات قانونية كبيرة نظراً لطبيعته الاستثنائية وتأثيره على حقوق الأفراد والحريات الشخصية.[1] تسعى هذه الدراسة إلى تحقيق التوازن بين حقوق المجتمع في محاربة جرائم الكمبيوتر والإنترنت وحقوق الأفراد في سياق الإجراءات الجنائية[2].

تتناول الدراسة تحليل ومقارنة التشريعات والنظم المحلية للتفتيش الجنائي في مصر والمملكة العربية السعودية. وتهدف الدراسة إلى تطبيق الأسس القانونية والمفاهيم التقليدية على مجال التفتيش والرقابة على أنظمة الحاسوب والإنترنت، مع التركيز على الصعوبات التقنية والتقنيات المستخدمة في جمع الأدلة وتحليلها.

---

[1] الشرقي حراث، الدفوع الشكلية في المادة الزجرية، مكتبة الرشاد السطات، الطبعة الأولى، السنة 2012

[2] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي، الإسكندرية، مصر، الطبعة الأولى، 2009

تناقش الدراسة أيضاً قضية الإثبات الجنائي في سياق أنظمة الحاسوب والإنترنت، وتسلط الضوء على صعوبة العثور على أدلة مادية ومحو الأدلة الرقمية. كما تستكشف قضية بيانات وأنظمة التشفير والتحديات التي تواجه المحققين في فك الشفرات واسترداد المعلومات الهامة[1].

تهدف الدراسة إلى إيجاد سبل لتعزيز الإجراءات الجنائية ذات الصلة بالتفتيش الجنائي، وحماية المعلومات الحساسة والحقوق الشخصية. وتوصي الدراسة بوجود آليات إضافية لتعزيز الأدلة وحماية المعلومات الرقمية، بالإضافة إلى تعزيز التعاون بين البلدين في مجال مكافحة الجرائم الالكترونية .[2]

يهدف هذا البحث إلى تطوير المنهجيات والإجراءات القانونية في التفتيش الجنائي على نظم الحاسوب والإنترنت في كل من مصر والسعودية، وذلك من خلال دراسة التشريعات الحالية وتحديد النواقص والثغرات فيها، وتقديم توصيات لتحسين التشريعات وتعزيز التعاون بين الجهات ذات العلاقة في بمجال التفتيش الجنائي على نظم الحاسوب والإنترنت في مصر والسعودية. ستتم دراسة التجارب القانونية والقضائية في كل من البلدين، وتحليل التحديات والمشاكل التي تواجهها عمليات التفتيش الجنائي، وتقديم حلول واقتراحات فعالة لتعزيز النظام القانوني وتحسين نتائج عمليات التفتيش.

---

[1] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2010

[2] عربوز فاطمة الزهراء، التفتيش الالكتروني كإجراء للتحقيق في الجرائم المعلوماتية، مجلة جيل الأبحاث القانونية المعمقة، العدد 34

من المتوقع أن تسهم الرسالة في إثراء المعرفة القانونية والقضائية حول التفتيش الجنائي على نظم الحاسوب والإنترنت، وتعزيز التفاهم والتعاون بين مصر والسعودية في هذا المجال الحيوي. ستكون النتائج والتوصيات التي سيتم الوصول إليها نتاجاً للدراسة المعمقة للتشريعات والأنظمة القانونية، وتحليل الخبرات السابقة والأبحاث العلمية ذات الصلة.1

سيستفيد من هذه الرسالة الباحثون والمتخصصون في مجال التفتيش الجنائي وعلوم الحاسوب والقانون، فضلاً عن القضاة والمحققين وأجهزة الشرطة والهيئات الرقابية والمهتمين بتنمية النظام القانوني في قطاع التكنولوجيا والمعلومات.

ويعتبر التفتيش في الجرائم الإلكترونية وسيلة مهمة للبحث عن الأدلة المتعلقة بالجرائم، وهناك نوعان رئيسيان للتفتيش: التفتيش على المكونات المادية والتفتيش على المكونات غير المادية. يشمل التفتيش على المكونات المادية البحث عن الأدلة المادية كالأشرطة والكابلات وشاشات العرض. أما التفتيش على المكونات غير المادية فيشمل البحث عن الأدلة على الحاسوب الآلي أو المعلومات والبيانات المخزنة أو المرسلة عبر الإنترنت. وعلى الرغم من أن المعلومات هي معاني يدركها الإنسان بواسطة نغمات أو ذبذبات إلكترونية، إلا أن البيانات المرتبطة بهذه المعلومات يمكن إخضاعها لقواعد التفتيش.

[1] هلالي عبد الإله أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، سنة 1997، ص 47.

تواجه قوانين الدول المتقدمة صعوبة في التعامل مع الحالات التي يوجد فيها نظام معلوماتي داخل منزل المتهم ونهاية طرفية في مكان آخر، حيث يتاح للمتهم فرصة التخلص من البيانات التي يستهدفها التفتيش. ولذلك، يجب على السلطات ذات الاختصاص الحصول على إذن التفتيش لدخول منزل المتهم واستجواب النهاية الطرفية.

يجب وضع عقوبات وتدابير تتناسب مع انتهاك حقوق المتهم والأشخاص الآخرين أثناء إجراءات التفتيش والمصادرة. وتتطلب هذه الإجراءات الاحترافية مراعاة حقوق المتهم والأفراد والمؤسسات الأخرى فيما يتعلق بخدمة الإنترنت.

إن أهمية هذا البحث تكمن في ضرورة معالجة التحديات القانونية والتشريعية المرتبطة بالتفتيش الجنائي على نظم الحاسوب والإنترنت في مصر والسعودية، وتحقيق التوازن بين حماية الحقوق والحريات الفردية وضمان الأمن الإلكتروني ومكافحة الجرائم المعلوماتية.1

أخيراً، أود أن أعرب عن أملي في أن يكون هذا البحث مساهمة فعالة في رفع مستوى الوعي القانوني والتشريعي بشأن التفتيش الجنائي على نظم الحاسوب والإنترنت في مصر والسعودية، وأن يسهم في تحسين الممارسات القانونية والإجرائية في هذا المجال الحيوي والحساس. إنني واثق بأن هذا البحث سيسهم في تحقيق التقدم والتطور في مجال الحماية القانونية للأنظمة

[1] الشرقي حراث، الدفوع الشكلية في المادة الزجرية، مكتبة الرشاد السطات، الطبعة الأولى، السنة 2012

الإلكترونية والمعلوماتية، وتحقيق العدالة والأمان الرقمي في مجتمعاتنا المتقدمة تكنولوجياً.

وتتطلع هذه الدراسة إلى إلقاء الضوء على جوانب مختلفة من التفتيش الجنائي على نظم الحاسوب والإنترنت في مصر والسعودية، من خلال دراسة مقارنة شاملة. وتهدف الدراسة إلى تحليل وتقييم الإطار القانوني والتشريعي المتعلق بهذا المجال في البلدين، بما يشمل التشريعات المعمول بها والسياسات الحكومية ذات الصلة.

ستتم مناقشة القضايا والتحديات التي تواجهها كل من مصر والسعودية في تفتيش نظم الحاسوب والإنترنت، بما في ذلك قضايا الخصوصية والحقوق الفردية وحماية البيانات. كما ستتم مقارنة النهج والممارسات القانونية في كل بلد، وتحليل النتائج والتوصيات المستخلصة من هذه المقارنة.1

سيتم استخدام منهجية بحثية متعددة لجمع البيانات وتحليلها، بما في ذلك دراسة وثائقية للتشريعات والسياسات، ومقابلات مع الخبراء والممارسين في المجال القانوني والأمن السيبراني. سيتم أيضاً تحليل القرارات القضائية ذات الصلة والدراسات السابقة المنشورة في هذا السياق.

من خلال هذه الدراسة، نأمل أن نساهم في إثراء المعرفة وفهم التفتيش الجنائي على نظم الحاسوب والإنترنت في مصر والسعودية، وتوفير أساس قانوني وتشريعي موثوق يمكن أن يستخدم في تحسين الممارسات وتعزيز الأمان

[1] هلالي عبد الإله أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، سنة 1997، ص 47.

السيبراني في هذين البلدين. كما نأمل أن تكون نتائج هذه الدراسة قابلة للتطبيق وتفيد القرارات السياسية والتشريعية المستقبلية في هذا المجال.

وتعتبر هذه الدراسة الأولى من نوعها التي تقوم بدراسة مقارنة بين التفتيش الجنائي على نظم الحاسوب والإنترنت في مصر والسعودية. ويعود ذلك إلى أهمية هذا الموضوع في ظل التطور السريع في مجال التكنولوجيا والانترنت وتزايد استخدام الحواسيب والشبكات الإلكترونية في العمليات الجنائية والجرائم السيبرانية.

تنطوي هذه الدراسة على تحليل شامل للأطر القانونية والتشريعية التي تنظم التفتيش الجنائي على نظم الحاسوب والإنترنت في كل من مصر والسعودية. ستتم مراجعة التشريعات والقوانين المعمول بها في البلدين وتحليل السياق القانوني والتطبيقي لهذه القوانين. سيتم أيضاً دراسة السياسات الحكومية ذات الصلة والإجراءات التنفيذية والمؤسسات المعنية بالتفتيش الجنائي على نظم الحاسوب والإنترنت.

بالإضافة إلى ذلك، ستتم دراسة الممارسات والنهج المعتمدة في كل بلد فيما يتعلق بالتفتيش الجنائي على نظم الحاسوب والإنترنت. ستتم مقارنة العمليات والإجراءات المتبعة في كل بلد، وتحليل الأسس القانونية والأدلة المقدمة والجوانب الفنية المرتبطة بعمليات التفتيش.

إشكالية الدراسة

يشكل التفتيش الجنائي على نظم الحاسوب والإنترنت في مصر والسعودية موضوعاً ذا أهمية كبيرة في ضوء التطور السريع للتكنولوجيا واعتماد الحواسيب والشبكات الإلكترونية في مختلف جوانب الحياة اليومية والعمليات الجنائية. ومع ذلك، تنشأ تحديات ومشكلات قانونية تتعلق بممارسات التفتيش الجنائي على نظم الحاسوب والإنترنت في البلدين، والتي تتطلب دراسة مقارنة شاملة لتحليل هذه المشكلات والبحث في النهج والممارسات القانونية في كل من مصر والسعودية

تعتبر إشكالية هذه الدراسة هي التحديات القانونية المتعلقة بالتفتيش الجنائي على نظم الحاسوب والإنترنت في مصر والسعودية، وتحديد الاختلافات والتشابهات بين النظامين القانونيين في هذا الصدد. وترتبط هذه التحديات بقضايا حماية الخصوصية والحقوق الفردية والتوازن بين حماية المجتمع والتحقيق الجنائي.[1]

تتناول هذه الدراسة التفتيش الجنائي على نظم الحاسوب والإنترنت في مصر والسعودية، وتهدف إلى تحليل الإطار القانوني والتحديات التي تواجه هذا النوع من التفتيش في كل من البلدين. تعتبر هذه الاشكالية ذات أهمية كبيرة نظراً للتطورات السريعة في مجال التكنولوجيا واستخدام الحواسيب والإنترنت في النشاطات الجنائية.

[1] نديم محمد حسن الترزي، سلطات النيابة العامة في الجرائم المعلوماتية، مجلة أندلس للعلوم الاجتماعية والإنسانية، العدد 19، مجلد 15، أبريل 2017

بشكل عام، يمكن تلخيص اشكالية الدراسة في**النقاط التالية:**

- تحديات التشريعات والقوانين المعمول بها في مصر والسعودية فيما يتعلق بالتفتيش الجنائي على نظم الحاسوب والإنترنت، وتحليل الفروق والتشابه بينهما.
- حماية الخصوصية والحقوق الفردية في عمليات التفتيش الجنائي، ودراسة التدابير القانونية المتخذة للحفاظ على تلك الحقوق في كل من مصر والسعودية.
- التوازن بين حماية المجتمع وحقوق الأفراد في عمليات التفتيش الجنائي على نظم الحاسوب والإنترنت في مصر والسعودية، وتحليل كيفية معالجة التوازن بين حقوق الأفراد ومصلحة المجتمع في كل من البلدين.
- التحديات التقنية المرتبطة بالتفتيش الجنائي على نظم الحاسوب والإنترنت، مثل جمع البيانات الإلكترونية وتحليلها وتحديد صحة الأدلة الرقمية والأساليب المستخدمة في استخراجها، وتحليل كيفية التعامل مع هذه التحديات في كل بلد.
- السياسات الحكومية والإجراءات التنفيذية المتعلقة بالتفتيش الجنائي على نظم الحاسوب والإنترنت، ودراسة كيفية تنظيم وتنسيق الجهود بين الجهات المختلفة المعنية بهذا المجال في كل من مصر والسعودية.

- الآليات القضائية المتاحة للتحقيق والمحاكمة في قضايا التفتيش الجنائي على نظم الحاسوب والإنترنت، وتحليل كيفية تطبيق وتفسير القوانين المعمول بها والقرارات القضائية ذات الصلة في كل بلد.
- تركز إشكالية الدراسة على تحليل هذه التحديات والبحث في الفروق والتشابهات بين مصر والسعودية في مجال التفتيش الجنائي على نظم الحاسوب والإنترنت، مما سيسهم في إثراء المعرفة القانونية وتعزيز التوجهات والسياسات المستقبلية في هذا المجال في البلدين.
- التشريعات والأنظمة القانونية المتعلقة بالتفتيش الجنائي على نظم الحاسوب والإنترنت في مصر والسعودية، بما في ذلك القوانين واللوائح والقرارات القضائية ذات الصلة. وتهدف الدراسة إلى تحليل هذه التشريعات وتقييم مدى فعاليتها في التعامل مع التحديات القانونية الناشئة عن التفتيش الجنائي على الأنظمة الحاسوبية وشبكات الإنترنت.
- حقوق المستخدمين والأفراد في ضوء التفتيش الجنائي على نظم الحاسوب والإنترنت، بما في ذلك حماية الخصوصية والحق في الأمانة والحفاظ على البيانات الشخصية. تهدف الدراسة إلى تحليل مدى احترام هذه الحقوق وتطبيقها في كل من مصر والسعودية.

أهمية الدراسة

تأتي أهمية هذه الدراسة نظراً للتحديات المتزايدة في مجال التفتيش الجنائي على نظم الحاسوب وشبكات الإنترنت في مصر والمملكة العربية السعودية. يعكس التطور السريع في التكنولوجيا والاعتماد المتزايد على الحواسيب والإنترنت في العديد من جوانب الحياة اليومية التحديات التي تواجه الجهات القانونية والأمنية في مواجهة الجرائم المعلوماتية وحماية البيانات والأفراد.

توفر هذه الدراسة إسهاماً هاماً في البحث القانوني والتطبيقي بالكشف عن الاختلافات والتشابهات في النظم القانونية المتعلقة بالتفتيش الجنائي على نظم الحاسوب والإنترنت في مصر والمملكة العربية السعودية. من خلال دراسة المقارنة بين البلدين، يتم تحديد العوامل التي تؤثر في تطبيق وتنفيذ التشريعات والسياسات المتعلقة بالتفتيش الجنائي وتقييم مدى فعاليتها في مكافحة الجرائم المعلوماتية وضمان الحماية القانونية للمستخدمين والأفراد.

علاوة على ذلك، تعزز الدراسة الفهم العميق للمفاهيم القانونية والقضايا الأخلاقية المرتبطة بالتفتيش الجنائي على نظم الحاسوب والإنترنت في سياق القانون الجنائي وحقوق الفرد. بواسطة تحليل النظم القانونية الجنائية والتفتيش الجنائي على نظم الحاسوب والإنترنت في مصر والمملكة العربية السعودية يمكن أن يكون له تأثير كبير على العديد من الجوانب القانونية والاجتماعية والاقتصادية في البلدين. لذلك، **تأتي أهمية هذه الدراسة على النحو التالي:**

- **المساهمة في تطوير القانون الجنائي:** يعمل هذا البحث على تحليل التشريعات والأنظمة المتعلقة بالتفتيش الجنائي على نظم الحاسوب والإنترنت في مصر والمملكة العربية السعودية. من خلال دراسة المقارنة بين البلدين، يمكن تحديد نقاط القوة والضعف في القوانين وتوصيات لتعزيزها وتحسينها بما يتوافق مع التحديات الحديثة التي تنشأ من استخدام التكنولوجيا الحديثة في الجرائم المعلوماتية.
- **حماية الأمان السيبراني ومكافحة الجرائم المعلوماتية:** تعد الحواسيب وشبكات الإنترنت أدوات أساسية في حياة الأفراد والمؤسسات، ولكنها أيضاً تعرض للعديد من التهديدات السيبرانية والجرائم المعلوماتية. من خلال فهم الإطار القانوني والإجرائي المتعلق بالتفتيش الجنائي، يمكن تعزيز قدرة البلدين على مكافحة الجرائم المعلوماتية وحماية الأمان السيبراني للمواطنين والمؤسسات.
- **التعاون الدولي في مجال الجرائم المعلوماتية:** يمثل التفتيش الجنائي على نظم الحاسوب والإنترنت تحدياً دولياً يتطلب التعاون والتنسيق بين البلدان. من خلال دراسة المقارنة بين مصر والمملكة العربية السعودية ، يمكن تعزيز التفاهم والتعاون الدولي في مجال مكافحة الجرائم المعلوماتية. يمكن أن تسهم هذه الدراسة في توضيح الاختلافات والتشابهات في النظم القانونية بين البلدين وتحديد المجالات التي يمكن تعزيز التعاون فيها، مثل تبادل المعلومات والخبرات وتطوير البرامج التدريبية المشتركة.

- **حماية حقوق المستخدمين والأفراد:** تتعدد التحديات المتعلقة بحقوق المستخدمين والأفراد في ظل التفتيش الجنائي على نظم الحاسوب والإنترنت، مثل حق الخصوصية وحماية البيانات الشخصية. [1]يهدف هذا البحث إلى تحليل الإجراءات المتبعة في كل من مصر والمملكة العربية السعودية لضمان احترام حقوق المستخدمين وتوفير آليات فعالة لحمايتها.
- **الإسهام في السياسات العامة والتشريعات المستقبلية:** من خلال تحليل القوانين والأنظمة القائمة وتقييمها، يمكن أن تقدم هذه الدراسة توصيات قيمة لتحسين السياسات العامة والتشريعات المستقبلية المتعلقة بالتفتيش الجنائي على نظم الحاسوب والإنترنت. [2]يتمثل الهدف في تطوير أطر قانونية فعالة تلبي تحديات العصر الرقمي وتحمي حقوق المستخدمين وتعزز الأمن السيبراني.

باختصار، تتمثل أهمية هذه الدراسة في فهم الإطار القانوني والتحديات التي تواجه التفتيش الجنائي على نظم الحاسوب والإنترنت في مصر والمملكة العربية السعودية، وتقديم توصيات قانونية وسياسية لتعزيز التعاون الدولي وتقديم توصيات قانونية وسياسية لتعزيز التعاون الدولي وحماية حقوق

[1] يوسف أوراها ياقو وعبد الناصر أحمد وحسن نعمة جعفر – المقدمة الغنية في الحاسبات الإلكترونية – مركز الفارابي – بغداد – ١٩٩٨م.

[2] ياكوف ميخايلو فيتش بيلسون – الإنتربول في الصراع ضد الجريمة الجنائية – ترجمة وإعداد : عماد محمود طحينة ومازن محمد نفاع – دار معد للنشر والتوزيع – دمشق – ١٩٩١م.

المستخدمين والأفراد وتعزيز الأمان السيبراني. تساهم هذه الدراسة في تطوير الممارسات القانونية والسياسات المتعلقة بالتفتيش الجنائي على نظم الحاسوب والإنترنت، وتعمل على تعزيز التوعية بأهمية حماية البيانات والخصوصية في العصر الرقمي.

بالإضافة إلى ذلك، توفر هذه الدراسة إطاراً قانونياً وتحليلًا مقارنًا بين مصر والمملكة العربية السعودية، مما يمكن الباحثين والمهتمين بالمجال القانوني من استخدامه كمرجع قيم في الأبحاث المستقبلية وصياغة السياسات والتشريعات. يعمل هذا التحليل المقارن على توضيح الأفضليات والتحسينات الممكنة في النظم القانونية لكل بلد، مما يسهم في تطوير التشريعات المستقبلية وتعزيز فعالية التفتيش الجنائي على نظم الحاسوب والإنترنت.

بشكل عام، تركز أهمية هذه الدراسة القانونية على تعزيز فهمنا للإطار القانوني والتحديات المتعلقة بالتفتيش الجنائي على نظم الحاسوب والإنترنت في مصر والمملكة العربية السعودية، وتقديم توصيات لتعزيز التعاون الدولي، وحماية حقوق المستخدمين والأفراد، وتحسين الأمان السيبراني، وتطوير السياسات والتشريعات المستقبلية في هذا المجال.

أهداف الدارسة.

1. تحليل وفهم الإطار القانوني للتفتيش الجنائي على نظم الحاسوب والإنترنت في كل من مصر والمملكة العربية السعودية. يهدف ذلك إلى فهم التشريعات واللوائح المعمول بها والمرجعيات القانونية ذات الصلة في البلدين.[1]
2. تحديد وتحليل التحديات والصعوبات التي تواجه التفتيش الجنائي على نظم الحاسوب والإنترنت في كل من مصر والمملكة العربية السعودية. يهدف ذلك إلى تحديد النقاط الضعيفة والفجوات في الأنظمة القانونية الحالية والعمل على توفير الحلول المناسبة لتلك التحديات.
3. إجراء تحليل مقارن بين الممارسات والأنظمة القانونية للتفتيش الجنائي على نظم الحاسوب والإنترنت في كل من مصر والمملكة العربية السعودية. يهدف ذلك إلى تحديد الاختلافات والتشابهات بين البلدين وتحليل أفضل الممارسات والسياسات القانونية.
4. توصيف وتقييم فعالية التشريعات والسياسات الحالية المتعلقة بالتفتيش الجنائي على نظم الحاسوب والإنترنت في كل من مصر والمملكة العربية السعودية. يهدف ذلك إلى تحديد النجاحات والعوائق التي تواجه تنفيذ تلك التشريعات والسياسات، واقتراح التحسينات الممكنة.

[1] د ممدوح خليل البحر – أصول المحاكمات الجزائية الأردني – ط١ – دار الثقافة – عمان – ١٩٩٨م.

5. تطوير مجموعة من التوصيات والإرشادات القانونية لتعزيز التفتيش الجنائي على نظم الحاسوب والإنترنت في مصر والمملكة العربية السعودية. يهدف ذلك إلى تعزيز التعاون الدولي وحماية حقوق المستخدمين والأفراد،تحقيق التوازن بين حقوق الأفراد وحماية المجتمع فيما يتعلق بالتفتيش الجنائي على نظم الحاسوب والإنترنت. يهدف ذلك إلى ضمان أن التفتيش يتم وفقًا للقوانين والضوابط القانونية، مع مراعاة حقوق الخصوصية والحريات الفردية.
6. توفير أساس قانوني ومعرفي لتحسين قدرة الجهات التنظيمية والقضائية في مصر والمملكة العربية السعودية على مكافحة جرائم الحوسبة والجرائم المعلوماتية.[1] يهدف ذلك إلى تعزيز القدرة على التحقيق وجمع الأدلة الرقمية وتقديمها في المحاكم.
7. تعزيز التعاون والتبادل المعرفي بين مصر والمملكة العربية السعودية في مجال التفتيش الجنائي على نظم الحاسوب والإنترنت. يهدف ذلك إلى تعزيز التبادل الثقافي والتعاون المشترك في تحقيق العدالة الجنائية في هذا المجال.
8. توفير إطار قانوني لتطوير التشريعات والسياسات الحكومية المتعلقة بالتفتيش الجنائي على نظم الحاسوب والإنترنت في مصر والمملكة العربية السعودية. يهدف ذلك إلى تعزيز القدرة على مواجهة التحديات

[1] د. نائل عبد الرحمن صالح – محاضرات في قانون أصول المحاكمات الجزائية – ط ١ – دار الفكر العربي – عمان – ١٩٩٧م.

القانونية المستقبلية ومواكبة التقدم التكنولوجي والتطورات الجنائية ذات الصلة.

9. تسهم الدراسة في تعزيز المعرفة العلمية في مجال التفتيش الجنائي على نظم الحاسوب والإنترنت، وتوفير قاعدة معرفية متينة للباحثين والأكاديميين والممارسين في هذا المجال. يهدف ذلك إلى تطوير وتعزيز الثقة في النظام القضائي والجهات التنظيمية في مصر والمملكة العربية السعودية من خلال تحقيق الشفافية والعدالة في عمليات التفتيش الجنائي على نظم الحاسوب والإنترنت. يهدف ذلك إلى تعزيز الثقة العامة والاحترام للسلطة القانونية وتعزيز مبادئ حكم القانون.
10. تسهم الدراسة في حماية المجتمع والحد من جرائم الحوسبة والجرائم المعلوماتية في مصر والمملكة العربية السعودية. يهدف ذلك إلى تطوير الإجراءات والسياسات القانونية الفعالة التي تساهم في الكشف عن الجرائم الإلكترونية وملاحقة المتسببين فيها وتقديمهم للعدالة.
11. تعزيز التوعية القانونية والتثقيف المجتمعي حول أهمية التفتيش الجنائي على نظم الحاسوب والإنترنت. يهدف ذلك إلى رفع مستوى الوعي لدى الأفراد والمؤسسات بأهمية الامتثال للقوانين والقواعد القانونية ذات الصلة وتعزيز الثقافة القانونية في المجتمع.

12.تقديم مساهمة علمية وعملية للتشريعات والسياسات القانونية في مجال التفتيش الجنائي على نظم الحاسوب والإنترنت في مصر والمملكة العربية السعودية. [1]يهدف ذلك إلى تحسين وتطوير القوانين واللوائح المعمول بها وتعزيز فاعلية التنفيذ والتطبيق العملي لتلك التشريعات.

13.توفير قاعدة معرفية قوية وشاملة تدعم عمل الباحثين والمختصين في مجال التفتيش الجنائي على نظم الحاسوب والإنترنت في مصر والمملكة العربية السعودية و يهدف ذلك إلى توفير المصادر والمعلومات اللازمة للدراسات والأبحاث المستقبلية في هذا المجال وتعزيز التطور والابتكار في مجال التفتيش الجنائي على نظم الحاسوب والإنترنت.

14.تسهم الدراسة في تعزيز التعاون الدولي وتبادل الخبرات في مجال التفتيش الجنائي على نظم الحاسوب والإنترنت بين مصر والمملكة العربية السعودية والمجتمع الدولي. يهدف ذلك إلى بناء شبكة تواصل قوية وتعزيز التبادل الثقافي والتعاون المشترك في مكافحة الجرائم الإلكترونية على مستوى العالم.

15.تطوير التشريعات والسياسات القانونية لتعزيز الحماية القانونية للأفراد والمؤسسات في مجال التفتيش الجنائي على نظم الحاسوب والإنترنت.

[1] د. نعمان الخطيب – الوسيط في النظم السياسية والقانون الدستوري – ط١ – دار الثقافة – عمان – ١٩٩٩م.

يهدف ذلك إلى تعزيز الثقة في استخدام التكنولوجيا الرقمية وتحقيق التوازن بين الأمان القانوني والحرية الشخصية.

16. تعزيز التطبيق العملي للتشريعات والسياسات القانونية المتعلقة بالتفتيش الجنائي على نظم الحاسوب والإنترنت في مصر والمملكة العربية السعودية. [1] يهدف ذلك إلى تعزيز قدرة الجهات التنفيذية والقضائية في تنفيذ القوانين بشكل فعال وتحقيق العدالة والشفافية في العمليات القضائية.

17. تعزيز الحوكمة الرقمية وتطوير آليات الرقابة والمراقبة على نظم الحاسوب والإنترنت في مصر والمملكة العربية السعودية. يهدف ذلك إلى تحسين الأمن السيبراني ومكافحة الجرائم الإلكترونية .

تساؤلات الدراسة.

1. ما هي التشريعات والقوانين المعمول بها في مصر والمملكة العربية السعودية المتعلقة بالتفتيش الجنائي على نظم الحاسوب والإنترنت؟ وما هي الفروقات والتشابهات بينهما؟
2. ما هي الصلاحيات والاختصاصات القضائية والتنظيمية المتعلقة بالتفتيش الجنائي على نظم الحاسوب والإنترنت في كل من مصر والمملكة العربية السعودية؟ وكيف يتم تنظيم وتنفيذ هذه الصلاحيات في كل دولة؟

[1] د. نائل عبد الرحمن صالح – محاضرات في قانون أصول المحاكمات الجزائية – ط ١ – دار الفكر العربي – عمان – ١٩٩٧م.

3. ما هي الضوابط القانونية والقضائية المطبقة على التفتيش الجنائي على نظم الحاسوب والإنترنت في مصر والمملكة العربية السعودية؟ وكيف يتم ضمان احترام حقوق الخصوصية والحريات الفردية أثناء عمليات التفتيش؟
4. ما هي الإجراءات القانونية المتبعة في جمع الأدلة الرقمية واستخدامها في المحاكم في كل من مصر والمملكة العربية السعودية؟ وما هي الضوابط المفروضة على استخدام هذه الأدلة في عمليات التفتيش الجنائي؟
5. ما هي التحديات القانونية التي تواجه التفتيش الجنائي على نظم الحاسوب والإنترنت في كل من مصر والمملكة العربية السعودية؟ وكيف يمكن تعزيز التشريعات والسياسات القانونية للتغلب على هذه التحديات ومكافحة الجرائم الإلكترونية بشكل فعال؟
6. ما هي التجارب القضائية والقضايا السابقة المتعلقة بالتفتيش الجنائي على نظم الحاسوب والإنترنت في كل من مصر والمملكة العربية السعودية ؟
7. ما هي الآليات المتبعة للتعاون الدولي في مجال التفتيش الجنائي على نظم الحاسوب والإنترنت بين مصر والمملكة العربية السعودية؟ وما هي الاتفاقيات والمعاهدات الدولية التي تنظم هذا التعاون؟ وكيف يمكن تعزيز وتطوير هذه الآليات لمكافحة الجرائم الإلكترونية بشكل فعال؟

8. ما هي التقنيات والأدوات المستخدمة في عمليات التفتيش الجنائي على نظم الحاسوب والإنترنت في مصر والمملكة العربية السعودية؟ وما هي التحديات التقنية التي تواجه عمليات التحقيق الرقمي والتفتيش الجنائي؟ وكيف يمكن تحسين التقنيات المستخدمة وتطوير القدرات التقنية لتحقيق أفضل النتائج في هذا المجال؟
9. ما هي الآثار القانونية والاجتماعية للتفتيش الجنائي على نظم الحاسوب والإنترنت في مصر والمملكة العربية السعودية؟ وكيف يمكن تقييم تلك الآثار على الأفراد والمؤسسات والمجتمع في البلدين؟ وما هي التدابير اللازمة لتقليل الآثار السلبية وتعزيز الآثار الإيجابية للتفتيش الجنائي على نظم الحاسوب والإنترنت؟

منهج الدراسة.

انطلاقا من طبيعة الدراسة وأهدافها استخدم الباحث ما يلي:

1 .الجانب النظري:

استخدم الباحث المنهج الوصفي بطريقته العلمية الاستقرائية الاستنتاجية، فهي تجمع بين مرحلة استقراء الجزئيات ومراقبتها الاستخراج المقترحات واستنباط الحلول التي يتوصل بها الى نتائج منطقية وحلول مقبولة [1]

[1] عبد الوهاب إبراهيم أبو سليمان، كتابة البحث العلمي، (صياغة جديدة) مكتبة الرشد، الرياض ط10 , 2007 ص 33-64

في الجانب النظري للدراسة، سيستخدم الباحث المنهج الوصفي بطريقة علمية استقرائية استنتاجية. ستجمع هذه الطريقة بين مرحلتين رئيستين: مرحلة استقراء الجزئيات ومرحلة استخراج المقترحات واستنباط الحلول.

- **مرحلة استقراء الجزئيات:** في هذه المرحلة، سيقوم الباحث بدراسة وتحليل المعلومات المتاحة حول التفتيش الجنائي على نظم الحاسوب والإنترنت في مصر والمملكة العربية السعودية. سيقوم بجمع الأدبيات القانونية والأبحاث السابقة والتشريعات والسياسات والقرارات القضائية ذات الصلة. سيتم تحليل هذه المعلومات لاستخلاص الجزئيات المهمة والتفاصيل القانونية والفروض الأولية.
- **مرحلة استخراج المقترحات واستنباط الحلول:** بعد استقراء الجزئيات، سيقوم الباحث بتحليل ومراجعة البيانات والمعلومات التي تم جمعها. سيستخدم تقنيات تحليلية لاستنتاج النتائج المنطقية واستخلاص المقترحات والحلول المقبولة. [1]سيتم تحليل البيانات بشكل نظامي ودقيق لتوضيح الأنماط والاتجاهات والفروق بين مصر والمملكة العربية السعودية في مجال التفتيش الجنائي على نظم الحاسوب والإنترنت.

باستخدام المنهج الوصفي بطريقة الاستقراء الاستنتاجي، سيتم توضيح الأحداث والظواهر والمعالم المهمة في مجال التفتيش الجنائي على نظم الحاسوب

[1] د. نواف كنعان – حق المؤلف – النماذج المعاصرة لحق المؤلف ووسائل حمايته – ط ٣ – توزيع دار الثقافة – عمان – ٢٠٠٠م.

والإنترنت. سيتم تحليل المعطيات واستنتاج المقترحات والحلول التي تطبق بها على الواقع العملي في مصر والمملكة العربية السعودية. ستساهم هذه الطريقة في توضيح الأسس النظرية والمفاهيم المرتبطة بالتفتيش الجنائي على نظم الحاسوب والإنترنت، وفهم التحديات والتطورات في السياقين المقارنين.

سيتم تطبيق الأدوات والتقنيات القانونية المناسبة في استقراء الجزئيات وتحليل البيانات، مثل تحليل المحتوى القانوني، وتحليل السياسات العامة، وتحليل البيانات الكمية والكيفية. ستساهم هذه الأدوات في فهم التشريعات والسياسات المتبعة في مجال التفتيش الجنائي على نظم الحاسوب والإنترنت في كلا البلدين، وتحديد الفروق والتشابهات بينهما.

بالإضافة إلى ذلك، ستشمل منهجية الدراسة مراجعة الدراسات السابقة والأبحاث المشابهة في هذا المجال، وذلك لبناء قاعدة نظرية قوية ولملاءمة نتائج الدراسة مع المعرفة الحالية. سيتم استخدام الأدبيات القانونية والمقارنة بين النظم القانونية والتشريعات المعمول بها في مصر والمملكة العربية السعودية لتحليل السياق المحلي وتحديد الاختلافات والتحديات المحتملة.

علاوة على ذلك، سيتم الاعتماد على دراسة ميدانية تشمل جمع البيانات من مصادر متعددة، مثل مقابلات مع الخبراء والمسؤولين القانونيين، واستطلاعات للرأي، وتحليل التقارير الحكومية والإحصائيات ذات الصلة. سيتم تحليل هذه البيانات بدقة واستخدامها لدعم المناقشة والتحليل واستنباط النتائج .

منهج الدراسة سيسمح بتحقيق الأهداف المحددة للبحث ومناقشة التساؤلات البحثية المطروحة. ستساهم الطريقة الوصفية بطريقة الاستقراء الاستنتاجي في فهم وتحليل التفتيش الجنائي على نظم الحاسوب والإنترنت في مصر والمملكة العربية السعودية، وتحديد الفروق والتشابهات بينهما. سيتم استخدام الأدوات والتقنيات القانونية المناسبة لتحليل البيانات واستنباط النتائج المنطقية.

من المتوقع أن تساهم الدراسة في إثراء المعرفة القانونية والتقنية المتعلقة بالتفتيش الجنائي على نظم الحاسوب والإنترنت، وتقديم توصيات قانونية ملموسة لتحسين التشريعات والسياسات المتعلقة بهذا الجانب في مصر والمملكة العربية السعودية. كما ستوفر الدراسة قاعدة نظرية قوية تساهم في البحوث والدراسات المستقبلية في هذا المجال.

يجب ملاحظة أنه قد يتطلب منهج الدراسة جمع البيانات والمعلومات من مصادر مختلفة والاعتماد على مراجعة الأدبيات والتشريعات والسياسات المتعلقة بالتفتيش الجنائي على نظم الحاسوب والإنترنت. يجب أيضاً أن يتم التعامل مع المعلومات بسرية واحترام للأخلاقيات البحثية والتشريعات المعمول بها في مصر والمملكة العربية السعودية.

باختصار، منهج الدراسة سيعتمد على الطريقة الوصفية بطريقة الاستقراء الاستنتاجي وستشمل استقراء الجزئيات واستخراج المقترحات واستنباط الحلول

2 .الجانب التطبيقي:

إستخدم الباحث المنهج التحليلي [1]،للمحتوى والمضمون من خلال عدد من القضايا المتعلقة بموضوع الدراسة.

تم استخدام الباحث المنهج التحليلي لتحليل ودراسة المحتوى والمضمون المتعلق بعدد من القضايا المتعلقة بموضوع الدراسة. ستكون هذه القضايا محددة بناءً على الأهداف والتساؤلات البحثية، وستعكس التحديات والتطورات

[1] وهو منهج يسلك سبيل المقارنة بين صور مختلفة من الأحداث والظواهر. وتعد واحدة من الإسهامات التي قدمها علماء الاجتماع الفرنسيون. إذ تعتبر المقارنة جزأ جوهرية في نظر المفكر سان سيمون Saint Simon لأنها الوسيلة الوحيدة التي تمكن الباحث من الاستفادة بالمعطيات التي يظهرها البحث. كما تمكنه أيضا من التعرف على العناصر الثابتة والعناصر المتغيرة للظواهر الاجتماعية. كذلك فقد توسع العالم إميل دور كايم Emile Durkheim في تطبيق المنهج المقارن. إذ يعتبره أكثر ملاءمة لطبيعة الظواهر الاجتماعية. لأنه يكشف لنا العلاقات السلبية بين هذه الظواهر. ذلك أن الوصف والتقدير دون مقارنة الظواهر خلال مرحلة معينة يفقدها قدرتها على إظهار الارتباط السببي بين الظواهر المختلفة. ويلاحظ أن أسلوب الباحث لا يتوقف عند حد إظهار أوجه الاتفاق والاختلاف في كل نقطة من نقاط البحث وبيان موقف التشريعات المختلفة منها، بل يتعدى ذلك إلى تفسير أسباب هذا الاتفاق أو الاختلاف، فلا شك أن وضع علامة الاستفهام لماذا هي التي تعطي الدراسة المقارنة معنى البحث العلمي الصحيح. لذا يقال إنه عندما لا يكون هناك مجال لنضال فكري يفرض على الوقائع أن تكشف عن معانيها، فإنه لا يكون هناك ما يمكن أن يسمى بالبحث العلمي. انظر: د. هلالي عبد اللاه أحمد: حقوق الطفولة في الشريعة الإسلامية "دراسة مقارنة بالقانون الوضعي"، رسالة دكتوراه، كلية حقوق بني سويف، جامعة القاهرة، 1415ه – 1994م، ص 31.

المتعلقة بالتفتيش الجنائي على نظم الحاسوب والإنترنت في مصر والمملكة العربية السعودية.

يتضمن الجانب التطبيقي للدراسة ما يلي:

- تحديد القضايا المهمة: قام الباحث بتحديد عدد من القضايا المهمة المرتبطة بالتفتيش الجنائي على نظم الحاسوب والإنترنت في كلا البلدين. قد تتضمن هذه القضايا قضايا قانونية وتشريعية وتقنية وأمنية وأخلاقية. سيتم اختيار هذه القضايا بناءً على الأهداف البحثية والتساؤلات البحثية.
- جمع البيانات والمعلومات: سيتم جمع البيانات والمعلومات المتعلقة بالقضايا المحددة من مصادر مختلفة. قد يتضمن ذلك مراجعة التشريعات والسياسات والتقارير الحكومية والقرارات القضائية ذات الصلة. سيتم جمع المعلومات بطرق متنوعة مثل المقابلات مع الخبراء والمشاركين ذوي الخبرة واستطلاعات الرأي وتحليل المحتوى للوثائق والمقالات العلمية.[1]
- تحليل البيانات: تم تحليل البيانات والمعلومات التي تم جمعها باستخدام الأدوات والتقنيات التحليلية المناسبة تم تطبيق البحث المتعلق بالمحتوى والتحليل الدلالي للمواد المجمعة.وتم تمييز الأنماط والمفاهيم الرئيسية المستخدمة في القضايا المدروسة، وتم فحص العلاقات

[1] د. نواف كنعان – حق المؤلف – النماذج المعاصرة لحق المؤلف ووسائل حمايته – ط ٣ – توزيع دار الثقافة – عمان – ٢٠٠٠م.

والترابطات بين العناصر المختلفة. سيساهم هذا التحليل في استخلاص المعاني والمفاهيم المشتركة والاختلافات بين البلدين.

- تحليل النتائج: سيتم تحليل النتائج التي تم الوصول إليها من خلال التحليل والمناقشة. وتم تحليل النتائج بناءً على الأطروحات النظرية والمعطيات القانونية والمعلومات الواردة من الدراسات السابقة. ستساهم هذه العملية في استنباط الاستنتاجات والمقترحات المقنعة التي تتعلق بالتفتيش الجنائي على نظم الحاسوب والإنترنت في مصر والمملكة العربية السعودية.[1]
- توصيات واستنتاجات: تم تقديم توصيات عملية واستنتاجات مبنية على النتائج التحليلية والأدلة القانونية والأدبيات السابقة حيث تتضمن هذه التوصيات مقترحات لتحسين التشريعات والسياسات المتعلقة بالتفتيش الجنائي على نظم الحاسوب والإنترنت في كلا البلدين، وتوجيهات لتعزيز الوعي والتدريب والتعاون الدولي في هذا المجال.

باختصار، الجانب التطبيقي للدراسة يستخدم المنهج التحليلي لتحليل واستنتاج البيانات المجمعة من مصادر مختلفة ستساهم هذه العملية في توفير رؤى وتوصيات عملية لتعزيز التفتيش الجنائي على نظم الحاسوب والإنترنت في مصر والمملكة العربية السعودية.

[1] د.هدى حامد قشقوش – الحماية الجنائية للتجارة الإلكترونية عبر الإنترنت – دار النهضة العربية – القاهرة – ٢٠٠٠م.

مفاهيم الدراسة.

في سياق الدراسة المقارنة للتفتيش الجنائي على نظم الحاسوب والإنترنت في مصر والمملكة العربية السعودية، يتضمن المفاهيم الرئيسية التالية:

- **التفتيش الجنائي:**

يشير إلى العملية القانونية التي تتم بموجبها التحقيق والتفتيش في الأنظمة والمعلومات المخزنة على الأجهزة الحاسوبية وعبر الشبكة الإلكترونية. يهدف إلى الكشف عن الجرائم المعلوماتية وجمع الأدلة وتقديمها للمحاكم في إطار إجراءات قانونية.[1]

- **نظم الحاسوب والإنترنت:**

يشمل الأجهزة الحاسوبية والشبكات والأنظمة المعلوماتية المرتبطة بالإنترنت. تشمل هذه النظم الأجهزة الشخصية، والخوادم، والشبكات المحلية والواسعة، والبرمجيات، والمواقع الإلكترونية، والتطبيقات الرقمية.[2]

- **الجريمة المعلوماتية:**

تشمل أي نشاط يتعلق بالتلاعب أو الاختراق أو استغلال الأنظمة الحاسوبية والشبكات الإلكترونية بطرق غير قانونية، سواء كان ذلك لسرقة المعلومات،

[1] هشام محمد فريد رستم – قانون العقوبات ومخاطر تقنية المعلومات – ط١ – مكتبة الآلات الحديثة – أسيوط – ١٩٩٢م.

[2] د. هلالي عبد اللاه أحمد – تفتيش نظم الحاسب الآلـــى وضمانات المتهم المعلوماتي – دراسة مقارنة – ط١ – دار النهضة العربية – القاهرة –١٩٩٧م.

أو تعطيل الخدمات، أو الاحتيال الإلكتروني، أو التجسس الصناعي، وغيرها من الأنشطة غير المشروعة.[1]

- **الإجراءات القانونية:**

تشير إلى الخطوات والإجراءات المنصوص عليها في القوانين والتشريعات المعمول بها في كل من مصر والمملكة العربية السعودية للتحقيق والتفتيش الجنائي على نظم الحاسوب والإنترنت. تشمل ضوابط جمع الأدلة وحماية حقوق المتهمين وإجراءات المحاكمة.[2]

- **التشريع القانوني:**

يشير إلى المجموعة من القوانين والتشريعات المتعلقة بتنظيم التفتيش الجنائي على نظم الحاسوب والإنترنت في كل من مصر والمملكة العربية السعودية. يتضمن هذا المفهوم القوانين الجنائية المنصوص عليها في النظام القانوني لكل دولة، بما في ذلك التشريعات المتعلقة بالجرائم

[1] أسامة بن غانم العبيدي. نديم محمد حسن الترزي، سلطات النيابة العامة في الجرائم المعلوماتية، مجلة أندلس للعلوم الاجتماعية والإنسانية، العدد 19، مجلد 15، أبريل 2017

[2] د. محمد الأمين البشري – الأدلة الجنائية الرقمية – مفهومها ودورها فـــي الإثبات – المجلة العربية للدراسات الأمنية والتدريب – المجلد ١٧-- العدد ٣٣– السنة ١٧ – الرياض – أبريل ٢٠٠٢م.

المعلوماتية وحقوق المستخدمين والإجراءات القانونية المطبقة على التفتيش الجنائي.[1]

- **حقوق الأفراد:**

تعني حقوق الأفراد المتأثرين بعمليات التفتيش الجنائي على نظم الحاسوب والإنترنت. يشمل ذلك حقوق الخصوصية وحق الحماية من التعدي غير المشروع على المعلومات الشخصية، فضلاً عن حقوق المتهمين والمشتبه بهم في الحصول على إجراءات قانونية عادلة وحق التعامل[2] مع الأدلة والتصرف فيها.

- **العمل التشريعي:**

يشمل تحليل القوانين والتشريعات المعمول بها في مصر والمملكة العربية السعودية وفهم كيفية تطبيقها في مجال التفتيش الجنائي على نظم الحاسوب والإنترنت. يهدف إلى فهم الفروق والتشابه في النهج التشريعي ومعرفة مدى توافق القوانين مع المعايير الدولية في هذا المجال.

- **التشريعات الدولية:**

تشمل المعاهدات والاتفاقيات الدولية التي تنظم التفتيش الجنائي على نظم الحاسوب والإنترنت. تهدف هذه التشريعات إلى توحيد المعايير والمبادئ

[1] د. محمد الأمين البشري – الأدلة الجنائية الرقمية – مفهومها ودورها فـــى الإثبات – المجلة العربية للدراسات الأمنية والتدريب – المجلد ١٧-- العدد ٣٣- السنة ١٧ – الرياض – أبريل ٢٠٠٢م.

[2] د. محمد عيد الغريب – الاختصاص القضائي لمأمور الضبط القضائي فى الأحوال العادية والاستثنائية – القاهرة –١٩٩٩ /٢٠٠٠م.

القانونية الدولية لحماية البيانات الشخصية ومكافحة الجرائم المعلوماتية عبر الحدود.[1]

- **السياسات العامة:**

تشمل السياسات والإجراءات التي تتبعها الحكومات والمؤسسات العامة في مصر والمملكة العربية السعودية للتعامل مع قضايا التفتيش الجنائي على نظم الحاسوب والإنترنت. تهدف هذه السياسات إلى وضع الإطار القانوني والتشريعي اللازم للتفتيش الجنائي، وتحديد صلاحيات الجهات المعنية، وضمان حماية الحقوق والخصوصية للأفراد والمؤسسات، وتعزيز التعاون والتنسيق بين الجهات المختلفة.[2]

- **التقنيات الحديثة:**

تشمل استخدام التكنولوجيا والأدوات المتقدمة في عمليات التفتيش الجنائي على نظم الحاسوب والإنترنت، مثل تقنيات استرجاع البيانات، وتحليل الأدلة الرقمية، والتحقق من الهوية الرقمية، وتتبع الأنشطة الإلكترونية. تهدف هذه التقنيات إلى تسهيل وتحسين عمليات التفتيش وتحقيق نتائج دقيقة وموثوقة.[3]

---

[1] د.محمد فهمي طلبة وآخرون – دائرة المعارف الحاسب الإلكتروني – مجموعة كتب دلتا – مطابع المكتب المصري الحديث – القاهرة – ١٩٩١م.

[2] د. محمد كامل إبراهيم – النظرية العامة للبطلان في قانون الإجراءات الجنائية – دار النهضة العربية – القاهرة – ١٩٨٩م.

[3] د. محمد كامل إبراهيم – النظرية العامة للبطلان في قانون الإجراءات الجنائية – دار النهضة العربية – القاهرة – ١٩٨٩م.

- **التعاون الدولي:**

يشمل التعاون والتنسيق بين الجهات القانونية والأمنية في مصر والمملكة العربية السعودية مع الجهات المعنية دولياً في مجال التفتيش الجنائي على نظم الحاسوب والإنترنت. يهدف التعاون الدولي إلى مشاركة الخبرات والمعلومات، [1]وتبادل الأفكار والممارسات الجيدة، وتعزيز قدرة الدولتين على مكافحة الجرائم المعلوماتية على المستوى الدولي.

- **الأمن السيبراني:**

يتعلق بتوفير الحماية والأمان للأنظمة الحاسوبية والشبكات الإلكترونية من التهديدات السيبرانية والاختراقات الإلكترونية. يتضمن هذا المفهوم تطوير استراتيجيات الأمن السيبراني، وتحديد السياسات والإجراءات الفنية والتنظيمية لحماية الأنظمة والبيانات والمعلومات من الاختراقات والتلاعب غير المشروع بها.[2]

- **تحليل الأدلة الرقمية:**

يشير إلى العملية القانونية والتقنية لتحليل الأدلة الرقمية المستخرجة من أنظمة الحاسوب والإنترنت. يتضمن ذلك استخدام تقنيات متقدمة لاسترجاع وتحليل البيانات والملفات الرقمية المتعلقة بالجرائم المعلوماتية،

---

[1] محمد محمد شتا – فكرة الحماية الجنائية لبرامج الحاسب الآلي – دار الجامعة الجديدة – الإسكندرية – ٢٠٠١م.

[2] د. محمود شريف بسيوني ود. عبد العظيم الوزير – الإجراءات الجنائية في النظم القانونية العربية وحماية حقوق الإنسان – ط ١ – دار العلم للملايين – بيروت – ١٩٩١م.

بهدف جمع الأدلة القانونية وتوفيرها للمحاكم لاتخاذ القرارات القانونية المناسبة.[1]

- **الاستجابة للحوادث السيبرانية:**

يتعلق بالتحضير والاستجابة الفعالة للحوادث السيبرانية والاختراقات الأمنية. يشمل ذلك إعداد خطط الطوارئ والاستجابة، وتشكيل فرق الاستجابة السريعة، وتنفيذ إجراءات استرجاع الأنظمة وتأمين البيانات بعد وقوع الحادث السيبراني.[2]

- **التدريب والتوعية:**

يعتبر التدريب والتوعية بالأمن السيبراني جزءًا أساسيًا من الجانب التطبيقي للدراسة. يهدف إلى توعية المستخدمين بأفضل الممارسات الأمنية، وتعزيز وعيهم بالتهديدات السيبرانية، وتطوير مهارات الفرق الفنية في مجال التحقيق والتفتيش الجنائي على الأنظمة الحاسوبية[3]

[1] د. محمود محمود مصطفى – شرح قانون الإجراءات الجنائية – ط٩ – دار النهضة العربية – القاهرة – ١٩٦٦م.

[2] د.محمود نجيب حسني – شرح قانون الإجراءات الجنائية – ط٣ – دار النهضة العربية – القاهرة – ١٩٩٦م /ط٢ – ١٩٨٨م.

[3] د.مدحت رمضان – جرائم الاعتداء على الأشخاص والإنترنت – دار النهضة العربية – القاهرة – ٢٠٠٠م.

فصل تمهيدي

الحاسوب والجريمة المعلوماتية

مقدمة

يشهد العصر الحديث تطوراً هائلًا في مجال التكنولوجيا الحاسوبية، وقد أدى ذلك إلى توفير فرص وتحسينات كبيرة في مختلف جوانب الحياة اليومية والأعمال التجارية والتواصل. ومع هذا التطور، ظهرت أيضاً جرائم جديدة تتعلق بالاستخدام غير القانوني للحاسوب والانترنت، وهو ما يعرف بالجرائم المعلوماتية.

في هذا الفصل التمهيدي، سنقوم بتقديم نظرة عامة على مفهوم الجريمة المعلوماتية وأهميتها وتأثيرها على المجتمع والاقتصاد. سنستعرض أيضاً تاريخ تطور التكنولوجيا الحاسوبية وأهمية الحاسوب في العصر الحديث، وكيفية تأثيرها على الحياة اليومية والأعمال التجارية والتواصل[1].

سنقوم أيضاً بعرض أنواع الجرائم المعلوماتية المشتركة، مثل الاختراقات القرصنة، والاحتيال الإلكتروني، وسرقة الهوية، وانتشار البرامج الضارة، وغيرها. سنستعرض أدوات وتقنيات الاختراق التي يستخدمها المهاجمون في الجرائم المعلوماتية، مما يساعد على فهم طبيعة هذه الجرائم والتحديات التي تواجه مكافحتها.

[1] د. محمود نجيب حسني – الدستور والقانون الجنائي – دار النهضة العربية – القاهرة – ١٩٩٢م.

وسنتحدث عن التأثيرات القانونية والاقتصادية للجرائم المعلوماتية على المؤسسات والأفراد، ونسلط الضوء على تكاليف مكافحة هذه الجرائم وتعويض الخسائر التي تنجم عنها. سنستعرض أيضاً التشريعات والقوانين المحلية والدولية.

تعريف الجريمة المعلوماتية:

تعتبر الجريمة المعلوماتية أو الجريمة الإلكترونية أو الجريمة المتعلقة بتكنولوجيا المعلومات من الأعمال الجنائية التي تتم باستخدام وسائل التكنولوجيا الحديثة وتستهدف البيانات والنظم المعلوماتية. تتميز الجريمة المعلوماتية بأنها تشمل أنشطة غير قانونية تتعلق بالاختراق الإلكتروني، وسرقة المعلومات، وتلفيق البيانات، والاحتيال الإلكتروني، والتجسس الإلكتروني، والقرصنة الإلكترونية، وانتشار الفيروسات الحاسوبية، والاعتداء على خصوصية الأفراد والمؤسسات، وغيرها من الأنشطة غير المشروعة التي تستهدف النظم المعلوماتية وتسبب أضراراً جسيمة.[1]

حيث تم تحليل ودراسة طرق التفتيش الجنائي على نظم الحاسوب والإنترنت بناءً على نماذج وأساليب مقارنة. يهدف البحث إلى استكشاف وتحليل الإجراءات الجنائية المتعلقة بالتحقيق في الجرائم المعلوماتية وجمع الأدلة الرقمية، وتقديم تحليل مقارن بين الممارسات والتشريعات القانونية في مجال التفتيش الجنائي على نظم الحاسوب والإنترنت في سياقات مختلفة. يهدف

[1] د.مدحت رمضان – جرائم الاعتداء على الأشخاص والإنترنت – دار النهضة العربية – القاهرة – ٢٠٠٠م.

البحث إلى توفير رؤية شاملة للممارسات الحالية والتحديات المرتبطة بالتفتيش الجنائي في هذا المجال وتقديم توصيات لتعزيز فعالية التحقيقات وتعزيز الأمان الرقمي وحماية البيانات والأنظمة الإلكترونية.

تهدف الدراسةإلى تقديم نتائج الدراسة المقارنة وتحليلها، وتوصيات لتعزيز ممارسات التفتيش الجنائي على نظم الحاسوب والإنترنت. يتم تحليل التشريعات الوطنية والدولية ذات الصلة، وتحديد أفضل الممارسات والأساليب المعتمدة في مختلف السياقات القانونية.

علاوة على ذلك، يتم تناول موضوعات أخرى ذات صلة مثل حقوق الأفراد والحماية القانونية للمعلومات الرقمية، والتحديات التقنية والقانونية التي يواجهها فريق التحقيقات الجنائية، وتأثير التكنولوجيا الجديدة مثل تقنيات التشفير والتحليل الرقمي على عمليات التفتيش الجنائي.[1]

تلخص هذه الدراسة المقارنة وتحليلها لتوفير فهم عميق للتفتيش الجنائي على نظم الحاسوب والإنترنت وتوصيات لتعزيز الإجراءات والتشريعات القانونية في هذا المجال. يهدف البحث إلى تعزيز قدرة الجهات القضائية والأجهزة الأمنية على مكافحة الجرائم المعلوماتية وحماية البيانات والأنظمة الحاسوبية، وتعزيز الثقة العامة في استخدام التكنولوجيا الرقمية.

[1] محمد علي سالم عياد الحلبي – الوسيط في شرح قانون أصول المحاكمات الجزائية – ج1 – مكتبة دار الثقافة للنشر – عمان – ١٩٩٦م.

- **تطور الحوسبة:**

يتعلق التطور التكنولوجي للحوسبة بالتقدم المستمر والمتسارع في مجال التكنولوجيا الحاسوبية واستخدام الحواسيب. يشمل هذا التطور تطوير الأجهزة الحاسوبية والبرمجيات، وزيادة سرعة المعالجات، وزيادة سعة التخزين، وتطوير وسائل الاتصال والشبكات، وتحسين أداء الأنظمة الحاسوبية والتطبيقات.[1]

تعد الحوسبة أحد العناصر الأساسية في العصر الحديث، حيث لها أهمية كبيرة في العديد من المجالات. تسهم التكنولوجيا الحاسوبية في تسريع العمليات، وتحسين الكفاءة والإنتاجية، وتمكين التواصل السريع والعالمي، وتوفير وسائل تخزين ومعالجة بشكل فعال، وتمكين الابتكار والتطوير في مجالات مختلفة مثل الطب، والتعليم، والعلوم، والتجارة، والصناعة، والترفيه.[2]

تأثير التكنولوجيا الحاسوبية على الحياة اليومية والأعمال التجارية والتواصل:

- ❖ تطور التكنولوجيا الحاسوبية قد أحدث تغييرات جذرية في حياة الناس وأساليب التفاعل والتواصل في المجتمع الحديث. فبفضل الحواسيب والإنترنت، أصبح من الممكن الوصول إلى المعلومات بسرعة وسهولة، وتبادل البيانات والملفات عبر الشبكات، وإجراء العمليات

[1] د.محمد عبد الظاهر حسين – الاتجاهات الحديثة في حماية برامج الكمبيوتر المعلوماتية – دار النهضة العربية – القاهرة – ٢٠٠٠/٢٠٠١م.

[2] د. محمد محدة – ضمانات المتهم أثناء التحقيق ج 3+٣٢ – ط١ – دار الهدى – الجزائر – ١٩٩٢م.

المالية والتجارية عبر الإنترنت، والتواصل مع الآخرين عبر وسائل التواصل الاجتماعي.[1]

- ❖ تأثير التكنولوجيا الحاسوبية يمتد أيضاً إلى الأعمال التجارية، حيث يتيح استخدام الحواسيب والبرمجيات الحديثة تحسين إدارة العمليات، وتحليل البيانات، وتوسيع نطاق العمل والوصول إلى العملاء عبر الإنترنت، وتطوير تطبيقات ومنصات إلكترونية لتحسين تجربة العملاء.[2]

بشكل عام، يمكن القول إن التكنولوجيا الحاسوبية قد غيرت طريقة حياتنا وعملنا، وأصبحت جزءًا أساسيًا في تقدم المجتمعات والاقتصادات. ومع استمرار التطور التكنولوجي، من المتوقع أن يستمر تأثير الحوسبة في التغير والتطور في المستقبل.[3]

- **تاريخ تطور التكنولوجيا الحاسوبية:**

يعود تاريخ تطور التكنولوجيا الحاسوبية إلى العقود الأولى من القرن العشرين، حيث تم تطوير أول حواسيب بآلية ميكانيكية واستخدام الصمامات الثنائية كوحدات تخزين. مع مرور الوقت، تطورت التقنيات وظهرت

---

[1] د. محمود نجيب حسني – الدستور والقانون الجنائي – دار النهضة العربية – القاهرة – ١٩٩٢م.

[2] د.محمد علي عياد الحلبي – الحرية الشخصية أثناء التحري والاستدلال في القانون المقارن – ط ١ – منشورات ذات السلاسل – الكويت (د.ت).

[3] د.محمد علي عياد الحلبي – الحرية الشخصية أثناء التحري والاستدلال في القانون المقارن – ط ١ – منشورات ذات السلاسل – الكويت (د.ت).

الحواسيب الإلكترونية التي تستخدم المصابيح الكهرونية والمفاتيح المغناطيسية.[1]

في العقود اللاحقة، شهدت التكنولوجيا الحاسوبية تطوراً جذرياً، حيث ظهرت الدوائر المتكاملة وتقنية النانو وزادت سرعة المعالجات وتقلص حجم الأجهزة. تطورت أنظمة التشغيل وظهرت الشبكات الحاسوبية والإنترنت، مما أدى إلى توسع استخدام الحواسيب في الحياة اليومية والأعمال التجارية والتواصل.[2]

في السياق القانوني، تُجرى الدراسة بهدف تحليل ومقارنة الممارسات القانونية المتعلقة بالتفتيش على أنظمة الحاسوب والإنترنت. تهدف هذه الدراسة إلى فهم التحديات القانونية المرتبطة بتلك التقنيات واستكشاف الأساليب التي تتفق مع الأصول القانونية وتلبي متطلبات الأمن والحقوق الفردية. يعتمد الباحثون في هذا المجال على خبرات الفقه المقارن والتشريعات المتعلقة بالتفتيش على نظم الحاسوب والإنترنت التي تم تطويرها في السنوات الأخيرة.

[1] محمد أحمد فكيرين – أساسيات الحاسب الآلي – دار الراتب الجامعية – بيروت – ١٩٩٣ م.

[2] د. محمد إبراهيم زيد – تنظيم الإجراءات الجزائية في التشريعات العربية – ج ٢ – المركز العربي للدراسات الأمنية والتدريب – الرياض – ١٩٩٠م

- **أهمية الحاسوب في العصر الحديث:**
- يعد الحاسوب وتكنولوجيا المعلومات والاتصالات أدوات حيوية وأساسية في جميع جوانب الحياة الحديثة، بما في ذلك القطاعات التجارية والمؤسسات الحكومية والتعليمية والترفيهية والاجتماعية.[1]

وتبرز أهمية الحاسوب في تمكين الأفراد والمؤسسات من تبادل المعلومات والبيانات بشكل سريع وفعال، وتسهيل العمليات الحسابية والإدارية، وتمكين الابتكار والتطوير التقني. كما أنه يلعب دوراً حيوياً في تحسين الاتصال والتواصل بين الأفراد والجهات المختلفة عبر الإنترنت وشبكات الاتصال.[2]

ومن المهم أن نفهم أن هذا التطور التكنولوجي السريع يشكل تحديات قانونية وأمنية جديدة، حيث يمكن استغلال الحواسيب والإنترنت في ارتكاب الجرائم الإلكترونية وانتهاك الخصوصية الشخصية والتجارية. وهنا تكمن أهمية الدراسة المقارنة للتفتيش الجنائي على نظم الحاسوب والإنترنت،[3] حيث يتعين

[1] د. محمد أمين الميداني – النظام الأوروبي لحماية حقوق الإنسان – دار البشير – عمان – ١٩٨٩م.

[2] د. محمد إبراهيم زيد ود. عبد الفتاح الصيفي – قانون الإجراءات الجنائية الإيطالي – دار النهضة العربية – القاهرة – ١٩٩٠م.

[3] د. مأمون محمد سلامة – الإجراءات الجنائية في التشريع المصري – ج ١ – دار النهضة العربية – القاهرة – ١٩٨٨م.

توفير إطار قانوني يضمن حماية المجتمع والأفراد والمؤسسات من هذه الجرائم ويحقق التوازن المناسب بين الأمن والخصوصية وحقوق الأفراد.[1]

ويتم تسليط الضوء على الدور الحاسم الذي يلعبه الحاسوب في تطور المجتمعات والاقتصادات، وتمكين الأفراد والمؤسسات من الوصول إلى مصادر المعلومات وتبادلها بشكل سريع وموثوق وتعتبر تقنية المعلومات والاتصالات، بما في ذلك الحواسيب والإنترنت، أداة قوية لتعزيز النمو الاقتصادي وتعزيز الابتكار وتحسين الإنتاجية. وتشمل الفوائد الرئيسية للحاسوب تسهيل العمليات الإدارية والتنظيمية، وتحسين التواصل والتعاون، وتمكين الوصول إلى المعلومات والخدمات بسهولة.[2]

مع ذلك، تنطوي هذه التكنولوجيا أيضاً على تحديات قانونية. فبجانب الاستفادة من فوائدها، يمكن استغلال الحواسيب والإنترنت في ارتكاب جرائم إلكترونية مثل الاختراق القانوني والاحتيال والتجسس الإلكتروني. ولهذا السبب، يلعب التفتيش الجنائي على نظم الحاسوب والإنترنت دوراً حيوياً في مكافحة الجرائم الإلكترونية وحماية المجتمع والأفراد.[3]

---

[1] د. مأمون محمد سلامة – الإجراءات الجنائية في التشريع المصري – ج ١ – دار النهضة العربية – القاهرة – ١٩٨٨م.

[2] د.لؤي جميل حدادين – نظرية البطلان في قانون أصول المحاكمات الجزائية – دراسة مقارنة – ط ١ – المؤلف نفسه) – عمان – ٢٠٠٠م

[3] كمال كمال الرخاوي – إذن التفتيش فقهاً وقضاء – ط ١ – دار الفكـــر والقانون – المنصورة – ٢٠٠٠م.

- **أنواع الجرائم المعلوماتية:**

تُسلط الدراسة الضوء على التحديات القانونية المرتبطة بهذه التكنولوجيا، حيث يُمكن استغلال الحواسيب والإنترنت في ارتكاب جرائم إلكترونية، مثل الاختراق القانوني والاحتيال والتجسس الإلكتروني. ويُعد التفتيش الجنائي على نظم الحاسوب والإنترنت أداة حيوية لمكافحة هذه الجرائم وحماية المجتمع والأفراد.

أنواع الجرائم المعلوماتية المشتركة وهي تشمل:

1. **الاختراق القرصنة:**

يتعلق هذا النوع من الجرائم بالاقتحام غير المشروع لنظام الحاسوب أو الشبكة والوصول إلى المعلومات المحمية دون إذن صاحبها. يتضمن ذلك اختراق الحسابات الشخصية، والشركات، والمؤسسات الحكومية.

ويعتبر الاختراق والقرصنة من الجرائم المعلوماتية التي تنتهك الأنظمة والشبكات الحاسوبية، وتعتبر هذه الجريمة غير قانونية وتعرض المعلومات الحماية للخطر. تتمثل أهمية هذه الجريمة في سرقة المعلومات الحساسة والتجسس على الأفراد والشركات والمؤسسات الحكومية.

2. **الاحتيال الإلكتروني:**

يشير إلى استخدام تكنولوجيا المعلومات والاتصالات للقيام بأنشطة احتيالية، مثل التلاعب في المعلومات المالية، والتزوير الإلكتروني للهوية، والاحتيال في التجارة الإلكترونية.[1]

الاحتيال الإلكتروني يعد نوعًا من الجرائم المعلوماتية التي تتضمن استخدام تقنيات المعلومات والاتصالات لارتكاب أعمال احتيالية. يتمثل ذلك في تلاعب المعلومات المالية، والتزوير الإلكتروني للهوية، والاحتيال في التجارة الإلكترونية. تُعتبر هذه الأنشطة غير قانونية وتشكل تهديدًا كبيرًا للأفراد والمؤسسات.[2]

تتناول الدراسة المقارنة المذكورة بعنوان "التفتيش الجنائي على نظم الحاسوب والإنترنت" هذا النوع من الجرائم وتقوم بتحليله بطريقة قانونية. تهدف الدراسة إلى دراسة المعايير القانونية والتشريعات المتعلقة بمكافحة الاحتيال الإلكتروني، وتحليل التشريعات العربية والغربية المتعلقة بهذه الجريمة.[3]

---

[1] د. كامل السعيد – شرح الأحكام العامة في قانون العقوبات الأردني – دراسة مقارنة – عمان – ١٩٩٨م.

[2] د. كامل السعيد – شرح الأحكام العامة في قانون العقوبات الأردني – دراسة مقارنة – عمان – ١٩٩٨م.

[3] د.كامل السعيد – الأحكام العامة في الاشتراك الإجرامي في قانون العقوبات الأردني – دراسة تحليلية مقارنة – ط ١ – دار مجدلاوي – عمان – ١٩٨٣م.

تعد هذه الدراسة المقارنة أداة هامة لتوعية القضاة والمحققين والمحامين بأهمية مكافحة الاحتيال الإلكتروني وتحسين الإجراءات القضائية المتعلقة بها. كما تساهم الدراسة في توجيه السياسات العامة لتعزيز التشريعات والإجراءات القانونية للحد من هذه الجريمة وتعزيز العدالة وتطبيق القانون في هذا الصدد. تحلل الدراسة المقارنة التشريعات الوطنية والدولية المتعلقة بالاحتيال الإلكتروني، وتقدم تحليلاً شاملاً للأدوات القانونية المتاحة لمكافحة هذه الجريمة.

3. **سرقة الهوية:**

يتعلق بسرقة معلومات شخصية للتلاعب بها أو استخدامها بطرق غير قانونية، مثل سرقة بيانات الهوية الشخصية والمصرفية واستخدامها في الاحتيال والتزوير.

سرقة الهوية تُعَدّ جريمة تتمثل في الاستيلاء على معلومات شخصية لأفراد آخرين بدون إذن قانوني واستخدامها بطرق غير قانونية. تشمل هذه المعلومات الشخصية بيانات الهوية الخاصة بالأفراد، مثل الاسم الكامل، وتاريخ الميلاد، ورقم الهوية، بالإضافة إلى بيانات مصرفية حساسة مثل أرقام الحسابات المصرفية ومعلومات البطاقات الائتمانية.

تعد سرقة الهوية جريمة خطيرة تهدف إلى التلاعب بالهوية الشخصية للضحية واستغلالها في أنشطة غير قانونية، مثل الاحتيال والتزوير. يقوم المرتكبون

بسرقة هذه المعلومات الشخصية من خلال تقنيات مختلفة، مثل الاختراق الإلكتروني، والتصيد الاحتيالي ((Phishing، والبرمجيات الخبيثة.[1]

4. **انتشار البرامج الضارة:**

يشمل هذا النوع من الجرائم إنشاء وانتشار البرامج الضارة والفيروسات التي تهدف إلى التلاعب بالأنظمة الحاسوبية وسرقة المعلومات أو تعطيلها.[2]

وتهدف الدراسة إلى تحديد التشريعات المتعلقة بمكافحة انتشار البرامج الضارة في الدول المختلفة وتقييم فعالية هذه التشريعات في مكافحة هذه الجريمة المعلوماتية. كما تقدم الدراسة توصيات قانونية لتعزيز التشريعات الحالية وتطوير إجراءات التفتيش الجنائي على نظم الحاسوب والإنترنت للحد من انتشار البرامج الضارة وحماية الأنظمة الحاسوبية والبيانات الحساسة.[3]

تسليط الضوء على جريمة انتشار البرامج الضارة بشكل قانوني وفقًا للأنظمة والتشريعات المعمول بها. يتم تحليل نوعية هذه الجريمة وأساليب انتشار

---

[1] قدري عبد الفتاح الشهاوي – ضوابط السلطة الشرطية في التشريع الإجرائي المصري والمقارن – ط ١ – منشأة المعارف – الإسكندرية –١٩٩٩م.

[2] د.فوزية عبد الستار – شرح قانون أصول المحاكمات الجزائية اللبناني – دار النهضة العربية – بيروت – ١٩٧٥م.

[3] فاروق محمد العامري – الشبكة العالمية للمعلومات – الإنترنت – ط ١ – النسر الذهبي للطباعة – القاهرة – ١٩٧٧م.

البرامج الضارة، وتحديد الأضرار التي يمكن أن تسببها للأنظمة الحاسوبية والمستخدمين.[1]

تشتمل الدراسة على تحليل التشريعات الوطنية والدولية المتعلقة بمكافحة انتشار البرامج الضارة وتقييم فعاليتها وكفاءتها في مجال التفتيش الجنائي. تُعرض النماذج والأطر القانونية المختلفة التي تستخدمها الدول للتصدي لهذه الجريمة ومكافحتها، بما في ذلك التشريعات الجنائية والقوانين المدنية والتدابير الإدارية.[2]

- **أدوات وتقنيات الاختراق:**

أدوات وتقنيات الاختراق التي يستخدمها المهاجمون في الجرائم المعلوماتية، مثل البرمجيات الخبيثة، والتصيد الاحتيالي، والهجمات الموزعة من الخدمة، وغيرها.

تتضمن الأدوات والتقنيات التي سيتم شرحها في الدراسة مثل البرمجيات الخبيثة، التي تشمل الفيروسات وبرامج التجسس وأحصنة طروادة وأدوات القرصنة. كما يتم استعراض التصيد الاحتيالي الذي يشمل التلاعب بالمستخدمين واستغلال الثغرات الأمنية في البرمجيات والتكنولوجيات المختلفة. بالإضافة إلى ذلك، يتم التطرق إلى الهجمات الموزعة من

[1] د.فوزية عبد الستار – شرح قانون أصول المحاكمات الجزائية اللبناني – دار النهضة العربية – بيروت – ١٩٧٥م.

[2] د.فوزية عبد الستار – شرح قانون أصول المحاكمات الجزائية اللبناني – دار النهضة العربية – بيروت – ١٩٧٥م.

الخدمة والتقنيات الأخرى المستخدمة في استغلال الأمان الضعيف للأنظمة والشبكات.[1]

تهدف الدراسة إلى توضيح أدوات وتقنيات الاختراق المستخدمة في الجرائم المعلوماتية وتسليط الضوء على التحديات التي تواجهها الأنظمة القانونية في مكافحة هذه الجرائم. كما تقدم الدراسة توصيات قانونية لتعزيز قدرات التفتيش الجنائي على نظم الحاسوب والإنترنت لمواجهة هذه الأدوات والتقنيات وضمان سلامة البيانات وأمن المعلومات.[2]

من بين الأدوات المشروحة في الدراسة، يتم التركيز على البرمجيات الخبيثة والفيروسات التي تستخدم لاختراق الأنظمة والتلاعب بها، بما في ذلك برامج التجسس وبرامج الاختراق وأحصنة طروادة. كما يتم استعراض التقنيات المستخدمة في التصيد الاحتيالي، والتي تهدف إلى استغلال الضحايا من خلال التلاعب والتحايل عليهم والحصول على معلومات شخصية أو مالية.[3]

---

[1] عمر الفاروق الحسيني – المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية – دراسة تحليلية نقدية – ط٢ – القاهرة – ١٩٩٥م.

[2] د. عوض محمد – الوجيز في قانون الإجراءات الجنائية – الجزء الأول – دار المطبوعات الجامعية – الإسكندرية (د.ت).

[3] عوض منصور – شبكة إنترنت دليلك السريع للاتصال بالعالم – ط١ – دار البشير – عمان – ١٩٩٦م.

بالإضافة إلى ذلك، يتم استعراض الهجمات الموزعة من الخدمة (DDoS) والتقنيات الأخرى المستخدمة في تعطيل الخدمات والمواقع عبر الإنترنت. يتم تحليل كيفية استغلال هذه الهجمات لتعطيل الأنظمة وتسبب انقطاع في توافر الخدمات عبر الإنترنت.

- **التأثيرات القانونية والاقتصادية:**

تحليل التأثيرات القانونية والاقتصادية للجرائم المعلوماتية على المؤسسات والأفراد، وتكاليف مكافحتها وتعويض الخسائر.

تتضمن التحليل القانوني تقدير للتأثيرات القانونية للجرائم المعلوماتية، مثل الاختراق القرصنة، والاحتيال الإلكتروني، وسرقة الهوية، وانتشار البرامج الضارة. يتم تحديد القوانين واللوائح المعمول بها والتي تنص على العقوبات المناسبة لهذه الجرائم، بما في ذلك العقوبات الجنائية والمدنية.[1]

بالإضافة إلى التأثيرات الاقتصادية، تنبثق تأثيرات قانونية أيضاً، حيث تقوم الحكومات بتحديث التشريعات والقوانين المتعلقة بالجرائم المعلوماتية لمواجهة التحديات الناشئة. وتتضمن هذه التأثيرات تشديد العقوبات وتعزيز التعاون الدولي في مكافحة الجرائم المعلوماتية، بالإضافة إلى تعزيز حقوق الأفراد والمؤسسات في حماية بياناتهم الشخصية والمعلومات الحساسة.[2]

---

[1] عوض منصور – شبكة إنترنت دليلك السريع للاتصال بالعالم – ط١ – دار البشير – عمان – ١٩٩٦م.

[2] د.غنام محمد غنام – الحماية الجنائية لأسرار الأفراد لدى الموظف العام – دار النهضة العربية – القاهرة – ١٩٨٨م.

- **القوانين والتشريعات:**

تعتبر التشريعات المحلية والدولية الخاصة بمجال مكافحة الجرائم المعلوماتية والأمن السيبراني أدوات قانونية هامة لتنظيم ومراقبة النشاطات السيبرانية وتحديد المسؤوليات وتحقيق العدالة. وتختلف هذه القوانين من دولة إلى أخرى وقد تشمل:

قوانين الحماية السيبرانية: تحدد الإطار القانوني لحماية الأنظمة السيبرانية وتعزيز الأمان والاستجابة للتهديدات السيبرانية. تتضمن هذه القوانين إجراءات للوقاية من الهجمات السيبرانية وتأمين الشبكات والبنية التحتية السيبرانية.[1]

قوانين مكافحة الجرائم المعلوماتية: تحظر وتعاقب على الأنشطة الجرمية المرتبطة بالمعلوماتية، مثل الاختراقات الإلكترونية، والتزوير الإلكتروني، والاحتيال الإلكتروني. تعطي هذه القوانين سلطات التحقيق الجنائي الرقمي لمكافحة وملاحقة المتسببين في الجرائم المعلوماتية.[2]

قوانين حماية البيانات الشخصية: تنظم جمع ومعالجة وتخزين البيانات الشخصية وتضمن حماية خصوصية الأفراد وسرية معلوماتهم الشخصية.

---

[1] فاروق الكيلاني – محاضرات في قانون أصول المحاكمات الجزائية الأردني والمقارن – ج ٢ – دار الفارابي – عمان – ١٩٨٥م.

[2] م.فاروق حسين – فيروسات الحاسب الآلي والإنترنت – ط١ – دار هـــــــــلا للنشر – ١٩٩١م.

اتفاقيات التعاون الدولي: تعزز التعاون والتبادل القانوني والمعلوماتي بين الدول في توفير إطار قانوني للتعاون الدولي في مكافحة الجرائم المعلوماتية. تشمل هذه الاتفاقيات تبادل المعلومات والأدلة الرقمية، وتسليم المتهمين والممتلكات المرتبطة بالجرائم المعلوماتية بين الدول المتعاقدة.[1]

- **تقنيات الحماية والأمان:**

تقنيات الحماية والأمان هي جوانب حيوية في مكافحة الجرائم المعلوماتية وضمان سلامة الأنظمة الحاسوبية والبيانات. تتعلق هذه التقنيات بتطبيق إجراءات وإعدادات تقنية للوقاية من الاختراق والاحتيال الإلكتروني وسرقة الهوية. وفي الدراسة المقارنة التي تحمل عنوان "التفتيش الجنائي على نظم الحاسوب والإنترنت"، يتم استعراض هذه التقنيات والإجراءات التي يجب اتباعها.[2]

من بين التقنيات الشائعة للحماية والأمان:

- التشفير: يتم استخدام تقنيات التشفير لتشفير البيانات وجعلها غير قابلة للقراءة أو التلاعب بها من قبل الأشخاص غير المصرح لهم.[3]

---

[1] د. فوزية عبد الستار – شرح قانون الإجراءات الجنائية – دار النهضة العربية – القاهرة – ١٩٨٦م.

[2] د. محمد الجبور – الجرائم الواقعة على أمن الدولة في القانون الأردني والقوانين العربية – ط ٢ – عمان – ٢٠٠٠م.

[3] د.قدري عبد الفتاح الشهاوي – أدلة مسرح الجريمة – منشأة المعـــــــــارف – الإسكندرية – ١٩٩٧م.

- جدران الحماية (:(Firewallsتُستخدم جدران الحماية لفصل الشبكات الداخلية عن الشبكات الخارجية والحماية من الاختراقات الخارجية غير المصرح بها.
- نظم الكشف عن التسلل (:(Intrusion Detection Systemsتعمل هذه النظم على رصد وتحليل السلوكيات غير المعتادة والمشتبهة في الشبكة أو النظام، وتنبيه المشرفين عند وجود محاولات اختراق.
- إدارة الهوية والوصول: تتضمن تلك التقنية إدارة الهوية والتحقق من صحة الهوية للأفراد الذين يحاولون الوصول إلى الأنظمة، وتحديد الامتيازات والصلاحيات المناسبة لكل مستخدم.[1]

توفر الدراسة المقارنة إطاراً لتقييم فعالية هذه التقنيات والإجراءات، وتوصي بتنفيذ أفضل الممارسات لضمان الحماية الشاملة للأنظمة والبيانات وتعزيز الأمان السيبراني.[2]

وتوفير الأمان السيبراني الشامل يتطلب أيضًا اتخاذ إجراءات إدارية وتقنية أخرى، مثل:

[1] د قدري عبد الفتاح الشهاوي – الحدث الجرمى – منشأة المعارف – الإسكندرية – ١٩٩٩م.

[2] د. فوزية عبد الستار – شرح قانون الإجراءات الجنائية – دار النهضة العربية – القاهرة – ١٩٨٦م.

- تحديث البرامج والنظم: يجب تحديث البرامج والنظم بانتظام لسد الثغرات الأمنية المعروفة وتحسين الأداء العام للنظام.
- الوعي الأمني والتدريب: ينبغي توعية الموظفين والمستخدمين بأهمية الأمان السيبراني وتدريبهم على ممارسات استخدام آمنة وكيفية التعامل مع الهجمات المحتملة.[1]
- النسخ الاحتياطي واستعادة البيانات: يجب إنشاء نسخ احتياطية من البيانات المهمة واختبارها بانتظام لضمان استعادتها في حالة حدوث خرق أمني أو فقدان بيانات.
- رصد الأمان والتحليل: يجب إنشاء نظام لرصد الأمان يقوم بتسجيل وتحليل الأنشطة غير المعتادة والمشتبهة في الشبكة والنظام، واتخاذ إجراءات فورية لمواجهة التهديدات.[2]
- سياسات الأمان والإجراءات القانونية: يجب وضع سياسات وإجراءات قانونية صارمة لضمان الامتثال وحماية الأنظمة والبيانات من الاختراقات والاستخدام غير المصرح به.

[1] د.مارسيل لوكلير – الوجيز في الشرطة التقنية – تعريب د. بسام الهاشم – ط١ – الدار العربية للموسوعات – بيروت ١٩٨٣م.

[2] د. محمد زكي أبو عامر – الإجراءات الجنائية – ط ٢ – منشأة المعارف – الإسكندرية – ١٩٩٠م.

- **أهمية التحقيق الجنائي الرقمي:**

توضيح أهمية التحقيق الجنائي الرقمي في حالات الجرائم المعلوماتية ودور التقنيات الرقمية في تحليل الأدلة الرقمية وتقديمها كدليل قانوني قوي. يُعتبر التحقيق الجنائي الرقمي جزءاً حاسماً في مكافحة الجرائم المعلوماتية وتحقيق العدالة.[1]

أولاً، يتم التركيز على أهمية التحقيق الجنائي في كشف الجرائم المعلوماتية وتحديد المسؤولين عنها. يتضمن ذلك جمع الأدلة الرقمية من الأجهزة الإلكترونية والشبكات وتحليلها بواسطة التقنيات الرقمية المتخصصة. يساعد التحقيق الجنائي في تحديد سبب الاختراق أو الاحتيال وتعقب المتسببين في الجريمة، مما يساهم في ضمان تقديمهم للعدالة وتقليل انتشار الجرائم المعلوماتية.[2]

ثانيًا، يلعب التحقيق الجنائي الرقمي دوراً حيوياً في تحليل الأدلة الرقمية وتقديمها كدليل قانوني قوي في المحاكم. يعتمد المحققون على التقنيات الرقمية لاسترجاع البيانات المحذوفة أو المخفية وتحليلها للكشف عن الأنشطة غير القانونية. تتضمن هذه التقنيات استخدام أدوات التشفير واستعادة البيانات

[1] د. محمد الجبور – الجرائم الواقعة على أمن الدولة في القانون الأردني والقوانين العربية – ط ٢ – عمان – ٢٠٠٠م.

[2] د. محمد الجبور – استعانة المتهم بمحام – دراسة مقارنة – ط١ – دار الثقافة – عمان – ٢٠٠٢م.

وتحليل الميتاداتا وتتبع النشاط الرقمي. بفضل هذه التقنيات، يمكن توثيق الأدلة الرقمية وتقديمها كدليل قوي في المحاكم[1]

نتيجة للتطور التكنولوجي السريع وانتشار استخدام الأنظمة الحاسوبية والإنترنت، أصبحت الجرائم المعلوماتية أمراً شائعًا في العصر الحديث. ومن هنا تتأتى أهمية التحقيق الجنائي الرقمي في هذه الجرائم. يعد التحقيق الجنائي الرقمي منهجًا قانونيًا متخصصًا يستخدم لجمع الأدلة الرقمية وتحليلها واستنتاج الحقائق المتعلقة بالجريمة المعلوماتية.[2]

توضح أهمية التحقيق الجنائي الرقمي في توفير العدالة والكشف عن المسؤولين عن الجرائم المعلوماتية. يتم استخدام التقنيات الرقمية المتقدمة لجمع الأدلة الرقمية وتحليلها، مما يساعد في تتبع المتسببين في الجرائم وتوجيه الاتهامات القانونية لهم. بفضل التحقيق الجنائي الرقمي، يتم تحقيق العدالة وتقديم المجرمين إلى المحاكمة وفرض العقوبات المناسبة عليهم.[3]

بالإضافة إلى ذلك، يلعب التحقيق الجنائي الرقمي دوراً مهماً في تحليل الأدلة الرقمية وتقديمها كدليل قوي في المحاكم. يتم استخدام التقنيات الرقمية لاسترجاع البيانات المحذوفة أو المخفية وتحليلها بطرق علمية وموثوقة. وبفضل هذه التحليلات الرقمية المتقدمة، يتم تقديم الأدلة الرقمية الصحيحة

---

[1] د. محمد الفاضل – التعاون الدولي في مكافحة الإجرام – بدون دار نشر)– د.ت.(

[2] د.محمد سامي الشوا – ثورة المعلومات وانعكاساتها على قانون العقوبات الجزء الثاني – دار النهضة العربية – القاهرة – ١٩٩٤م.

[3] د.محمد صبحي نجم – قانون أصول المحاكمات الجزائية – ط١ – دار الثقافة – عمان –٢٠٠٠م.

والقوية التي تسهم في إقناع المحكمة بالجانب القانوني وتعزز الحكم بالإدانة أو البراءة[1]

- **التعاون الدولي في مكافحة الجرائم المعلوماتية:**

يعتبر التعاون الدولي أمراً حاسماً في مكافحة الجرائم المعلوماتية التي تتجاوز الحدود الوطنية وتشكل تهديداً عابراً للدول.

أولاً، يتم التركيز على التعاون القانوني بين الدول في مجال مكافحة الجرائم المعلوماتية. تشمل هذه الجهود التبادل القانوني للمعلومات والأدلة الرقمية بين الجهات القضائية والشرطة ووكالات إنفاذ القانون في الدول المعنية. يتم تسهيل هذا التعاون من خلال توقيع اتفاقيات التعاون القضائي وتقاسم المعلومات القانونية ذات الصلة لضمان تحقيق العدالة وملاحقة المجرمين.[2]

ثانيًا، يتم إقامة الشراكات الدولية لتعزيز الأمن السيبراني ومكافحة الجرائم المعلوماتية. تعمل الدول معًا لتبادل المعرفة والخبرات وتعزيز قدراتها في مجال الأمن السيبراني، بما في ذلك تطوير إطارات قانونية وتقنيات متقدمة للكشف والوقاية والتحقيق في الجرائم المعلوماتية. تُشكل هذه الشراكات الدولية

[1] د. محمد شلال العاني وعلي حسن طوالبه – علم الإجرام والعقاب – ط ١ – دار المسيرة – عمان – ١٩٩٨م.

[2] د.مدحت محمد الحسيني – البطلان في المواد الجنائية – دار المطبوعات الإسكندرية – ١٩٩٣م.

مساحة للتعاون المستمر وتبادل المعلومات والممارسات الأفضل لتعزيز القدرة على التصدي للتهديدات السيبرانية.[1]

ثالثًا، يعزز التعاون الدولي السرعة والكفاءة في التحقيق ومكافحة الجرائم المعلوماتية. بفضل تبادل المعلومات والخبرات، يمكن للدول تجاوز التحديات القانونية والتقنية التي تعترضها في مواجهة الجرائم المعلوماتية. يتيح التعاون الدولي أيضًا استخدام الموارد البشرية والتقنية المتطورة المتاحة في الدول الشريكة لتعزيز القدرة على تحقيق النتائج الإيجابية في وقت قصير.[2]

- **التحديات والاتجاهات المستقبلية:**

أحد التحديات الحالية التي تواجه مجال مكافحة الجرائم المعلوماتية هو التطور السريع للتقنيات السيبرانية وتعقيد الهجمات الإلكترونية. يزداد تعقيد الهجمات وتطورها باستمرار، مما يتطلب تحديث القدرات التقنية والمعرفية للتحقق منها والتصدي لها. كما تزداد تنوع وتعقيد الجرائم المعلوماتية، مما يشكل تحديًا للتحقيق الجنائي الرقمي في تحديد المتسببين وجمع الأدلة الرقمية اللازمة.[3]

---

[1] د. محمد الفاضل – التعاون الدولي في مكافحة الإجرام – بدون دار نشر)– د.ت.(

[2] هشام محمد فريد رستم – الجوانب الإجرائية للجرائم المعلوماتية – دراسة مقارنة – مكتبة الآلات الحديثة – أسيوط – ١٩٩٤م.

[3] د. هلالي عبد اللاه أحمد – حجية المخرجات الكمبيوترية في الإثبات الجنائي – ط١ – دار النهضة العربية – القاهرة – ١٩٩٧م.

واجهةً لهذه التحديات، تظهر العديد من الاتجاهات المستقبلية المتوقعة في مجال مكافحة الجرائم المعلوماتية. يتضمن ذلك تطور التحقيق الجنائي الرقمي للتكيف مع التطورات التقنية، مثل استخدام الذكاء الاصطناعي وتحليل البيانات الضخمة في عمليات التحقيق واستخلاص الأدلة الرقمية. كما يشهد المجال تقدماً في مجال تكنولوجيا التشفير والتعرف على الأنماط وحماية البيانات، مما يسهم في تعزيز الأمان السيبراني والحماية من الهجمات الإلكترونية.[1]

في النهج الشامل لمكافحة الجرائم المعلوماتية، يتعين على الدول تعزيز التعاون الدولي وتبادل المعلومات والخبرات في مجال الأمن السيبراني. يجب أن تكون هناك جهود مشتركة لتحقيق التنسيق والتعاون بين الدول في تطوير إستراتيجيات وسياسات فعّالة لمكافحة الجرائم المعلوماتية وتحقيق الأمن السيبراني.[2]

بالإضافة إلى ذلك، يتوجب على المؤسسات القضائية والأجهزة الأمنية في الدول تعزيز قدراتها في مجال التحقيق الجنائي الرقمي وتوفير التدريب والتحصيل المهني للمحققين والخبراء الرقميين. ينبغي أيضاً الاستثمار في

[1] د. هلالي عبد اللاه أحمد – حقوق الدفاع في مرحلة ما قبل المحاكمة بين النمط المثالي والنمط الواقعي – (في فرنسا ومصر والمملكة العربية السعودية) – دار النهضة العربية – القاهرة – ١٩٩٥م.

[2] د. عمر السعيد رمضان – مبادئ الإجراءات الجنائية – دار النهضة العربية – القاهرة – ١٩٨٥م.

البحث والتطوير لتطوير أدوات وتقنيات جديدة تساهم في تسهيل وتحسين عمليات التحقيق الجنائي الرقمي واستخلاص الأدلة الرقمية.[1]

الفصل الأول : ماهية تفتيش نظم الحاسوب والإنترنت.

والفصل الثاني: الطبيعة القانونية لتفتيش نظم الحاسوب والانترنت.

[1] علي عبد القادر القهوجي – الندب للتحقيق – دار الجامعة الجديدة للنشر . الإسكندرية – ١٩٩٧م.

الفصل الأول

ماهية تفتيش نظم الحاسوب والإنترنت

تمهيد وتقسيم

تعتبر مفاهيم الحاسوب والانترنت جوانب حيوية في عصرنا الرقمي الحديث. يتم تنظيم وتشريع هذه المفاهيم بواسطة مجموعة من القوانين والتشريعات المعمول بها في العديد من الدول. في هذا المبحث الأول، سنقوم بتعريف الحاسوب والانترنت وتوضيح مكوناتهما الأساسية ودورها في تنفيذ العمليات الحسابية وتبادل المعلومات.

أولاً: تعريف التفتيش وذاتيته

لم تشتمل التشريعات العربية على تعريف دقيق للتفتيش، بل اكتفت بالإشارة إلى أنه إجراء من إجراءات التحقيق. ومع ذلك، يقدم الفقه العربي تعريفات متعددة للتفتيش كإجراء تحقيقي. على الرغم من اختلاف هذه التعريفات في الشكل، إلا أنها تتفق في المضمون. يعرف الفقه بعض جوانب التفتيش على أنه "الإطلاع على مكان له حرمة للبحث عن أدلة تساعد في التحقيق". ويعرف جانب آخر من الفقه التفتيش بأنه "إجراء من إجراءات التحقيق يتم تنفيذه بواسطة سلطة محددة بالقانون، يهدف إلى البحث في مكان السر عن أدلة

الجريمة وكل ما يساعد في كشف الحقيقة، ويشمل مكان السر الشخص المشتبه به أو المكان الذي يعمل فيه أو يقيم فيه[1]."

وهناك من يرى أن التفتيش هو إجراء من إجراءات التحقيق يهدف إلى ضبط أدلة الجريمة المشمولة بالتحقيق وكل ما يساعد في كشف الحقيقة.

قد تعتبر أفضل التعريفات هي تلك التي ترى أن التفتيش يشمل البحث في مكان السر للمشتبه به عن أشياء تساعد في كشف الحقيقة وربطها به. أو يمكن أن يكون التفتيش هو الاطلاع على مكان يحظى بحماية خاصة بموجب القانون نظراً لكونه مكاناً سرياً لصاحبه، سواء كان ذلك المكان هو سكن أو أي مكان آخر يخضع لنفس النظام. ويؤيد الباحث التعريف الأخير للتفتيش؛ لأنه يشمل جميع العناصر والشروط التي يجب توافرها في مثل هذا الإجراء[2].

يلاحظ أن الفقه الغربي يتقارب مع التعريفات التي وردت في الفقه العربي بشأن التفتيش، وربما يكون العكس صحيحاً نظراً لتأثر الفقهاء العرب بالفقه اللاتيني أو الفقه الانكلوسكسوني،[3] وكذلك نظراً لتأثير القوانين الغربية في القوانين العربية. على سبيل المثال، يعرف الفقه الفرنسي التفتيش بأنه "البحث

---

[1] الرائد كمال أحمد الكركي – النواحي الفنية لإساءة استخدام الكمبيوتر – ورقة عمل مقدمة لندوة الجرائم الناجمة عن التطور التكنولوجي – المنعقدة في عمان بتاريخ ٢٨-١٩٩٨/١٠/٢٩م.

[2] د. أحمد فتحي سرور – حضور المتهم أثناء التفتيش – مجلة إدارة قضايا الحكومة – السنة ٣١ – العدد ١ – يناير / مارس – ١٩٥٩م.

[3] نور الدين الواهلي، الاختصاص في الجريمة الإلكترونية، سلسلة ندوات محكمة الاستئناف، الرباط، العدد السابع، 2014

الدقيق عن جميع عناصر الأدلة التي يمكن استخدامها في الدعوى الجزائية والتي تتم على مسكن المتهم". يميز المشرع الفرنسي بين تفتيش المساكن (La Perquisition) والمعروف أيضاً باسم "الزيارة المنزلية (Visite domicilaire)"، وتفتيش الأشخاص(La fouilic corporale) ، والذي يتعلق بجسم الإنسان وملابسه[1].

وبناءً على ذلك، يمكن اقتراح تعريف لتفتيش نظم الحاسوب والإنترنت بأنه "البحث في مكان السر للمتهم عن عناصر مادية أو معنوية تساعد في كشف الحقيقة وربطها به"، أو "الاطلاع على مكان يحظى بحماية خاصة بموجب القانون نظراً لكونه مكاناً سرياً لصاحبه، ويمكن أن يكون هذا المكان جهاز الحاسوب أو نظمه أو الإنترنت."

ومن هذه التعاريف يمكن أن نستخلص أهم خصائص تفتيش نظم الحاسوب والإنترنت والتي تميزه عن غيره من إجراءات التحقيق الأخرى ، وهي:

١. يحوي التفتيش في مضمونه على قدر من الجبر والإكراه حيث أنه تعرض قانوني لحرية المتهم الشخصية أو لحرمة أسراره الموجودة على جهاز الحاسوب خاصته أو على برامج خاصة به أو على بريده الإلكتروني عبر شبكة الإنترنت.[2]

---

[1] أحمد أسامة حسنية، التفتيش في الجرائم الإلكترونية في التشريع الفلسطيني، دراسة تحليلية مقارنة بالتشريع العُماني، 2016

[2] د. عادل رياض محمد – جرائم الحاسوب وأمن البيانات – مجلة العربي – العدد ٤٤٠– السنة ٣٨ – الكويت – يوليو – ١٩٩٥م.

٢. إن التفتيش يُعد قيداً على حرمة أو حصانة الشخص الذاتية، ويعتبر قيداً على حرمة أسراره الشخصية أي فيه مساس بحق السر.

٣ . يمتاز التفتيش بهذه الصورة بأنه وسيلة للبحث عن الأدلة المادية والمعنوية للجريمة وضبطها. وتشير الخصيصة الأخيرة إلى الهدف من التفتيش وهو ضبط الأدلة التي تفيد في كشف الحقيقة.[1]

المبحث الأول: تعريف الحاسوب والانترنت ومكوناتهما

تفتيش نظم الحاسوب والإنترنت هو عملية تقنية وقانونية تهدف إلى فحص وتحليل الأنظمة الحاسوبية وشبكات الإنترنت بحثًا عن أي تهديدات أمنية أو انتهاكات قانونية قد تعرض المعلومات والبيانات للخطر. يشمل تفتيش نظم الحاسوب والإنترنت استخدام التقنيات الخاصة لجمع الأدلة الرقمية وتحليلها بهدف التعرف على أنماط الاختراق وتحديد المسؤوليات والتوصل إلى الأدلة اللازمة للتحقيق الجنائي وتقديمها كدليل قانوني قوي[2].

تتضمن عملية تفتيش نظم الحاسوب والإنترنت فحص وتحليل الملفات وسجلات النشاط، والبحث عن آثار الاختراقات والبرمجيات الضارة، وتحليل ثغرات الأمان وتقييم السياسات والإجراءات الأمنية المعتمدة .

---

[1] الرائد كمال الكركي – جرائم الحاسوب ودور مديرية الأمن في مكافحتها – ورقة عمل مقدمة إلى ندوة قانون حماية حق المؤلف – نظرة إلى المستقبل – المنعقدة في عمان بتاريخ ١٩٩٩/٧/٥م.

[2] د. أحمد فتحي سرور – مراقبة المكالمات التلفونية – المجلة الجنائية القومية العدد ١ – مارس – ١٩٦٣م. ٤. أنطوان بطرس وآخرون – الإنترنت – ملف خاص – مجلة الكمبيوتر والاتصالات الإلكترونية – المجلد ١٢– العدد ٧ – أيلول ١٩٩٥م.

المطلب الأول: تعريف الحاسوب ومكوناته

تعريف الحاسوب:

يعرف الحاسوب (Computer) : بأنه: (عبارة عن جهاز إلكتروني يتكون من مجموعة من الأجهزة أو الوحدات التي تعمل بصورة متكاملة مع بعضها بعضا بهدف تشغيل مجموعة البيانات الداخلة طبقا لبرنامج محدد تم وضعه مسبقا للحصول على نتائج معينة) ويتكون الحاسوب من كيانات مادية (Computer Hardware)، وكيانات منطقية (computer Software)، [1]وللتعرف على العناصر التي يمكن أن يقع عليها التفتيش التحقيقي يستعرض الباحث الأجزاء والكيانات التي تم ذكرها بشيء

من التفصيل:

أولاً: مكونات الحاسوب المادية(Computer Hard ware) :

يتكون الحاسوب من مجموعة من الوحدات لكل منها وظيفة محددة، وتتصل هذه الوحدات مع بعضها بعضاً بشكل يجعلها تعمل كنظام متكامل. [2] ومجموعة هذه الوحدات تكون ما يسمى بمعدات الحاسوب، وهذه الوحدات هي:

---

[1] كامل السعيد – جرائم الكمبيوتر والجرائم الأخرى في مجال التكنولوجيا – بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي – القاهرة – في ٢٥–٢٨/ اكتوبر / ١٩٩٣م.

[2] د.مدحت رمضان – الأحكام العامة للقانون الجنائي وجرائم الإنترنت – بحث مقدم لندوة الجرائم الناجمة عن التطور التكنولوجي – المنعقدة في عمان بتاريخ ٢٨–١٩٩٨/١٠/٢٩م.

١ – وحدات الإدخال (Input Unit) :

وظيفة أجهزة هذه الوحدة استقبال البيانات ، المدخلة إلى الحاسوب وتمريرها إلى داخل الجهاز (وهي عادة تمرر إلى وحدة الذاكرة للتخزين) ومن الأمثلة على أجهزة الإدخال نذكر منها:

أ. لوحة المفاتيح (Keyboard)

ب. القارة (Mouse)

ج. مشغل الأقراص (Disk Drive)

د. الماسح (Scanner)

وحدة الذاكرة (Memory Unit)

تقوم هذه الوحدة بتخزين البرنامج أو البرامج والبيانات. وهذه الوحدة على صنفين

أ– وحدة الذاكرة الرئيسية أو العشوائية: (Random Access Memory:RAM) وتسمى كذلك ذاكرة القراءة والكتابة وتستخدم لتخزين البرامج والبيانات التي تقع تحت المعالجة، أي أن محتويات هذه الذاكرة قابلة للتعديل (حذف، إضافة تغيير)، كما أنها تفقد محتوياتها بانقطاع التيار الكهربائي . لذا لزاماً على القائم بتنفيذ التفتيش أن ينتبه إلى هذه المسألة المهمة كي لا يفقد المعلومات الموجودة على هذه الذاكرة.[1]

[1] مختار محمد أمين – جرائم الحاسب الإلكتروني – مجلة الأمن العام – العدد ٩٠– السنة ٢٣ – القاهرة – ١٩٨٠م.

ب وحدة ذاكرة القراءة فقط (Read Only Memory:ROM): حيث تتم برمجة هذه الذاكرة (تخزينها بالبيانات المطلوبة) أثناء مرحلة التصنيع، ويمكن قراءتها عند الحاجة، ولا يمكن تخزين أي معلومات جديدة أثناء استخدامها، ولا تفقد هذه الذاكرة محتوياتها بانقطاع التيار الكهربائي.

وسنبحث في الباب الثاني من هذه الاطروحة إن شاء الله المشاكل القانونية المثارة في الفقه حول إمكانية تفتيش وضبط هذا الجزء من الحاسوب.[1]

٣- وحدة الحساب والمنطق (Arithmetic and Logic Unit:ALU):

وظيفة وحدة الحساب والمنطق هي إجراء العمليات الحسابية والمنطقية المطلوبة، وتتكون من مجموعة من الدوائر الحسابية والمنطقية المبينة باستخدام البوابات المنطقية ومجموعة من المسجلات (Registers) اللازمة لتنفيذ العمليات[2]المطلوبة.

[1] غسان حزين – قصة اختراع البريد الإلكتروني – مجلة العربي – العدد ٥٣٠ – الكويت – يناير – ٢٠٠٣م.

[2] د. كامل فريد السالك – الجريمة المعلوماتية – مجلة المحامون السورية – العدد (٥-٦) – السنة (٦٦) – أيار وحزيران – ٢٠٠١م.

٤-وحدة التحكم (Control Unit):

ووظيفتها التحكم بعمل وحدات الحاسوب وتنسيق تبادل البيانات والأوامر وتحتوي على مجموعة من المسجلات والعدادات ودوائر فك الرموز وتحليلها ومولدات إشارات التزامن والتحكم.[1]

٥- وحدة الذاكرة المساعدة (Auxiliary Memory):

وتستخدم لتخزين كميات هائلة من البيانات وبصورة دائمة، أي أنها لا تفقد محتوياتها بانقطاع التيار الكهربائي. ومن أهم وسائط التخزين المستخدمة: الأقراص المرنة (Floppy Disks) والأقراص الصلبة (Hard Disks) والأشرطة الممغنطة (Magnetic Tape) والأقراص المضغوطة (Compact Disks) ، وتصل سعة القرص الصلب في الحواسيب الشخصية الحديثة إلى ما يزيد عن ٤٠ غيغابايت (GB) . ويمكن ضبط الأقراص المرنة[2]

والاسطوانات عند إجراء التفتيش وتحتاج عملية ضبط الأقراص الصلبة إلى إجراءات فنية سنتطرق إليها لاحقاً.

---

[1] د.فاضل نصر الله عوض – ضمانات المتهم أمام سلطة التحقيق الابتدائي في التشريع الكويتي – دراسة مقارنة بالتشريعيين المصري والفرنسي – مجلة الحقوق – الكويت – ١٩٩٨م.

[2] د.مدحت رمضان – الأحكام العامة للقانون الجنائي وجرائم الإنترنت – بحث مقدم لندوة الجرائم الناجمة عن التطور التكنولوجي – المنعقدة في عمان بتاريخ ٢٨-١٩٩٨/١٠/٢٩م.

٦- وحدة الإخراج (Output Unit) :

وظيفة أجهزة هذه الوحدة استقبال البيانات من الحاسوب وتمريرها إلى المستخدم بالصيغة المناسبة، أي إخراج نتائج المعالجة. ومن الأمثلة على أجهزة

الإخراج:-

أ. الشاشة (Screen)

ب. الطابعة (Printer)

ج. مشغلات الأقراص (Disk Drives)

يمكن لأجهزة الإخراج القيام بأعمال فنية وصناعية مثل تجميع السيارات أو صهر المعادن أو القيام بأعمال النقل أو الدفع أو التغليف في المعامل الصناعية الحديثة. وهناك أجهزة توليف الصوت- وهي أجهزة إخراج للكلمات المنطوقة [1]بحيث يتمكن المستخدم من الاستماع إلى شخص آخر يتحدث أو يتحدث إليه، أو يستمع للموسيقى بواسطة الشبكات وهناك الأجهزة التي تجيب المستخدم عبر الهاتف عن أمر ما مثل الاستفسار عن رقم هاتف معين أو حالة الهاتف المطلوب أو خدمة البنوك أو الحصول على النقود من أجهزة الصراف الآلي. ويتم عادة تجميع وحدة الحساب والمنطق ووحدة التحكم في وحدة واحدة تسمى وحدة المعالجة المركزية (CPU).

[1] Stefani,.4 "L'acted' instruction" in Problems contemporains de procedure penale, paris- 1964.

ثانياً: مكونات الحاسوب المنطقية (Computer Software) :

يعرف الكيان المنطقي بأنه: (مجموعة البرامج والأساليب والقواعد وعند الاقتضاء الوثائق المتعلقة بتشغيل وحدة معالجة البيانات). إذن يشتمل الكيان المنطقي على جميع العناصر غير المادية اللازمة لتشغيل الكيان المادي فيشتمل[1]

على:-

١. البرامج . ٢. وصف البرامج. 3- المستندات الملحقة بالبرنامج.

والكيان المنطقي مصطلح أعم وأشمل من البرنامج، حيث يضم بالإضافة إلى البرنامج وصفه ومستنداته الملحقة.

وتنقسم الكيانات المنطقية إلى نوعين هما:

١ – الكيانات الأساسية وتضم كل البرامج الضرورية من أجل استخدام أفضل للحاسوب وملحقاته، وهي مندمجة في الجهاز ذاته مثل أنظمة التشغيل وأنظمة البرمجة.[2]

٢- الكيانات التطبيقية : وتضم هذه الفئة البرامج التي تمكن مستخدم الجهاز من أن ينفذ بواسطته عملاً محدداً بدقة ومتصلاً باحتياجات هذا المستخدم الخاصة والذي يسعى لمواجهة مشكلة ما وتساعد المستخدم في عمله ومن

---

[1] د.معتصم مشعشع – استعانة المشتكى عليه بمحام خلال الاســ تجواب في مرحلة التحقيق الابتدائي – دراسة في القانون الأردني مقارنة مع القانون الفرنسي – مجلة الدراسات – الجامعة الأردنية – المجلد ٢٦ العدد ١ –١٩٩٩م.

[2] د. علاء عبد الرزاق السالمي – تكنولوجيا المعلومات – ط ١ – كحلـــــــــــــــون – عمان – ١٩٩٧م.

أمثلتها برامج معالجة النصوص وجداول البيانات الإلكترونية وبرامج قواعد البيانات وبرامج التحليل الإحصائي وبرامج لتطبيقات مختلفة مثل : الرسم والتصميم الهندسي والألعاب ... الخ . ولا شك أن هذه الكيانات المنطقية تحتاج إلى الحماية القانونية نظراً لمساسها المباشر بحياة الأشخاص أو نشاط المؤسسات أو بعمل الهيئات. [1]

وما يتطلبه ذلك من حفاظ على سرية ما يتداول من معلومات وبعدها عن القرصنة والاعتداءات . ومن هنا ظهرت الحاجة إلى تشريعات خاصة لحماية برامج ونظم الحاسوب وشبكة الإنترنت.

ولما كان هذا البحث متخصصاً بالقانون فان الباحث سيكتفي بهذا القدر من الإيضاح بالنسبة للكيانات المنطقية للحاسوب، لكن يبقى السؤال عن كيفية استخدام هذه المكونات المعنوية في ارتكاب الجرائم المعلوماتية وبالتالي إمكانية إجراء التفتيش وضبط الدليل في هذه الجرائم. ومن الأساليب المستخدمة في ارتكاب الجرائم المعلوماتية بواسطة هذه الكيانات المنطقية.

أولاً: التلاعب في المدخلات:

كإدخال بيانات مختلفة أو محرفة في نظام معلومات الحاسوب أو تغيير مسار البيانات الصحيحة المدخلة، أو الجمع بين الأمرين معاً، وهي أمور سهل القيام بها في أولى مراحل تشغيل نظام معلومات الحاسوب ، وهي مرحلة

[1] أحمد أسامة حسنية، التفتيش في الجرائم الإلكترونية في التشريع الفلسطيني، دراسة تحليلية مقارنة بالتشريع العُماني، 2016

إدخال البيانات لمعالجتها. حيث إن أكثر من نصف الجرائم المعلوماتية يقع باستخدام هذه الطريقة .

ثانياً: التلاعب في البرامج: ومن أبرز صوره:

١- **إدخال تعديلات غير مرخص بها على البرامج المستخدمة:** تمر في العادة معظم البرامج بعد إعدادها واختبارها بعدد من التعديلات الثانوية أثناء فترة تنفيذها لتصحيح ما قد تتضمنه من أخطاء لم يتم اكتشافها من قبل. وفي بعض الأحيان قد يقتضي الأمر تطويرها. ومن المتاح في هاتين المرحلتين إدخال تغييرات غير مرخص بها على البرامج تسمح بارتكاب جرائم على المال وإخفائه.[1]

٢- **استخدام البرامج الخبيثة** : وهي تتخذ صوراً عدة، وتستهدف أغراضاً شتى. ومنها ما يهدف إلى الاحتيال والاستيلاء على المال بواسطة الحاسوب، ومنها ما يُعد بهدف التدمير والابتزاز ومن أخطرها ذلك البرنامج الذي يتيح لمعده إدخال أوامر غير مشروعة إلى الحاسوب تحقق أغراضه الإجرامية مثل:

أ- **برنامج حصان طروادة :** وهو برنامج خادع يخفي ظاهره غرضاً غير مشروع يضمره، إذ يظهر كبرنامج عادي يؤدي بعض المهام المفيدة والمألوفة لمستخدمه بينما يكون موجوداً بطريقة خفية داخله بعض الأوامر أو التعليمات التي تؤدي عند تشغيله مهام ضارة غير متوقعة تمثل حقيقة البرنامج فيقوم

[1] د. عفيفي كامل عفيفي – جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون – دراسة مقارنة – (د.ت).

بمحو البيانات من ذاكرة الحاسوب أو التهديد بذلك لابتزاز مستخدمه أو الاستيلاء على المال بتحريف البيانات المدخلة أو المخزنة.[1]

ب. **القنابل المنطقية أو الموقوتة** : وهي برامج مصممة بحيث تكون ساكنة وغير فعالة وغير مكتشفة ، لمدة قد تصل إلى أشهر أو أعوام. وهذه المدة يحددها مؤشر زمني يحتويه البرنامج، كتاريخ معين حيث ينشط البرنامج عند حلوله فيؤدي مهامه الهدامة.[2]

ج –**برامج الدودة** : وهي برامج تستغل أية فجوات في نظم التشغيل لتنتقل من حاسوب إلى آخر مغطية الشبكة بأكملها، وقد تنتقل من شبكة إلى أخرى عبر الوصلات التي تربط بينها وأثناء عملية انتقالها تتكاثر مثل البكتريا، بإنتاج نسخ منها، وهدفها شغل أكبر مجال ممكن من سعة الشبكة، وبالتالي تقليل أو خفض كفاءتها. وقد تقوم بتخريب الملفات والبرامج ونظم التشغيل وبروتوكولات الاتصال.[3]

د. **فيروس الحاسوب:** وهي برامج مهاجمة تصيب أنظمة الحاسوب بأسلوب يماثل إلى حد كبير أسلوب الفيروسات الحيوية التي تصيب الإنسان، وهي في العادة برنامج صغير مكتوب بلغة متدنية المستوى مثل لغة التجميع مما يزيد

---

[1].3 Procedure Penale - Informatique code 1993.

[2] د. عفيفي كامل عفيفي – جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون – دراسة مقارنة – (د.ت).

[3] د.عصمت عبد المجيد بكر ود صبري حمد خاطر – الحماية القانونية للملكية الفكرية – ط ١ – بيت الحكمة – بغداد - ٢٠٠١م.

من صعوبة اكتشافه. وأنواع فيروسات الحاسوب كثيرة، ومن الممكن تصنيفها من حيث تكوينها وأهدافها إلى:[1]

١ . فيروس عام العدوى: وهو ينتقل إلى أي برنامج أو ملف.

٢ . فيروس محدد العدوى وهو يستهدف نوعاً معيناً من النظم لينتقل إليه. وهو أبطأ في انتشاره وأصعب في اكتشافه من سابقه.

٣. فيروس عام الهدف وتنطوي تحته غالبية الفيروسات المعروفة.

٤. فيروس محدد الهدف ويحتاج إعداده إلى درجة عالية من المهارة وإلى دراية تامة بالتطبيق الذي يستهدفه الفيروس، وقد يجري هذا الفيروس تلاعباً مالياً أو يدخل تعديلات في تطبيق عسكري مثلاً.

٣- استخدام برامج معدة خصيصاً لتنفيذ وإخفاء الاحتيال لاختلاس المال.

٤- استخدام البرامج الجاهزة المخصصة لتخطي أنظمة الحماية الفنية في الحالات الطارئة.

[1] د. عبد الوهاب حومد – الوسيط في الإجراءات الجزائية الكويتية – ط ٢ – جامعة الكويت – الكويت – ١٩٨٢م.

مكونات الحاسوب:

وفقًا للمصادر القانونية والمعايير المعترف بها، تتكون الحواسيب من مجموعة من المكونات الأساسية التي تعمل معًا لتحقيق وظائف الحاسوب. من بين هذه المكونات الأساسية يمكن الاشارة إلى:

1. **وحدة المعالجة المركزية** :(CPU) وحدة المعالجة المركزية هي المكون الأساسي في الحاسوب وتقوم بتنفيذ التعليمات ومعالجة البيانات. تعمل الـــ CPU على تنفيذ العمليات الحسابية والمنطقية والتحكم في تدفق البيانات داخل الحاسوب[1].

وحدة المعالجة المركزية (CPU) هي العنصر الأساسي في الحاسوب وتعتبر "دماغ الحاسوب". تقوم وحدة المعالجة المركزية بتنفيذ التعليمات ومعالجة البيانات بطريقة سلسة ومنظمة. تتألف وحدة المعالجة المركزية من مجموعة من الدوائر والوحدات الداخلية التي تعمل معًا لتحقيق العمليات المطلوبة.[2]

تعمل وحدة المعالجة المركزية على تنفيذ العمليات الحسابية والمنطقية، مثل الجمع والطرح والضرب والقسمة، وتنفيذ العمليات المنطقية مثل المقارنة والتحقق من الشروط واتخاذ القرارات المنطقية. كما تقوم بإدارة تدفق البيانات

[1] د. عبد الفتاح بيومي حجازي – النظام القانوني لحماية التجارة الإلكترونية – ط ١ – دار الفكر الجامعي – الإسكندرية – ٢٠٠٢م.

[2] د. عبد الفتاح بيومي حجازي – الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت – دراسة متعمقة في جرائم الحاسب الآلي والإنترنت – دار الكتب القانونية – القاهرة – ٢٠٠٢م.

داخل الحاسوب، حيث تقوم بتنظيم حركة البيانات بين الذاكرة والأجهزة الأخرى مثل القرص الصلب والوحدات الإدخال والإخراج.[1]

تتكون وحدة المعالجة المركزية من وحدات متعددة تعمل معًا، بما في ذلك وحدة التحكم التي تدير تنفيذ التعليمات وتنظم تسلسل العمليات، ووحدة الحساب التي تقوم بالعمليات الحسابية، ووحدة التخزين المؤقت التي تستخدم لتسريع عمليات الوصول إلى البيانات. تعتمد أداء وحدة المعالجة المركزية على سرعتها وعدد النوى الموجودة فيها.[2]

2. **الذاكرة العشوائية** :(RAM) تعتبر الذاكرة العشوائية مكونًا مهمًا في الحاسوب حيث تقوم بتخزين المعلومات المؤقتة التي يحتاجها الحاسوب خلال تشغيله. تلعب الـــ RAM دورًا حاسمًا في تسريع عمليات الوصول إلى البيانات وتحسين أداء الحاسوب.

الذاكرة العشوائية (RAM) وهي مكون أساسي في الحواسيب يقوم بتخزين المعلومات المؤقتة التي يحتاجها الحاسوب خلال تشغيله. تعتبر الـــ RAM جزءًا هامًا من الذاكرة العامة للحاسوب وتسهم في تسريع عمليات الوصول إلى البيانات وتحسين أداء الحاسوب بشكل عام.

[1] عبد الفتاح مراد – التحقيق الجنائي التطبيقي – القاهرة – ١٩٩٥م.

[2] د. عبد الوهاب حومد – الوسيط في الإجراءات الجزائية الكويتية – ط ٢ – جامعة الكويت – الكويت – ١٩٨٢م.

تعمل الذاكرة العشوائية على تخزين البيانات التي يتم استخدامها بشكل متكرر ومؤقت. عندما يقوم الحاسوب بتشغيل برامج وتطبيقات، يتم نقل البيانات من القرص الصلب إلى الذاكرة العشوائية لتكون متاحة للمعالجة بشكل سريع. وبمجرد انتهاء استخدام البيانات، يتم حذفها من الذاكرة العشوائية لتوفير مساحة للبيانات الجديدة.

تمتاز الذاكرة العشوائية بسرعة الوصول إلى البيانات، حيث يمكن للمعالج أن يقوم بالوصول إلى البيانات المخزنة في الـــ RAM بسرعة عالية. هذا يساعد في تحسين أداء الحاسوب وزيادة سرعة تنفيذ البرامج والعمليات. كما تساهم الذاكرة العشوائية في تسريع عمليات التحميل والتخزين المؤقت للبيانات، مما يوفر وقتًا وجهدًا للمستخدم.[1]

ومع ذلك، يجب الانتباه إلى أن الذاكرة العشوائية هي ذاكرة مؤقتة وتكون غير مستدامة، حيث تتم محو البيانات المخزنة فيها عند إيقاف تشغيل الحاسوب. ولذلك، يتم الاعتماد على القرص الصلب لتخزين البيانات بشكل دائم.[2]

[1].2 Merle et vitu: Traite de droit Criminel, paris, 1967

[2] عبد الحميد المنشاوي – المرجع العلمي في إجراءات التحقيق الجنائي – دار الفكر الجامعي – القاهرة – ١٩٩٤م.

3. **القرص الصلب**(Hard Disk) :

يعتبر القرص الصلب وسيلة لتخزين البيانات بشكل دائم وطويل الأمد. يقوم القرص الصلب بتخزين الملفات والبرامج والنظام التشغيل، ويمكن الوصول إليها في أي وقت[1].

والقرص الصلب (Hard Disk) هو مكون هام في الحواسيب يستخدم لتخزين البيانات بشكل دائم وطويل الأمد. يعتبر القرص الصلب وسيلة فعالة للحفظ والوصول إلى الملفات والبرامج والنظام التشغيل.

يتكون القرص الصلب من أقراص مغناطيسية تدور بسرعة عالية، وتحتوي على طبقات مغناطيسية تمكنها من تخزين البيانات. [2]يتم كتابة وقراءة البيانات على القرص الصلب باستخدام رؤوس القراءة/الكتابة المغناطيسية المتحركة. تستخدم القراءة/الكتابة المغناطيسية إشارات مغناطيسية لتمثيل البيانات الرقمية وتسجيلها على الأقراص المغناطيسية[3].

يتم تجزئة القرص الصلب إلى مساحات صغيرة تسمى قطاعات، وتخزن البيانات في هذه القطاعات. يتم تعيين عناوين لكل قطاع على القرص الصلب

---

[1] م.عبد الحميد بسيوني عبد الحميد – شبكات الكمبيوتر – ج ١ – مكتبة ابن سينا – القاهرة – ١٩٩٥م.

[2] د. عبد الرؤوف مهدي – شرح القواعد العامة للإجراءات الجنائية وفقاً لآخر التعديلات – دار النهضة العربية – القاهرة – ٢٠٠٠م.

[3] د. عبد العظيم الوزير – شرح قانون العقوبات – القسم الخاص – جرائم الاعتداء على الأموال – ط ١ – دار النهضة العربية – القاهرة – ١٩٩٣م.

لتمكين الوصول إلى البيانات بشكل دقيق وفعال. يتم تنظيم البيانات في هيكل ملفات يسمح بتنظيمها وإدارتها بطريقة منظمة[1].

يمتاز القرص الصلب بسعة تخزين عالية، مما يسمح بتخزين كميات كبيرة من البيانات مثل الملفات النصية والصور والفيديو والمستندات وغيرها. كما يتميز القرص الصلب بالاستقرار والموثوقية، حيث يمكن الوصول إلى البيانات المخزنة عليه في أي وقت دون الحاجة إلى اتصال بالشبكة أو مصدر طاقة خارجي.

باختصار، يتكون الحاسوب من مجموعة من المكونات الأساسية مثل وحدة المعالجة المركزية والذاكرة العشوائية والقرص الصلب، وتتعاون هذه المكونات معًا لتحقيق وظائف الحاسوب ومعالجة البيانات بشكل فعال وفقًا للمعايير القانونية والمعترف بها[2].

البرمجيات ونظام التشغيل:

تنص قوانين حماية حقوق الملكية الفكرية على أن البرمجيات ونظام التشغيل يخضعان لحقوق الملكية الفكرية. تعني هذه القوانين أن البرمجيات ونظام التشغيل محمية بموجب القانون ولا يحق للأفراد أو المؤسسات استخدامها أو توزيعها أو نسخها بدون إذن صريح من صاحب حقوق الملكية الفكرية.

---

[1] د. عبد الفتاح بيومي حجازي – الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت – دراسة متعمقة في جرائم الحاسب الآلي والإنترنت – دار الكتب القانونية – القاهرة – ٢٠٠٢م.

[2] Jean Larguier- Procedure Penale -Dolloz- 1991.

حقوق الملكية الفكرية تشمل حقوق المؤلف وحقوق الملكية. حقوق المؤلف تعني أن الشخص الذي قام بكتابة البرمجيات أو تطوير نظام التشغيل لديه حقوق حصرية على عمله، وهذا يشمل حقوق الاستنساخ، والتوزيع، والعرض العام، والتعديل، والترجمة والأعمال المشتقة.

ويعني ذلك أنه يجب الحصول على إذن صريح من صاحب حقوق الملكية الفكرية لاستخدام البرمجيات أو نظام التشغيل بأي طريقة.

بالإضافة إلى ذلك، هناك أيضًا قوانين تنظم تراخيص استخدام البرمجيات ونظام التشغيل. تتضمن هذه التراخيص شروطًا وقيودًا لاستخدام البرمجيات ونظام التشغيل، وتحدد حقوق وواجبات المستخدمين فيما يتعلق باستخدامها ولذلك، من الناحية القانونية، يجب على المستخدمين الامتثال لحقوق الملكية الفكرية لصاحب البرمجيات ونظام التشغيل، والحصول على التراخيص اللازمة قبل استخدامها أو توزيعها أو نسخها[1].

دور نظام التشغيل في إدارة الموارد وتوفير واجهة بين المستخدم والحاسوب.

نظام التشغيل يلعب دوراً حاسماً في إدارة الموارد وتوفير واجهة بين المستخدم والحاسوب. وفقًا للقوانين المتعلقة بحقوق الملكية الفكرية والبرمجيات، نظام

[1] د. عبد الحافظ عبد الهادي عابد – الإثبات الجنائي بالقرائن – دراسة مقارنة – دار النهضة العربية – القاهرة – ١٩٩١م.

التشغيل يعتبر عملاً فكرياً محمياً بموجب القانون، وبالتالي يجب احترام حقوق الملكية الفكرية لصاحبه[1].

- **أولاً،** يتحكم نظام التشغيل في إدارة الموارد المتاحة في الحاسوب. يقوم بتخصيص المعالج والذاكرة والتخزين والشبكة والملفات وغيرها من الموارد للبرامج والعمليات المختلفة. يتم تنظيم استخدام الموارد وتنسيقها بواسطة نظام التشغيل لضمان تنفيذ فعال ومنسق للعمليات على الحاسوب.
- **ثانياً،** يقوم نظام التشغيل بتوفير واجهة بين المستخدم والحاسوب، وهذه الواجهة تسهل التفاعل والتواصل بين المستخدم والأدوات والبرامج المثبتة على الحاسوب. تشمل واجهة المستخدم الرسومية (GUI)العناصر المرئية مثل القوائم والأزرار والنوافذ والأيقونات، وتسهل على المستخدم تنفيذ العمليات والوصول إلى الموارد وإدارة الملفات والتطبيقات بطريقة سهلة وفعالة[2].

وبموجب القوانين القانونية، يتم حماية حقوق الملكية الفكرية لصاحب نظام التشغيل وواجهته. يلزم الحصول على إذن من صاحب حقوق الملكية الفكرية

[1] عبد الحميد المنشاوي – المرجع العلمي في إجراءات التحقيق الجنائي – دار الفكر الجامعي – القاهرة – ١٩٩٤م.

[2] Avizienis, A., Laprie, J.-C., Randell, B., & Landwehr, C. (2004). Basic Concepts and Taxonomy of Dependable and Secure Computing. Dependable and Secure Computing, IEEE Transactions on, 1, 11-33

لاستخدام نظام التشغيل أو أجزاء منه أو تعديله. يجب احترام حقوق البرمجيات والعلامات التجارية والواجهة المستخدمة في نظام التشغيل .

حقوق الملكية الفكرية للبرمجيات

هي حقوق قانونية تمنح لصاحب البرمجية حقوقًا حصرية على العمل الذي قام به. وفقًا للقوانين المعمول بها في العديد من الدول، تعتبر البرمجيات محمية بموجب قوانين حماية حقوق الملكية الفكرية والبرمجيات.

قانون حماية حقوق البرمجيات يهدف إلى حماية حقوق الملكية الفكرية المتعلقة بالبرمجيات وتنظيم استخدامها. يمنح هذا القانون صاحب البرمجية حقوقًا قانونية حصرية مثل حق التكوين، وحق التوزيع، وحق النسخ، وحق العرض، وحق التعديل، وحق التأليف. ويعتبر انتهاك حقوق الملكية الفكرية للبرمجيات جريمة قانونية قد يترتب عليها عواقب قانونية وجزائية.

وبموجب هذا القانون، يتعين على الأشخاص والمؤسسات الاحترام والامتثال لحقوق الملكية الفكرية لصاحب البرمجية. يجب الحصول على إذن صاحب البرمجية لاستخدامها أو توزيعها أو نسخها أو تعديلها أو عرضها بطرق قانونية. يتعين على الأطراف المتعاقدة على استخدام البرمجيات الالتزام بشروط الترخيص وعدم تجاوز نطاق الاستخدام المصرح به[1].

[1] عبد الأمير العكيلي – أصول الإجراءات الجنائية في قانون أصول المحاكمات الجزائية – ج ١ – ط ١ – مطبعة المعارف – بغداد – ١٩٧٥م.

ينص القانون على أنه في حالة انتهاك حقوق الملكية الفكرية للبرمجيات، يمكن لصاحب البرمجية مطالبة المخالفين بتحمل المسؤولية القانونية والمدنية. ويمكن للمحاكم تنفيذ إجراءات قانونية لحماية حقوق الملكية الفكرية للبرمجيات وتطبيق عقوبات وغرامات على المخالفين[1].

حماية الملكية الفكرية والبرمجيات:

حماية الملكية الفكرية والبرمجيات تعتبر قضية قانونية ذات أهمية كبيرة. توجد قوانين متعددة في معظم الدول تهدف إلى حماية حقوق الملكية الفكرية والبرمجيات، وضمان حقوق صاحب العمل الأصلي.

قانون حماية الملكية الفكرية[2] يوفر الإطار القانوني لحماية الأعمال والابتكارات الفكرية، بما في ذلك البرمجيات. يتضمن هذا القانون حقوقًا قانونية حصرية لصاحب البرمجية، مثل حق التكوين، وحق التوزيع، وحق النسخ، وحق العرض، وحق التعديل، وحق التأليف. يلزم القانون أيضًا احترام حقوق الملكية الفكرية للأشخاص الآخرين.

يمنح قانون حماية الملكية الفكرية صاحب البرمجية حقوقًا قانونية حصرية لفترة زمنية محددة، ويعتبر انتهاك هذه الحقوق جريمة قانونية. يتعين على الأشخاص والمؤسسات الاحترام والامتثال لحقوق الملكية الفكرية لصاحب

[1] د. عبد الحميد الشواربي – ضمانات المتهم في مرحلة التحقيق الابتدائي – منشأة المعارف – الإسكندرية – ١٩٨٨م.

[2] Cohen, F. (2009). Two Models of Digital Forensic Examination. In Proceedings of the IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE) (pp. 42-53

البرمجية والامتناع عن استخدامها أو توزيعها أو نسخها أو تعديلها أو عرضها بدون إذن قانوني

تعتبر حماية الملكية الفكرية والبرمجيات أمراً هاماً لتشجيع الابتكار والإبداع، وتعزيز الاستثمار في قطاع التكنولوجيا والبرمجيات.[1] وفي حالة انتهاك حقوق الملكية الفكرية للبرمجيات، يمكن لصاحب البرمجية أن يلجأ إلى القضاء وطلب الحماية القانونية والمدنية، ويمكن للمحاكم تنفيذ إجراءات قانونية لحماية حقوق الملكية الفكرية وتطبيق عقوبات وغرامات.[2]

[1] **********

[2] Rogers, M., & Meyers, M. (2005). Digital Forensics: Meeting the Challenges of Scientific Evidence. International Federation for Information Processing Digital Library; Advances in Digital Forensics, 194

المطلب الثانى

تعريف الإنترنت ومكوناته

الإنترنت هو شبكة عالمية تربط الأجهزة والشبكات المختلفة ببعضها البعض عن طريق بروتوكولات الاتصال القياسية. تتيح هذه الشبكة تبادل المعلومات والبيانات بين المستخدمين في مختلف أنحاء العالم. يعتمد الإنترنت على بنية موزعة تسمح بتوصيل الأجهزة والشبكات المختلفة معاً وتوجيه حركة البيانات بينها

- **تعريف الإنترنت:**

يمكن تعريف الإنترنت على النحو التالي:

يعتبر الإنترنت بمثابة مجموعة من الشبكات المترابطة التي تستخدم تقنيات الاتصال والتبادل القياسية مثل بروتوكول الإنترنت (IP) وبروتوكول التحكم في النقل (TCP) لضمان توصيل البيانات بشكل آمن وفعال. تتيح الإنترنت للمستخدمين الوصول إلى مجموعة واسعة من الخدمات والمحتوى، بما في ذلك البريد الإلكتروني، والمواقع الإلكترونية، والتطبيقات العامة والخاصة.[1]

[1] عبد الأمير العكيلي – أصول الإجراءات الجنائية في قانون أصول المحاكمات الجزائية – ج ١ – ط ١ – مطبعة المعارف – بغداد – ١٩٧٥م.

عناصر شبكة الإنترنت

تعرف شبكة الحاسوب (Network)، بأنها (مجموعة مكونة من اثنين أو أكثر من أجهزة الحاسوب والمتصلة ببعضها اتصالاً سلكياً أو لا سلكياً). وهي تتخذ عدة أشكال مثل النجمة والحلقة.[1] وقد تكون الأجهزة موجودة في نفس الموقع وتسمى (الشبكة المحلية Local Area Network - LAN ، وقد تكون موزعة في أماكن متفرقة ويتم ربطها عن طريق خطوط الهاتف وتسمى الشبكة واسعة النطاق أو الشبكة بعيدة المدى

(Wide Area Network-WAN)[2]

ويتم الاتصال أو نقل المعلومات بواسطة الشبكة بأشكال ثلاثة هى :

١ – اتصال أحادي الجانب – من طرف واحد (Simplex)

ويتم هذا الاتصال بين جهاز الحاسوب للمستفيد مع جهاز مركزي مثال

على ذلك جهاز الحاسوب الموجود في مكتب عضو هيئة التدريس في الجامعة مع الجهاز الرئيسي في الجامعة، ويتم من خلاله معرفة أعداد وأسماء الطلبة

[1] د.جميل عبد الباقي الصغير – القانون الجنائي والتكنولوجيا الحديثة – الكتاب الأول – الجرائم الناشئة عن استخدام الحاسب الآلي – ط١ – دار النهضة العربية – القاهرة – ١٩٩٢م.

[2] جون فورستر – مجتمع التقنية العالية – قصة ثورة تقنية المعلومات – ط١ – ترجمة ونشر مركز الكتاب الأردني – الأردن – ١٩٨٩م.

المسجلين في المواد الخاصة بالأستاذ أو علاماتهم السابقة ومعدلاتهم أو أية معلومات أخرى.[1]

٢ – اتصال ثنائي غير كامل المعلومات (Half Duplex) :

ويتم الاتصال بين جهازين ، فيرسل الأول المعلومات ويستقبلها الثاني، وبعد انتهاء الأول، يقوم الثاني بإرسال المعلومات ويستقبلها الأول، وهكذا، لكن لا يستطيع الاثنان التخاطب " الإرسال والاستقبال" في نفس الوقت.[2]

3– اتصال ثنائي كامل للمعلومات (Full Duplex) :

ويتم الاتصال بواسطته بسهولة بين جهازين، ويمكن للأطراف التخـــاطب "الإرسال والاستقبال " في نفس الوقت.

لم يعد نطاق الاتصالات محدوداً في إقليم دولة واحدة بل امتد ليشمل كـــــــــــل أرجاء العالم، مما يزيد في تعقيد المسألة، بحيث يحتاج الأمر إلى اتفاقيات دولية لضبط الجرائم ومرتكبيها عبر شبكات الحاسوب وهذا ما سيتم بحثه لاحقاً، بعد بيان وتوضيح طبيعة شبكة الإنترنت (Internet).[3]

---

[1] بيل جيتس وآخرين – المعلوماتية بعد الإنترنت طريق المستقبل) – ترجمة أ. عبد السلام رضوان – سلسلة عالم المعرفة – المجلس الوطني للثقافة والفنون الآداب – العدد ٢٣١ – الكويت – مارس ١٩٨٨م.

[2] بيتر كنت – الدليل الكامل إلى الإنترنت – ترجمة سامح الخلف – ط ١ – الدار العربية للعلوم – بيروت – ١٩٩٧م.

[3] Egan, M., & Mathar, T. (2005). The Executive Guide to Information Security: Threats, Challenges, and Solutions

والإنترنت (Internet) اختصار للكلمات الإنكليزية التالية (Internation Network)، وهي منظومة واسعة جداً من شبكات المعلومات الحاسوبية المتصلة مع بعضها بعضاً بطريقة لامركزية، ويدخل في تركيب هـــــــــــذه الشبكة ملايين الحواسيب الموزعة في مختلف دول العالم ، بالإضافة إلى أجهزة

الاتصالات والتحكم التي تعمل جميعا لتوفير وتوصيل الخدمات المختلفة للمستفيدين وهذا يعني اتساع إمكانية ارتكاب الجرائم وصعوبة التفتيش، لهذا تسمى الشبكة بالدولية .[1]

وهناك عدد كبير من الاستخدامات لشبكة الإنترنت وفي مختلف مجالات الحياة، لا يتسع المجال هنا لذكرها كلها ، لذا يكتفي الباحث باستعراض أهمها لعلاقتها بموضوع بحثنا التفتيش :

1- البريد الإلكتروني (E.mail): ويعرف بأنه: إرسال واستقبال الرسائل الإلكترونية عن طريق شبكة الإنترنت . وهو يوفر إمكانية الاتصال بالملايين من البشر حول العالم كبديل عن البريد التقليدي في نقل الرسائل أو الهاتف العادي . [2]ومن خلال معرفة مستخدم الإنترنت للرمز البريدي يمكنه إيداع

---

[1] بيل جيتس وآخرين – المعلوماتية بعد الإنترنت طريق المستقبل) – ترجمة أ. عبد السلام رضوان – سلسلة عالم المعرفة – المجلس الوطني للثقافة والفنون الآداب – العدد ٢٣١ – الكويت – مارس ١٩٨٨م.

[2] د. آمال عبد الرحيم عثمان – الإثبات الجنائي ووسائل التحقيق العلمية – دار النهضة العربية – القاهرة – ١٩٧٥م.

رسائل في البريد الإلكتروني للغير، قد تتضمن مغازلة أو كلاماً جارحاً أو رسومات مبتذلة أو ربما شتائم مما يقع تحت طائلة الجرائم المخلة بالآداب العامة أو الذم أو القدح، مثال ذلك ما قام به حزب العمل المعارض في (إسرائيل) من نشر صورة عارية لزوجة نتياهو رئيس الوزراء الإسرائيلي الأسبق على شبكة الإنترنت.[1] وهي صورة متطورة في المعاكسات تضاف إلى المعاكسات البريدية والهاتفية، ومثالها ما حدث في إمارة (أبو ظبي). حيث بث أحد مستخدمي الإنترنت صورة لامرأة عارية وأرسلها إلى المشتركين الآخرين، الذين تبدأ أسماؤهم بالحروف (XYZ)، من خلال البريد الإلكتروني الخاص بهم، وقضت محكمة أبو ظبي (الدائرة الأولى) في القضية رقم ٤٣٧٣ لسنة ١٩٩٧م – جنح أبو ظبي – بإدانة المتهم بغرامة قدرها عشرة آلاف درهم مع مصادرة الصورة المضبوطة وإتلافها .

ومن الجهود المبذولة لحماية شبكة الإنترنت والبريد الإلكتروني مشروع كليبر (Clipper Project) الذي تتبناه الحكومة الأمريكية والذي يهدف إلى تطوير نظام آلي لتشفير الرسائل الإلكترونية والصوتية لحمايتها من المتطفلين، وفي الوقت الذي يجد فيه هذا المشروع تأييداً من الأغلبية في مجتمع الإنترنت[2]، إلا أنه يواجه جدلاً في بعض الأوساط الحكومية والتي تؤكد على أهمية أن يكون للحكومة وباستمرار إمكانية الإطلاع والتنصت على الرسائل

[1] Whitcomb, C. (2002). An Historical Perspective of Digital Evidence. International Journal of Digital Evidence, 1

[2] د. آمال عبد الرحيم عثمان – شرح قانون الإجراءات الجنائية – دار النهضة العربية – القاهرة – ١٩٧٥م.

الإلكترونية والصوتية وذلك بغية مراقبة الإرهابيين وتجار المخدرات ، وبحيث يتم ذلك من قبل المعنيين في السلطة التنفيذية وبناء على أمر الحكومة. وهناك قائمة البريد الإلكتروني التي تساعد الأشخاص في الاشتراك بما يسمى بنقاش المجموعة .(Group Discussions)

ويمكن البريد الإلكتروني مستخدمه من الوصول إلى الملفات والبيانات والمواقع على الإنترنت التي لا يمكنه الوصول إليها واستخدامها عن طريق البريد العادي ، إلا أن هذه التقنية الرائعة تتعرض لهجوم أشخاص أطلق عليهم مصطلح هاكرز(Harkers)ومصطلح آخر كريكرز (Crackers)، وهم الأشخاص الذين يهاجمون أنظمة الآخرين ويدخلون إليها بصورة غير مشروعة بنية إجرامية ، ويسعون إلى فتح أبواب خلفية لشبكات الحاسوب والإنترنت . فقد استخدم شخص في الولايات المتحدة الأمريكية عنوان البريد الإلكتروني لشخص آخر لإرسال رسائل مخالفة للقانون على الخط الأمريكي المباشر لمجلس الإنذار بوجود قنابل في ولاية أوكلاهوما، وقد أعطى هذا الرجل المزيف رقم هاتف ضحيته الذي استلم تهديدات بالموت، وقد يكون هدف هؤلاء المزيفين هو إزعاج ضحاياهم فقط، وقد يسعون في أحيان أخرى إلى تدمير السمعة كأن يرسل شخص ما رسائل بذيئة إلى رئيسه في العمل باستخدام حساب البريد الإلكتروني لشخص آخر .[1]

[1] Carrier, B., & Spafford, E. (2005). Automated Digital Evidence Target Definition Using Outlier Analysis and Existing Evidence. In Digital Forensic Research Workshop 2005

٢ – شبكة العنكبوت العالمية (The World Wide Web - WWW):
وهو نظام برمجي يعمل على شبكة الإنترنت، يتكون من مجموعة كبيرة من النصوص الفعالة المكونة من كم هائل من المستندات المتصلة والمتشعبة.[1] ويمكن من خلالها تصفح مواقع المعلومات متعددة الوسائط والمرتبطة فيما بينها، وهذه الخدمة تجمع النصوص والصور والأصوات والأفلام المتحركة بطريقة تفاعلية (تخاطب وحوار وسحب وإيداع بيانات). وبالنسبة لمواقع الويب (Web) فإنه من الصعب تكليف متعهدي الخدمة مراقبة مشروعيتها، لأن هذه المواقع تتجاوز الآلاف ويتم تغييرها يوميا ، مما يجعل من مسألة تفتشيها مهمة صعبة وشاقة.[2]

3– استرجاع المعلومات(Information Retm al) :

تحتوي الشبكة على العديد من قواعد المعلومات التي يمكن الرجوع إليها مجاناً، كما أن هناك قواعد معلومات يمكن الدخول إليها لقاء اشتراك شهري أو سنوي، ويمكن تصنيف هذه المواقع إلى نوعين: الأول – مواقع خاصة بحيث لا يسمح بالدخول إليها إلا لمن يملك ترخيصاً بذلك، أي–أن المستخدم لهذا النوع من المواقع يجب أن يملك اسماً خاصاً للدخول (Login) وكلمة سر

[1] د. آمال عبد الرحيم عثمان – شرح قانون الإجراءات الجنائية – دار النهضة العربية – القاهرة – ١٩٧٥م.

[2] انتصار نوري الغريب – أمن الكمبيوتر والقانون – دار الراتب الجامعية – بيروت – ١٩٩٤م.

(Password). [1]وأن بعض الباحثين والمؤلفين والناشرين قد يحملون ترخيصاً للدخول إليها. والنوع الثاني من المواقع (عامة)، أي أنها مفتوحة للاستخدام العام (مجانية) بحيث لا يحتاج المستخدم إلى ترخيص للدخول إليها، ولا يحتاج ســــــــــوى إلى إدخال عنوانه البريدي بدلاً من كلمة السر .

فهل يمكن أن تطبق على الحالة الأولى التفتيش الواقع على الأماكن الخاصة، والتي تحتاج إلى مذكرة خاصة بذلك، وعلى الحالة الثانية التفتيش الواقع على الأماكن العامة والذي لا يحتاج للتفتيش ،هذا ما سيبحثه الباحث في الفصل الثاني إن شاء الله.

4- الحلقات النقاشية والتحاور والاستشارة أو ما يسمى بالتخاطب (Chatting) ويمكن هذا النظام المستخدمين من التحدث بطريقة الكتابة الإلكترونية فيما بينهم مباشرة والمخاطبة أو التخاطب بواسطة الإنترنت، هو نظام يتيح إمكانية التحدث إلى الآخرين باستخدام الكلمات المطلوبة، ومزايا هذا النظام توزيع وتبادل البرامج والملفات بين الأشخاص والشركات عبر العالم. [2]

[1] جميل عبد الباقي الصغير – أدلة الإثبات الجنائي والتكنولوجيا الحديثة – (أجهزة الرادار – الحاسبات الآلية – البصمة الوراثية – دراسة مقارنة – دار النهضة العربية – القاهرة – ٢٠٠١م.

[2] جميل عبد الباقي الصغير – أدلة الإثبات الجنائي والتكنولوجيا الحديثة – (أجهزة الرادار – الحاسبات الآلية – البصمة الوراثية – دراسة مقارنة – دار النهضة العربية – القاهرة – ٢٠٠١م.

ه – الاتصال عن بعد (تلنت Telent) : شجعت شبكة الإنترنت عدداً كبيراً من العاملين على إنجاز أعمالهم عن بعد، وتلنت عبارة عن خدمة تقدمها الإنترنت وتسمح للمستخدم من الاتصال عبر جهاز الحاسوب خاصته مع أي شخص آخر موجود في أي مكان في العالم عبر شبكة الإنترنت . مما يساعد في ارتكاب جرائم الحاسوب والإنترنت.[1]

- **مكونات الإنترنت:**

المكونات الأساسية للإنترنت هي مجموعة من الأجهزة والبرامج التي تعمل معًا لتمكين التواصل وتبادل المعلومات عبر الشبكة العالمية. وفقًا للمعايير المعترف بها، يتم تعريف المكونات الرئيسية للإنترنت على النحو التالي:

- **الخوادم** :(Servers) وهي أجهزة تعمل باستمرار لتوفير المحتوى والخدمات للمستخدمين. وتتضمن الخوادم خوادم الويب (Web Servers)، وخوادم البريد الإلكتروني(Mail Servers) ، وخوادم الألعاب(Game Servers) ، وغيرها[2].
- **الموجهات** :(Routers) وهي أجهزة تقوم بتوجيه حركة المعلومات بين الشبكات المختلفة. وتستخدم الموجهات عادة لربط الشبكات المحلية بالإنترنت وتحديد المسار الأمثل للحزم المرسلة والمستلمة.

[1] Janes, S. (2000). The Role of Technology in Computer Forensic Investigations. Information Security Technical Report, 5, 43-50

[2] حسن الجوخدار – شرح قانون أصول المحاكمات الجزائية – ط٢ – مكتبة دار الثقافة – عمان – ١٩٩٧م.

- **المفاتيح** :(Switches) وهي أجهزة تستخدم لتوصيل الأجهزة داخل الشبكة المحلية وتمكينها من التواصل وتبادل المعلومات[1].
- **بروتوكول الإنترنت** :(IP Protocol) وهو مجموعة من القواعد التي تحدد كيفية تبادل المعلومات عبر الإنترنت. ويستخدم بروتوكول الإنترنت لتحديد عناوين الأجهزة وتوجيه حركة البيانات بينها.

بنية الإنترنت تتألف من مجموعة من الشبكات المترابطة التي تشكل الشبكة العالمية. وتستخدم الشبكات المختلفة تكنولوجيات مختلفة، مثل التوصيل بالألياف البصرية والاتصال اللاسلكي، وتعتمد على البروتوكولات الموحدة لتحقيق التواصل الفعال[2].

- **خدمات الإنترنت:**

خدمات الإنترنت هي مجموعة من الخدمات المتاحة عبر الشبكة العالمية وفقًا للمصادر القانونية المعترف بها. وفي هذا السياق، يتم تعريف بعض الخدمات الرئيسية التي تقدمها الإنترنت وفقًا للقوانين والتشريعات المنصوص عليها كالتالي:

[1] حسن صادق المرصفاوي – قانون الإجراءات الجنائية مع تطوراته التشريعية ومذكراته الإيضاحية وأحكام النقض في خمسين عاماً – موسوعة الفقه والقضاء للدول العربية – الجزء (١٤٠) – الدار العربية للموسوعات – بيروت – ١٩٨١م.

[2] د.رؤوف عبيد المشكلات العملية الهامة في الإجراءات الجنائية – ج ١ – ط ٣ – دار الفكر العربي.

1. البريد الإلكتروني: يشير إلى خدمة تبادل الرسائل الإلكترونية بين المستخدمين عبر الإنترنت. تتعامل هذه الخدمة مع معايير وقوانين تنظيم استخدامها وتأمينها للمستخدمين[1].
2. المواقع الإلكترونية: تشير إلى الصفحات والمواقع المتاحة عبر الإنترنت والتي توفر معلومات ومحتوى مختلف للمستخدمين. قد ينص القانون على الشروط والقيود المتعلقة بتشغيل ونشر مواقع الويب، بما في ذلك حقوق الملكية الفكرية وقوانين النشر وحماية البيانات[2].
3. التجارة الإلكترونية: تشير إلى عمليات الشراء والبيع والتجارة التي تتم عبر الإنترنت. قد تنظم هذه العمليات بواسطة قوانين وتشريعات خاصة تهدف إلى حماية المستهلكين وتنظيم العمليات التجارية الإلكترونية وتوفير ضمانات الأمان والخصوصية.
4. حماية المستهلك وحماية البيانات الشخصية: تعتبر هذه القضايا من الأهمية القصوى في سياق الإنترنت. تشمل حماية المستهلك قوانين وتشريعات لضمان سلامة وجودة الخدمات المقدمة عبر الإنترنت وتحمي حقوق المستهلكين في حالة وجود أي ممارسات غير قانونية أو غير عادلة.

[1] د.رؤوف عبيد المشكلات العملية الهامة في الإجراءات الجنائية – ج ١ – ط ٣ – دار الفكر العربي.

[2] Boddington, R., Hobbs, V., & Mann, G. (2023). Validating Digital Evidence for Legal Argument. Australian Digital Forensics Conference

- **الأمان والخصوصية على الإنترنت:**

الأمان والخصوصية على الإنترنت هما جوانب حيوية تتطلب تنظيماً وحماية قانونية للمستخدمين. وفقًا للمصادر القانونية، يمكن تصفية هذه الجوانب على النحو التالي:

1. الأمان على الإنترنت: يشير إلى مجموعة من القوانين والتشريعات المعترف بها التي تهدف إلى حماية المستخدمين والأنظمة الحاسوبية من التهديدات الإلكترونية. تشمل هذه القوانين تنظيم استخدام الأدوات الأمنية والتدابير الوقائية لحماية البيانات والشبكات، بما في ذلك الكشف عن انتهاكات الأمان ومكافحة الجرائم الإلكترونية[1].

2. الخصوصية على الإنترنت: تشير إلى القوانين والتشريعات التي تنظم جمع واستخدام وتخزين البيانات الشخصية على الإنترنت. تهدف هذه القوانين إلى حماية خصوصية المستخدمين وتحديد القواعد والمعايير التي يجب أن تلتزم بها الشركات والمنظمات في التعامل مع البيانات الشخصية، بما في ذلك ضمان الحصول على موافقة المستخدمين والإفصاح الشفاف عن كيفية استخدام البيانات وحمايتها من الوصول غير المصرح به[2].

---

[1] د.حمودي الجاسم – دراسة مقارنة في أصول المحاكمات الجزائية – ج ١ – مطبعة العاني – بغداد – ١٩٦٢م.

[2] د.رؤوف عبيد – مبادئ الإجراءات الجنائية في القانون المصري – ط ١١ – القاهرة – ١٩٧٦م / وط ١٦ – ١٩٨٥م.

المبحث الثانى

المقصود بالجريمة المعلوماتية واتجاهات تصنيفها وصورها.

تمهيد وتقسيم

على الرغم من الفوائد الكبيرة التي جلبها الإنترنت للعالم، إلا أنه أصبح بيئة خصبة لبعض المجرمين الذين يعتمدون سلوكهم الإجرامي على التقدم التكنولوجي في مختلف المجالات. ونتيجة لذلك، ظهرت الجريمة المعلوماتية التي استحوذت على اهتمام كبير من قبل أعضاء القانون والمشرعين.

لفهم ما يُقصد بالجريمة المعلوماتية وتصنيفاتها وأشكالها، سيتم تقسيم هذا الموضوع إلى مطلبين رئيسيين. وللتعرف على المقصود بالجريمة المعلوماتية واتجاهات تصنيفها وصورها، سوف يتم تقسيم هذا المبحث إلى مطلبين، هما:

- المطلب الأول: المقصود بالجريمة المعلوماتية.
- المطلب الثاني: اتجاهات تصنيف الجريمة المعلوماتية وصورها.

المطلب الأول

المقصود بالجريمة المعلوماتية

مقدمة

تواجه ظاهرة الجريمة المعلوماتية المشكلة الأساسية والأولى في غياب تعريف موحد لها. حيث بذل الباحثون والمهتمون بدراسة هذا النوع الجديد من الجريمة جهوداً كبيرة لتحقيق تعريف مناسب يتناسب مع طبيعة الجريمة المعلوماتية. ومع ذلك، فقد فشلت العديد من هذه المحاولات، وحتى يقال إن الجريمة المعلوماتية تقاوم التعريف. ونتيجة لذلك.[1]

تعريف الجريمة المعلوماتية :

أصبح العديد من الباحثين يتجنبون استخدام تعريف محدد للجريمة المعلوماتية، مدافعين عن وجهة نظر تقول إن الجريمة المعلوماتية مجرد جريمة تقليدية ترتكب بواسطة أساليب جديدة. وبالرغم من أن هذا الرأي صحيح في بعض الحالات، إلا أن العديد من جرائم الحوسبة تتمتع بخصائص فريدة تجعل تطبيق التعريفات التقليدية عليها أمراً صعباً[2].

[1] Mandya, K., & Prosise, C. (2023). Incident Response: Investigating Computer Crime

[2] د.رؤوف عبيد – مبادئ الإجراءات الجنائية في القانون المصري – ط ١١ – القاهرة – ١٩٧٦م / وط ١٦ – ١٩٨٥م.

لا شك أن عدم التوافق على تعريف جرائم الحاسب الآلي ينجم عنه عدة مشكلات عملية مهمة، منها صعوبة تقدير مدى انتشار هذه الظاهرة وتعذر إيجاد الحلول اللازمة لمواجهتها، بالإضافة إلى صعوبة تحقيق التعاون الدولي لمكافحتها. تمت محاولات متعددة لتعريف الجريمة المعلوماتية، وعلى الرغم من أنها لم تتبع اتجاهًا واحدًا، إلا أنها تنقسم عمومًا إلى اتجاهين:

- الاتجاه الأول هو الاتجاه الضيق الذي يحد من مفهوم الجريمة المعلوماتية، حيث يقلل من عدد الحالات التي يمكن أن يشملها هذا النوع من الجريمة الإلكترونية[1].
- والاتجاه الثاني هو الاتجاه الواسع الذي يوسع مفهوم الجريمة المعلوماتية، حتى يتم تصنيف أفعال غير مشروعة تتعلق بتقنية المعلومات والحوسبة، ويمكن القول في كثير من الأحيان أنه يشمل أفعالًا لا يمكن تصنيفها كجرائم حوسبة[2].

يتبنى التعريف الواسع لجريمة الحاسب الآلي فكرة تشمل كل فعل عمدًا ينشأ عن استخدام غير قانوني لتقنية المعلومات ويهدف إلى التسبب في أضرار مادية أو معنوية. على سبيل المثال، قد عرف الفقيه الألماني تيادمان جريمة الحاسب الآلي بأنها "تشمل جميع أشكال السلوك غير المشروع التي تُرتكب

[1] . انتصار نوري الغريب – أمن الكمبيوتر والقانون – دار الراتب الجامعية – بيروت – ١٩٩٤م.

[2] Ieong, R. (2006). FORZA: Digital Forensics Investigation Framework That Incorporates Legal Issues. Digital Investigation, 3, 29-36

باستخدام الحاسب الآلي". وعرفها الفقيه ليزلي د. بول بأنها "فعل إجرامي يستخدم الحاسب الآلي كأداة رئيسية". وعرفها الفقيهان

يتسبب عدم التوافق على تعريف جرائم الحاسوب في حدوث عدة مشكلات عملية، من بينها صعوبة تقدير مدى انتشار هذه الظاهرة وعدم القدرة على إيجاد الحلول اللازمة لمكافحتها. كما يعوق التعاون الدولي في مجال مكافحة جرائم الحاسوب. تمت محاولات متعددة لتعريف الجريمة المعلوماتية، وعلى الرغم من ذلك، فإنها تنحصر في اتجاهين رئيسيين.

الاتجاه الأول يقيد مفهوم الجريمة المعلوماتية، مما يقلل من عدد الحالات التي يمكن أن ينطبق عليها تصنيف الأنشطة الإجرامية المتعلقة بالحواسيب. والاتجاه الثاني، على العكس من ذلك، يوسع مفهوم الجريمة المعلوماتية ليشمل أفعالًا غير قابلة للتصنيف عادةً كجرائم الحواسيب.

يشمل التعريف الواسع للجريمة المعلوماتية أي فعل متعمد مرتبط بالحواسيب يتسبب في خسارة للأموال أو الأضرار الناجمة عنها، أو يتسبب في كسب غير قانوني. تعرف الجريمة المعلوماتية بأنها أي فعل جنائي يستخدم الحاسوب كأداة رئيسية لارتكابه وتعرفها أيضاً بأنها الجرائم التي تنطوي على

عمليات فعلية داخل نظام الحاسوب، وببساطة هي الجرائم التي يكون للحاسوب دور إيجابي أكثر من الدور السلبي فيها[1].

وفقًا للتعريف الواسع، يمكن أن تشمل جرائم الحواسيب جميع التصرفات غير المشروعة المرتبطة بالحواسيب بغض النظر عن الدور الذي يلعبه الحاسوب فيها، سواء كان الحاسوب وسيلة لارتكاب الجريمة، أو كان موضوع الجريمة نفسه. ويمكن تصنيف الحالات عموماً إلى حالات تستخدم فيها الحواسيب كوسيلة لارتكاب الجريمة، وحالات تتعلق بالحواسيب كأداة لارتكاب الجريمة، وحالات تتعلق بالحواسيب كموضوع للجريمة[2].

تعريف تقنية المعلومات وسيلة تم استخدامها لتحديد نطاق جرائم الحاسوب. فهي تشمل جميع الأدوات الإلكترونية والبصرية والكهروكيميائية وغيرها التي تستخدم لمعالجة البيانات الإلكترونية والقيام بالعمليات المنطقية والحسابية والتخزينية. يشمل ذلك أيضًا الوسائط المتصلة أو المرتبطة مباشرة بتلك الأدوات والتي تسمح بتخزين المعلومات الإلكترونية أو نقلها إلى الآخرين وباختصار، فإن تعريف الجريمة المعلوماتية الواسع يسمح بتضمين جميع

[1] بيل جيتس وآخرين – المعلوماتية بعد الإنترنت طريق المستقبل) – ترجمة أ. عبد السلام رضوان – سلسلة عالم المعرفة – المجلس الوطني للثقافة والفنون الآداب – العدد ٢٣١ – الكويت – مارس ١٩٨٨م.

[2] Cohen, F. (2010). Toward a Science of Digital Forensic Evidence Examination (Vol. 337). IFIP Advances in Information and Communication Technology.

الأفعال غير المشروعة المرتبطة بالحواسيب، بينما التعريف الضيق يعتمد فقط على الوسيلة المستخدمة في ارتكاب الجريمة[1].

ثانيا: التعريف الضيق

انطلق أنصار التعريف الضيق للجريمة المعلوماتية من النقطة المرتبطة بضرورة العلاقة بين المعلوماتية والأفعال المشروعة لتحديد ما إذا كانت تلك الأفعال تدخل في نطاق الجريمة المعلوماتية أم لا.

وبعبارة أخرى، حتى تشكل الأفعال غير المشروعة جريمة معلوماتية، فإنها يجب أن تكون موجهة ضد "الأموال المعلوماتية"، مع استبعاد الأفعال التي تستخدم الإعلام الآلي كوسيلة للاعتداء على الآخرين، سواء أشخاصاً أو أموالًا أو الثقة العامة[2].

منظمة التعاون الاقتصادي والتنمية قدمت تعريفًا للجريمة المعلوماتية ينص على أنها: "كل سلوك مشروع أو غير مشروع أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات ونقلها."

[1] بيل جيتس وآخرين – المعلوماتية بعد الإنترنت طريق المستقبل) – ترجمة أ. عبد السلام رضوان – سلسلة عالم المعرفة – المجلس الوطني للثقافة والفنون الآداب – العدد ٢٣١ – الكويت – مارس ١٩٨٨م.

[2] Reith, M., Carr, C., & Gunsch, G. (2003). An Examination of Digital Forensic Models. Journal of Digital Forensics, 1

وهناك اتجاه فقهي يتزعمه الفقيه "قراري" يقيد مجال الجريمة المعلوماتية، حيث يقتصر على الاعتداءات الموجهة ضد الكيان المنطقي للمعلوماتية، ويشكك في اعتبار الاعتداءات التي تستهدف الكيان المادي للمعلوماتية جرائم معلوماتية. يبرر هذا الاتجاه ذلك بأن العناصر المادية للمعلوماتية يمكن أن تخضع لأحكام جريمة السرقة، وبالتالي فإن الاعتداء عليها لا يعتبر جريمة معلوماتية. وأعرب الفقيه "قراري" عن رأيه بقوله: "إن سرقة شريط ممغنط أو أسطوانة أو حتى الكمبيوتر ذاته لا يمكن أن تصنف تحت تسمية الجريمة المعلوماتية". ومع ذلك، يتم انتقاد هذا الرأي لأن الهدف من التجريم هو حماية النظام المعلوماتي بكل مكوناته، سواء كانت مادية أو معنوية، وتشمل حتى منتجاته[1].

تُطلق على الجريمة المعلوماتية العديد من التسميات مثل جريمة الكمبيوتر والإنترنت، وبعض الأشخاص يشير إليها باسم الجريمة الإلكترونية، وهي جريمة تسيء استخدام تقنية المعلومات. وهناك أيضًا من يطلق عليها اسم "الجرائم المستحدثة."

[1] جميل عبد الباقي الصغير – أدلة الإثبات الجنائي والتكنولوجيا الحديثة – (أجهزة الرادار – الحاسبات الآلية – البصمة الوراثية – دراسة مقارنة – دار النهضة العربية – القاهرة – ٢٠٠١م.

المقربون من التعريف الفني يرون الجريمة المعلوماتية على أنها "نشاط إجرامي يستخدم تقنية الحاسوب بشكل مباشر أو غير مباشر كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود[1]."

ويروى الجانب القانوني أن تعريف جرائم الحاسوب يتطلب تعريف المصطلحات الأساسية المرتبطة بعناصر الجريمة المعلوماتية، وهي: 1) الحاسوب، 2) برنامج الحاسوب، 3) البيانات، 4) الممتلكات، 5) الدخول، 6) الخدمات، 7) الخدمات الحيوية[2].

يختصر الجانب الجنائي جرائم الحاسوب بأنها "استخدام غير قانوني للحواسيب، وتأخذ شكل فيروس يهدف إلى تدمير الثروة المعلوماتية". وهناك أنواع متعددة من فيروسات الحاسوب وفقًا للأهداف المطلوبة، وتشمل:

1. اختراق أنظمة معلومات بنوك معينة لتحويل الأموال من حسابات العملاء إلى حساب المجرم.
2. اختراق أنظمة معلومات الآخرين لنقل المعلومات المعالجة إلكترونياً أو نقل برنامج من برامجهم إلى نظام المجرم.

---

[1] .جميل عبد الباقي الصغير – الإنترنت والقانون الجنائي – الأحكام الموضوعية للجرائم المتعلقة بالإنترنت – دار النهضة العربية – القاهرة –٢٠٠١م.

[2] د.جميل عبد الباقي الصغير – القانون الجنائي والتكنولوجيا الحديثة – الكتاب الأول – الجرائم الناشئة عن استخدام الحاسب الآلي – ط١ – دار النهضة العربية – القاهرة – ١٩٩٢م.

3. اختراق أنظمة معلومات الآخرين للتجسس على مؤسسات هامة في الدولة أو التجسس على أسرار الأفراد أو التلاعب في بياناتهم الشخصية بالحذف أو الإضافة أو التعديل.
4. اختراق أنظمة معلومات الآخرين للاستفادة من إمكانيات الحاسوب ذاته، وهو ما يعرف بسرقة وقت الحاسوب.
5. اختراق أنظمة المعلومات لتدمير الثروة المعلوماتية المخزنة فيها جزئيًا أو كليًا[1].

وبينما يشمل التعريف السابق الجريمة المعلوماتية المرتبطة بالحاسوب وشبكة الإنترنت، إلا أنه لا يشملها بشكل شامل. تعتبر الحوسبة وشبكة الإنترنت وسائل يمكن استخدامها في ارتكاب جرائم متنوعة مثل التزوير والقتل والاحتيال[2].

توجد زاوية أخرى في الفقه القانوني لتعريف الجريمة المعلوماتية، وهو التعريف الذي ينص على أنها "الجريمة التي ترتكب باستخدام الحاسوب الآلي أو عليه، أو عن طريق شبكة الإنترنت". يمتاز هذا التعريف بالوضوح والبساطة، لكنه يعاني من عدم إشارته إلى وقوع الجريمة المعلوماتية على

[1] Agarwal, A., Gupta, M., Gupta, Mr., Gupta, Y., & Gupta, C. (2011). Systematic Digital Forensic Investigation Model. Gupta International Journal of Computer Science and Security, 2011, 118

[2] جون فورستر – مجتمع التقنية العالية – قصة ثورة تقنية المعلومات – ط١ – ترجمة ونشر مركز الكتاب الأردني – الأردن – ١٩٨٩م.

شبكة الإنترنت في حالا تعطيل الشبكة أو بطء سرعتها أو إتلاف المواقع على الشبكة

يروي هذا الجانب الفقهي أن الجريمة المعلوماتية تتميز بكونها جريمة مستترة وسرعة تطورها في أساليب ارتكابها، كما أنها أقل عنفًا في تنفيذها وقادرة على تجاوز الحدود. يعتبر من الصعب إثباتها نظراً لعدم وجود أدلة مادية، ويسهل تدمير الأدلة المتعلقة بها. كما يعاني الجهات المعنية بتطبيق القانون من نقص الخبرة وعدم كفاية القوانين الحالية في مواجهة هذه الجرائم.[1].

هناك تعريف آخر للجريمة المعلوماتية وفقًا للفقه، وينص على أنها "سلوك غير قانوني يعاقب عليه قانوناً، ينبع من إرادة متعمدة ويتعلق ببيانات الحاسوب". يشمل السلوك الإجرامي الأفعال والامتناع عنها، ويُعتبر غير قانوني بسبب عدم مطابقته للقوانين. تعاقب عليه قانوناً لأن تحديد الطابع الجنائي للسلوك يتطلب إرادة المشرع والتعبير عن ذلك في النصوص القانونية، حتى إن كان السلوك ضاراً بالأخلاق. ويعتبر المحل الرئيسي

[1] حسن الجوخدار – شرح قانون أصول المحاكمات الجزائية – ط٢ – مكتبة دار الثقافة – عمان – ١٩٩٧م.

لجريمة الحاسوب هو البيانات بمفهومها الواسع، والتي تشمل البيانات المدخلة والمخرجة والمخزنة والبرامج.[1]

تولي التشريعات الإماراتية اهتماماً بالغاً للبيانات الحكومية، حيث تعرفها في المادة (1) من المرسوم بقانون اتحادي رقم (5) لسنة 2012 بأنها "البيانات أو المعلومات الإلكترونية الخاصة بالحكومة الاتحادية أو الحكومات المحلية لإمارات الدولة أو الهيئات العامة أو المؤسسات العامة الاتحادية أو المحلية". هذا التعريف البسيط يشمل جريمة الحاسوب، لكنه لا يشمل الجرائم التي ترتكب عن طريق شبكة الإنترنت والتي تتطلب وجود حاسوب بأشكاله المختلفة[2]

وباستناد إلى التقدم العلمي الحالي، فإن هناك أجهزة إلكترونية محوسبة تقوم بوظائف الحاسوب، مثل الهواتف المحمولة وأجهزة السيارات المزودة بأنظمة حاسوبية والتي يمكنها الاتصال بشبكة الإنترنت. لذلك، فإن تعريف الجريمة المعلوماتية يجب أن يشمل هذه الاحتمالات الجديدة.

---

[1] حسن صادق المرصفاوي – قانون الإجراءات الجنائية مع تطوراته التشريعية ومذكراته الإيضاحية وأحكام النقض في خمسين عاماً – موسوعة الفقه والقضاء للدول العربية – الجزء (١٤٠) – الدار العربية للموسوعات – بيروت – ١٩٨١م.

[2] حسن الجوخدار – شرح قانون أصول المحاكمات الجزائية – ط٢ – مكتبة دار الثقافة – عمان – ١٩٩٧م.

كذلك بأنها : "الاستخدام غير المصرح به لأنظمة الكمبيوتر المحمية أو ملفات البيانات أو الاستخدام المتعمد الضار لأجهزة الكمبيوتر أو ملفات البيانات".

ونرى أنه رغم تعدد التعريفات ضيقاً واتساعاً، إلا أن الراجح فقهاً أن الجريمة المعلوماتية هي الجريمة التي يكون "المال المعلوماتي" موضوعاً (محلاً) لها، أما الجريمة التقليدية المرتكبة بواسطة المعلوماتية، فتقصى من طائفة الجرائم المعلوماتية، إذ إن تعريف أية جريمة لا يتم بالاعتماد على الوسيلة المستخدمة في ارتكابها ، إنما بالرجوع إلى العمل الأساسي المكون لها.[1]

[1] Cohen, F. (2010). Toward a Science of Digital Forensic Evidence Examination. IFIP Advances in Information and Communication Technology, 337, 17-35

المطلب الثاني

اتجاهات تصنيف الجريمة المعلوماتية وصورها

مقدمة

تواجه المجتمعات والأجهزة الأمنية تحدياً في مكافحة الجريمة القديمة والجرائم المستحدثة التي زادت في حجم الضحايا والخسائر على كافة المستويات. مع انتشار استخدام الإنترنت كوسيلة تجارية، زادت الجريمة على الإنترنت بشكل مطرد وتنوعت أشكالها، مثل سرقة بيانات الحسابات المصرفية وبطاقات الائتمان، وترويج صور الأطفال في المواقع الإباحية، وغسل الأموال عبر حسابات بنكية على الإنترنت[1].

تم اختراع التقنية ووسائلها لتسهيل حياة الإنسان عبر العصور، ولكن استغلال المجرمين للبيانات التقنية يشكل قلقاً عالمياً. رغم أن التقنية وشبكات المعلومات ساهمت في التواصل الحضاري والثقافي، إلا أنها أيضاً ساهمت في عولمة الجريمة، حيث أصبحت التحديات الجرمانية تهدد الأمن الوطني والدولي. [2]فقد خلقت تسهيلات كبيرة للأنشطة الإجرامية المنظمة والفردية، وتساعد في

---

[1] د.حسني الجندي – الدفع ببطلان التفتيش في ضوء أحكام محكمة النقض دراسة تحليلية تأصيلية – دار النهضة العربية – القاهرة – ١٩٨٨/١٩٨٩م.

[2] حسن صادق المرصفاوي – قانون الإجراءات الجنائية مع تطوراته التشريعية ومذكراته الإيضاحية وأحكام النقض في خمسين عاماً – موسوعة الفقه والقضاء للدول العربية – الجزء (١٤٠) – الدار العربية للموسوعات – بيروت – ١٩٨١م.

تنشيط النشاط الإجرامي. يثار التساؤل عن فعالية آليات مكافحة الجرائم الجديدة، سواء من خلال التقنية العلمية أو تأهيل العناصر البشرية لاكتشاف الجرائم التقنية المعقدة والتعامل مع الأدلة الرقمية.[1]

تتنوع أشكال الجرائم عبر الإنترنت، ولكن يجمعها الحاجة إلى العملات الرقمية لتسهيل التبادل التجاري، سواء كانت قانونية أو غير قانونية، عبر أجهزة الكمبيوتر المتصلة بالشبكة.

منذ بداية ظهور الإنترنت، ظهرت العديد من البدائل للعملات الورقية التقليدية، وآخرها كانت "إي–جولد المحدودة"، وهي شركة أمريكية تقدم عملة رقمية تسمى الذهب الإلكتروني كبديل فريد للمعاملات التجارية عبر الإنترنت. يمكن للعملاء الحصول على حساب دون جهة رقابية، ويمكنهم استخدام أسماء مزيفة. يتم شراء وحدات الذهب الإلكتروني عن طريق بطاقة ائتمان أو تحويل إلكتروني، ويمكن نقلها بسهولة لأي عميل آخر لديه حساب لدى الشركة[2].

بالنسبة لمستلم الأموال، يمكن تحويل وحدات الذهب الإلكتروني إلى أموال تقليدية بنفس السهولة، دون الكشف عن هويته الحقيقية. تجذب فكرة الذهب

[1] Cohen, F. (2010). Toward a Science of Digital Forensic Evidence Examination. IFIP Advances in Information and Communication Technology, 337, 17-35

[2] Ieong, R. (2006). FORZA: A Digital Forensics Investigation Framework Incorporating Legal Issues. Digital Investigation, 3, 29-36

الإلكتروني الأشخاص الذين يفضلون الاستثمار في الذهب ويرغبون في ربط الأموال به.

فيما يتعلق بالجرائم المعلوماتية، يجب التركيز على الحالات التي تثير مشكلة في تطبيق النصوص القانونية والتي تختلف عن الجرائم التقليدية، سواء بسبب عدم مطابقتها للنصوص التقليدية أو بسبب الفراغ التشريعي لمعالجتها. نظراً لتعدد أنواع الجرائم المعلوماتية، يتم اختيار الجرائم التي تشكل تحديات قانونية أكثر، مثل جرائم الاعتداء على الحياة الخاصة وجرائم الأموال وجريمة التزوير.

أولاً: جرائم الاعتداء على الحياة الخاصة للأفراد:

تعد جرائم الاعتداء على الحياة الخاصة للأشخاص أمراً صعباً لمواجهته بالنصوص التقليدية. تتم هذه الجرائم باستخدام التكنولوجيا، مما يؤدي إلى انتهاك الخصوصية والسلوك الشخصي. تتناول هذه المقالة الحالات التي تثير مشكلات في تطبيق القوانين التقليدية وتسلط الضوء على الحاجة الملحة لمعالجة هذا النوع من الجرائم، وهي جرائم الاعتداء على الحياة الخاصة[1].

تشمل عناصر الحياة الخاصة على حرمة جسم الإنسان والمسكن والصورة والمحادثات والمراسلات والحياة المهنية. يرتبط الحياة الخاصة بالتكنولوجيا

[1] Cohen, F. (2010). Toward a Science of Digital Forensic Evidence Examination. In IFIP Advances in Information and Communication Technology (Vol. 337, pp. 17-35

المعلوماتية، حيث ازدادت أهميتها مع انتشار بنوك المعلومات في الفترة الأخيرة لتلبية احتياجات المستخدمين في المجالات العلمية والثقافية والعسكرية.

أصبحت الشبكات المعلوماتية مستودعاً خطيراً لأسرار الإنسان، حيث يمكن الوصول إليها بسهولة وسرعة غير مسبوقة. بنوك المعلومات أصبحت عناصر الحياة الخاصة الأكثر أهمية وخطورة في العصر الحديث[1].

من خلال بروتوكولات الاتصال الموحدة، مثل بروتوكول نقل البريد الإلكتروني(HITP) ، يمكن الوصول إلى بيانات شخصية المستخدمين، بما في ذلك رقم أجهزتهم ومواقعهم وعناوين بريدهم الإلكتروني. بعض المواقع تستخدم ملفات تعريف الارتباط (cookies) لجمع معلومات عن المستخدمين. [2]

وأحد أخطر جوانب استخدام الإنترنت هو أن كل ما يكتبه الشخص يمكن الاحتفاظ به في أرشيف يمكن الوصول إليه حتى بعد سنوات، ويمكن لمزود الخدمة على الإنترنت الوصول إلى هذه المعلومات ومعرفة المواقع التي يزورها العميل.

---

[1] د.م.ي. باجا نوف ود. يوم غرو شيفري– شرح الإجراءات الجنائية السوفيتية – ترجمة صالح العبيدي – جامعة بغداد – بغداد – ١٩٩٠م.

[2] د.رؤوف عبيد – مبادئ الإجراءات الجنائية في القانون المصري – ط ١١ – القاهرة – ١٩٧٦م / وط ١٦ – ١٩٨٥م.

اهتمت القوانين المقارنة بمسألة حماية البيانات الشخصية وتبنت العديد من الضمانات المهمة، ويمكن تلخيصها كالتالي:

1. مبدأ الإخطار العام: يتطلب من الهيئات المعنية بجمع البيانات إبلاغ الجمهور بمعلومات حول عملية جمع البيانات ونوع المعلومات التي يتم تسجيلها. يجب وضع قيود على إنشاء أنظمة المعلومات المختلفة لمعالجة البيانات.
2. شرعية الحصول على المعلومة: يجب أن يتم الحصول على المعلومات بطرق شرعية وخالية من الغش والاحتيال. تحظر بعض القوانين تسجيل أي معلومة دون موافقة صاحبها، كما هو الحال في القانون الفرنسي للمعلوماتية.
3. التناسب بين المعلومات الشخصية المسجلة والهدف من التسجيل: يجب على الجهة المعنية بإنشاء نظام معلوماتي تحديد هدفها من تسجيل تلك المعلومات[1].

وتضمنت بعض القوانين العربية نصوصاً وقواعد تحمي البيانات الشخصية وتفرض عقوبات على كشف هذه البيانات، مثل الفصل العاشر من قانون التجارة الإلكترونية المصري الصادر في عام 2004، الذي يحمي سرية البيانات المشفرة ويحترم الحق في الخصوصية، وكذلك قوانين التجارة

[1] د. عبد الحميد الشواربي – ضمانات المتهم في مرحلة التحقيق الابتدائي – منشأة المعارف – الإسكندرية – ١٩٨٨م.

الإلكترونية والمعاملات الإلكترونية في دبي وتونس، الصادرة في عام 2002 وعام 2000 على التوالي.

تشتمل النصوص الجنائية التي صاغت لحماية الحياة الخاصة على تجريم عدة أفعال، ويمكن تلخيصها على النحو التالي:

1. جريمة انتهاك حرمة المسكن: تأتي هذه الجريمة نظراً للأهمية الكبيرة التي يُعتبر بها المسكن في القوانين العربية عموماً. وتكمن أهمية المسكن ليس فقط في حرمته الكبيرة، ولكن أيضاً لأنه يُمثل قلعة حصينة يجب ألا يُخترق إلا بطرق غير مشروعة أو بدون موافقة صاحبه[1].
2. جريمة الاطلاع على الرسائل: تحظى هذه الجريمة بتنصيصات في معظم التشريعات العربية. وقد قام المشرع العربي بتوسيع مفهوم الرسالة، حيث يمكن أن يشمل ذلك رسائل البريد الإلكتروني. ومع ذلك، لا يمتد هذا الحماية إلى البيانات المخزنة في أنظمة المعلومات لجهات أخرى، سواء كانت عامة أو خاصة. فالحاسوب الآلي أصبح اليوم مستودعاً ضخماً للمعلومات والبيانات في آن واحد، وليس مجرد جهاز للاتصال ومعالجة المعلومات[2].

[1] د.رؤوف عبيد – مبادئ الإجراءات الجنائية في القانون المصري – ط ١١ – القاهرة – ١٩٧٦م / وط ١٦ – ١٩٨٥م.

[2] Kundi, G. M., Nawaz, A., & Akhtar, R. (2014). Digital Revolution, Cyber Crimes And Cyber Legislation: A Challenge To Governments In

3. جريمة إذاعة معلومات تتعلق بإجراء جنائي: تقتصر الحماية في هذه الجريمة على الإجراءات الجنائية.

ويجب الإشارة أيضًا إلى معاهدة بودابست لعام 2001 التي تهدف إلى توحيد الجهود الدولية لمكافحة جرائم الكمبيوتر. وتضمنت المعاهدة العديد من التعريفات للأفعال المجرمة، وتترك لكل دولة تحديد العقوبة المناسبة لتلك الأفعال[1].

وتنص المادة الثانية من المعاهدة على تجريم الدخول غير المشروع إلى أنظمة معلوماتية، بينما تنص المادة الثالثة على تجريم اعتراض تلك البيانات بأي وسيلة إلكترونية دون وجه حق. وتنص المواد اللاحقة على تجريم تعديل البيانات أو تحريفها أو تدميرها أو تعديلها أو تغيير مسارها، بالإضافة إلى تجريم التدخل في النظام المعلوماتي والعمليات المنطقية. وتنص المادة السادسة على تجريم إساءة استخدام النظام المعلوماتي بطريقة تؤدي إلى كشف نظم الحماية الخاصة به بدون وجه حق.

لذا، ينبغي على المشرع في الدول العربية التدخل لتوفير الحماية الجنائية اللازمة، حيث أن عناصر الحياة الخاصة لم تعد تقتصر فقط على المسكن

Developing Countries. International Journal of Academic Research in Business and Social Sciences, 4

[1] Adams, R., Hobbs, V., & Mann, G. (2013). The Advanced Data Acquisition Model (Adam): A Process Model for Digital Forensic Practice. Journal of Digital Forensics, Security and Law

والصورة والمحادثات الهاتفية أو الرسائل البريدية. ففي عصر العولمة، أنتجت تكنولوجيا المعلومات عناصر جديدة للخصوصية تحتاج بشدة إلى الحماية القانونية[1].

ثانيا: جرائم الاعتداء على الأموال:

في الدول العربية، تُجرم قوانين العقوبات الاعتداء على الأموال بصورها التقليدية، مثل السرقة والنصب وخيانة الأمانة واختلاس الأموال العامة. ومع ذلك، في الماضي، كانت تلك القوانين تنطبق بشكل رئيسي على الأموال الورقية والمعدنية والصكوك والأوراق المالية التقليدية، مثل الكمبيالات والسندات الإذنية المرتبطة بالمصارف التقليدية التي كانت لديها مقرات ثابتة. كانت أقصى درجات التطور في هذا المجال هي تنفيذ عمليات التحويل المصرفي بوساطة إجراءات ورقية معقدة وبدفع رسوم مالية[2].

فيما يتعلق بالسرقة، يمكن تطبيق مفهوم الاختلاس المادي على التحويلات المالية غير المشروعة التي تتم عبر المصارف التقليدية. فقد لم يحدد المشرع شكل السلوك الجنائي للسرقة في إطار الجرائم ذات القالب الحر، ويمكن

[1] د. عبد العظيم الوزير – شرح قانون العقوبات – القسم الخاص – جرائم الاعتداء على الأموال – ط ١ – دار النهضة العربية – القاهرة – ١٩٩٣م.

[2] Kamran, A., Arafeen, Q., & Sheikh, A. (2020). Existing Cyber Laws and Their Role in Legal Aspects of Cybercrime in Pakistan. International Journal of Cyber-Security and Digital Forensics, 8, 241-249

للسرقة أن تتم عن طريق أي فعل يؤدي إلى سلب المال المنقول من المجني عليه وتحويله للجاني[1].

بالنسبة للنصب، يتحقق السلوك الجنائي بالاستيلاء على أموال الآخرين بوساطة طرق احتيالية. والآن يطرح السؤال: هل ينطبق ذلك على جرائم السرقة والاحتيال التي تتم باستخدام التكنولوجيا المعلوماتية؟

سنناقش الآن الوسائل التقنية التي يتم من خلالها الاختلاس، ومن ثم سنعرض التكييف القانوني لتلك الجرائم في غياب تشريعات واضحة في معظم الدول العربية.

[1] د. عبد الفتاح بيومي حجازي – الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت – دراسة متعمقة في جرائم الحاسب الآلي والإنترنت – دار الكتب القانونية – القاهرة – ٢٠٠٢م.

1- الوسائل الفنية للتحويل الإلكتروني للأموال

تعتمد عمليات التحويل غير المشروع للأموال على عدة وسائل متنوعة نظراً للتطور السريع في هذا المجال. ومن بين تلك الوسائل، يمكن التركيز على الأكثر انتشاراً وشيوعاً

.أ- استخدام برامج مخصصة لتنفيذ الاختلاس: تعتبر تصميم برامج معينة أحد أشهر الوسائل المستخدمة لتنفيذ عمليات التحويل الآلي من حساب إلى آخر، سواء كان ذلك داخل نفس المصرف أو بين مصارف مختلفة. كمثال على ذلك، قام أحد الموظفين المتعاقدين مع مصرف الكويت التجاري بتطوير أنظمة المعلومات بالاستيلاء على مبالغ ضخمة من المصرف. عمل هذا الموظف على تحديد خمسة حسابات غير نشطة في خمسة فروع محلية للمصرف، وقام ببرمجة برنامج يقوم بتحويل مبالغ محددة من تلك الحسابات إلى حسابات أخرى أنشأها باسمه في نفس الفروع.

تم تنفيذ عملية التحويل أثناء تواجده على متن الطائرة المتوجهة إلى المملكة المتحدة بعد انتهاء فترة عمله. وعند وصوله، قام بفتح حسابات جديدة وطلب من المصرف تحويل تلك المبالغ إلى حساباته الجديدة في بريطانيا. هناك أيضاً برامج أخرى تقوم بخصم مبالغ صغيرة من الفوائد المصرفية عن طريق تجاهل الكسور العشرية، حيث يتم تحويل الفارق مباشرة إلى حساب الجاني. [1]

[1] د. أحمد أبو الروس – التحقيق الجنائي والتصرف فيه والأدلة الجنائية – دار المطبوعات الجامعية – الإسكندرية – ١٩٩٢م.

وتعتمد هذه البرامج على التكرار الآلي لمعالجة معينة، وهو ما يجعل من الصعب اكتشاف هذه الطريقة حتى في حالة المبالغ الكبيرة. يتم خصم هذه المبالغ من آلاف الحسابات في وقت واحد، مع أن المبلغ المخصوم من كل حساب يكون صغيراً بحيث يكون من الصعب على العملاء التنبه لهذه العمليات.

ب- التحويل المباشر للأرصدة: يتم ذلك عن طريق اختراق أنظمة الحاسوب وشفرات المرور. على سبيل المثال، قام خبير حاسوب في الولايات المتحدة بتسلل إلى نظام معلوماتي لأحد المصارف ونجح في تحويل 12 مليون دولار إلى حسابه الشخصي في ثلاث دقائق فقط. وعادةً ما يتم ذلك أيضاً من خلال إدخال معلومات مزيفة وإنشاء حسابات وهمية وتحويل الأموال إلى حساب المتسلل. يمكن أيضاً تنفيذ التحويل المباشر عن طريق التقاط الإشعاعات الصادرة عن الأجهزة المتصلة بشبكات الأقمار الصناعية، حيث يمكن اعتراض هذه الإشعاعات وفك تشفيرها باستخدام جهاز مخصص لذلك وإعادة بثها بعد التلاعب بها. هذا ما تنص عليه اتفاقية بودابست في المادة الخامسة[1].

8. Losavio, M., Adams, J., & Rogers, M. (2006). Gap Analysis: Judicial Experience and Perception of Electronic Evidence. Journal of Digital Forensic Practice, 1, 13-17

[1] إبراهيم صالح المحامي – التعليمات العامة للنيابات في المسائل الجنائية حسب آخر التعديلات – القاهرة – ١٩٩٤م

ج- التلاعب بالبطاقات المالية: يتم ذلك عن طريق استخدام أرقام سرية لبطاقات الائتمان والبطاقات المالية المختلفة بعد سرقتها أو الحصول عليها بشكل غير قانوني. يتم ذلك عن طريق اختراق بعض المواقع التجارية التي يتم تسجيل أرقام البطاقات عليها.

وفي هذه الحالات، يمكن تطبيق قوانين السرقة والنصب على الأفراد الذين يستخدمون هذه البطاقات بصورة غير مشروعة، سواءً كان ذلك بسرقة البطاقة نفسها أو الرقم السري واستخدامه للتلاعب في المؤسسات المالية وسحب الأموال. ويجدر بالذكر أن الجرائم المرتبطة بالاحتيال ليست مقتصرة على الأفراد، بل يمكن أن تشمل أيضًا الآلات، حيث يكفي أن تؤدي هذه الأفعال الاحتيالية إلى الحصول على منفعة غير مشروعة مع إلحاق ضرر بالآخرين[1].

د- جرائم الاعتداء على أجهزة الصراف الآلي للنقود: تنشأ هذه المشكلة عندما يتم استخدام جهاز الصراف الآلي لسحب مبالغ تتجاوز الرصيد الفعلي لحامل البطاقة. في هذه الحالة، يتم اعتبارها مسألة مديونية بين العميل والمؤسسة المالية، ولا يمكن اعتبارها سرقة، لأن المبلغ المستولى عليه لا يتم الحصول

[1] د. عبد الفتاح بيومي حجازي – الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت – دراسة متعمقة في جرائم الحاسب الآلي والإنترنت – دار الكتب القانونية – القاهرة – ٢٠٠٢م.

عليه دون موافقة المؤسسة المالية. فالمؤسسة على علم بأن الجهاز لا يمتلك حداً أقصى للسحب يمنع تجاوزه[1].

هـــ- جرائم الاستيلاء على النقود الإلكترونية: يمكن تعريف النقود الإلكترونية (المال الإلكتروني) على أنها قيمة نقدية مخزنة على وسيلة إلكترونية مدفوعة مسبقًا وغير مرتبطة بحساب بنكي، وتقبلها الأطراف المستقبلة التي أصدرتها كوسيلة للدفع. تتميز النقود الإلكترونية بأنها تُحمَّل على بطاقة بلاستيكية أو تخزن على القرص الصلب للحاسوب الشخصي للمستهلك.[2]

وتختلف عن البطاقات الائتمانية، حيث يتم دفع النقود الإلكترونية مسبقًا، ولا ترتبط بحساب العميل، بل تعتبر استحقاقًا مستقلًا يتم تبادله بين العميل والتاجر دون الحاجة لجهة ثالثة، مثل البنك. تستخدم النقود الإلكترونية مجموعة من البروتوكولات والتوقيعات الرقمية التي تمكن الرسائل الإلكترونية من استبدال التداول النقدي. يتم إدخال هذه البطاقات إلى جهاز المعاملات المالية للتاجر أو

[1] علي عبد القادر القهوجي – الندب للتحقيق – دار الجامعة الجديدة للنشر . الإسكندرية – ١٩٩٧م.

[2] د.أحمد عوض بلال – الإجراءات الجنائية المقارنة والنظام الإجرائي فى المملكة العربية السعودية – دار النهضة العربية – القاهرة – ١٩٩٠م.

الدائن، حيث يتم نقل المعلومات من البطاقة إلى جهاز البائع، وتحويل نتائج العمليات التجارية إلى بنك البائع[1].

2- التكييف القانوني لهذه الأنماط من السلوك :

تدخل القانون العربي النموذجي بالنص على تجريم الصور السابقة، والاستيلاء على الأموال، فقضى في المادة السادسة أنه كل من استخدم بطاقة ائتمانية للسحب الإلكتروني من الرصيد خارج حدود رصيده الفعلي، أو باستخدام بطاقة مسروقة ، أو تحصل عليها بأية وسيلة بغيرحق، أو استخدم أرقامها في السحب أو الشراء وغيرها من العملات المالية مع العلم بذلك، يعاقب بالحبس وبالغرامة، وهو ما يعني أن هذا النص قاصر على توفير الحماية لغيرها من البطاقات لتقدير الدولة.[2]

أما اتفاقية بودابست السابق الإشارة إليها، فقد نصت المادة الثامنة منها والخاصة بالتحايل المرتبط بالحاسب computer related frau على معاقبة أي شخص يتسبب بأي خسائر مادية للغير عن طريق تعديل أو محو أو إيقاف أي بيانات مخزنة في أي نظام معلوماتي، أو عن طريق أي تدخل فيه، وبذلك

[1] د. أحمد فتحي سرور – الشرعية والإجراءات الجنائية – دار النهضة العربية – القاهرة – ١٩٧٧م – وط ١٩٩٥م.

[2] أسامة أحمد المناعسة وجلال محمد الزعبي وصايل الهواوشة – جرائم الحاسب الآلي والإنترنت – دراسة تحليلية مقارنة – ط ١ – دار وائل – عمان – ٢٠٠١م.

تتوفر الحماية الجنائية اللازمة للأموال في مواجهة السلوك المرتكب بالحاسب الآلي.[1]

إذا كانت جرائم الأموال المرتكبة بواسطة الحاسب الآلي تواجه فراغاً تشريعياً في العديد من الدول العربية، فإن المشكلة الحقيقية في نظرنا بالنسبة لهذه الجرائم لا تتمثل في الفراغ التشريعي بقدر ما هي كامنة في طرق ضبطها وإثباتها، وهو ما يرجع إلى افتقاد الآثار التقليدية التي قد تتركها أي جريمة في الجريمة المعلوماتية[2]فالبيانات يتم إدخالها مباشرة في الجهاز دون أن تتوقف على وجود وثائق أو مستندات، لأنه كثيراً ما يكون هناك برامج معدة ومخزنة سلفاً على الجهاز، ولا يكون عليه سوى إدخال البيانات في الأماكن المعدة لها، كما هو الحال بالنسبة للمعاملات المصرفية.[3]

والمؤسسات التجارية الكبرى، ويمكن في هذه الفروض اقتراف جرائم الاختلاس والتزوير، فتفقد الجريمة آثارها التقليدية . فالجريمة المعلوماتية ترتكب في مسرح خاص يتمثل في عالم اقتراضي مفرغ cyberspace وهو ما يختلف كلياً عن المسرح الذي ترتكب فيه الجرائم في صورتها التقليدية،

---

[1] أسامة محمود أبو عباس – رحلة إلى عالم الإنترنت – ط ١– شركة النجار للكمبيوتر والإلكترونيات – الأردن – اربد – ١٩٩٩م.

[2] د. أحمد عوض بلال – قاعدة استبعاد الأدلة المتحصلة بطرق غير مشروعة في الإجراءات الجنائية المقارنة – دار النهضة العربية – القاهرة – ١٩٩٤م.

[3] Casey, E. (2001). Handbook of Computer Crime Investigation: Forensic Tools and Technology. In E. Casey (Ed.), Handbook of Computer Crime Investigation: Forensic Tools and Technology

حيث تطبق القواعد العامة لانتداب الخبراء في اقتفاء آثار الجناة الذين يرتكبون جرائم تتكون من سلوك مادي ملموس، وله محل مادي ملموس أيضاً، مما لا يتناسب ونوع الخبرة المطلوبة لمعاينة المسرح السيبيري للجريمة المعلوماتية المرتكبة في الفضاء الإلكتروني.[1]

فالخبرة المطلوبة للتحقيق في الجريمة المعلوماتية يجب أن تكون على درجة عالية من الكفاءة العلمية أو العملية أيضاً، وهو ما يوجب أن يكون الخبير في الجريمة المعلوماتية ملماً بأدق تفاصيل تركيب الحاسب وعمل الشبكات المعلوماتية والأماكن المحتملة للأدلة، كالمواضع التي يمكن أن تحتفظ بآثار الاختراق وتوقيته، والبرامج المستخدمة في أي عملية تمت أثناء الاختراق، بالإضافة إلى إمكانية نقل الأدلة إلى أوعية أخرى دون تلف.[2]

ويجب الإشارة إلى أن ملاحقة الجرائم المعلوماتية لا تتطلب رفع كفاءة الخبراء فقط، بل تحتاج إلى رفع كفاءة مأموري الضبط القضائي بصفة عامة، لأن مأمور الضبط القضائي أول شخص يكتشف الجريمة، ويتصل بمسرحها ، والمسؤول الأول عن التحفظ على أي أثر يتركه الجاني بعد ارتكابه للجريمة، مما يستوجب أن يكون المتعامل الأول مع النظام المعلوماتي على درجة من

[1] بيتر كنت – الدليل الكامل إلى الإنترنت – ترجمة سامح الخلف – ط ١ – الدار العربية للعلوم – بيروت – ١٩٩٧م

[2] Ieong, R. (2006). FORZA: A digital forensics investigation framework that incorporates legal issues. Digital Investigation, 3, 29-36

الكفاءة، تسمح له بالتحفظ على هذه الأدلة، لأن أي خطأ في التعامل الأولي مع هذه الأجهزة قد يؤدي إلى محو الأثر أو الأدلة.[1]

أما اتفاقية بودابست السابق الإشارة إليها، فقد أشارت في القسم الإجرائي منها في المادة السادسة عشر إلى أنه: "على الدول الأعضاء العمل على تطبيق أنظمة فنية لحماية البيانات المخزنة مع إلزام العاملين في أي نظام معلوماتي بحفظ كل العمليات المنطقية التي تجري على الأجهزة لمدة لا تقل على 90 يوماً"، وهو ما يعني أن الاتفاقية تشترط مستوى معيناً للكفاءة الفنية في العمل بهذه التقنية، مما يعني أننا نحتاج إلى برنامج وطني متكامل لرفع مستوى كفاءة العمل بهذه التقنية قبل الحديث عن إمكانية تطبيق هذه المعاهدة.[2]

ثالثاً: جريمة التزوير:

ما يهمنا في هذا الصدد محل جريمة التزوير، لأن هذه الأخيرة من الجرائم ذات القالب الحر التي لم يحدد المشرع فيها شكلاً معيناً للسلوك الإجرامي، لكن المشرع يحدد محل هذا السلوك بالوثيقة دون أن يعرفها أو يحدد مضمونها ، تاركاً للفقه والقضاء هذه المهمة.[3]

---

[1] د. أحمد عوض بلال – قاعدة استبعاد الأدلة المتحصلة بطرق غير مشروعة في الإجراءات الجنائية المقارنة – دار النهضة العربية – القاهرة – ١٩٩٤م.

[2] توفيق الشاوي – فقه الإجراءات الجنائية – ط ٢ – ج ١– ج ٢–١٩٥٤

[3] د.جميل عبد الباقي الصغير – الإنترنت والقانون الجنائي – الأحكام الموضوعية للجرائم المتعلقة بالإنترنت – دار النهضة العربية – القاهرة –٢٠٠١م.

فالوثيقة هي مجموعة من المعاملات والرموز التي تعبر تعبيراً اصطلاحياً عن مجموعة مترابطة من الأفكار والمعاني الصادرة عن شخص أو أشخاص معينين ، وتكمن القيمة الحقيقية لها ليس في مادتها أو ما تحتويه، بل تكمن فيما لهذا التعبير من دلالة اجتماعية .

فجوهر جريمة التزوير هو الإخلال بالثقة العامة التي أراد المشرع حمايتها في هذه الوثيقة، لما لها من آثار قانونية باعتبارها وسيلة للإثبات.[1]

ولما كان ذلك، فإن قوة الوثيقة في الإثبات هي جوهر الحماية الجنائية لها، ومن هنا ذهبت بعض الآراء الفقهية إلى أن كل مادة تصلح للإثبات يجوز أن تكون محلاً للتزوير، مهما كان شكلها أو مساحتها، ولا أهمية للمادة المستعملة في الكتابة، يستوي أن تكون مصنوعة من خشب أو جلد، فإذا كانت فكرة التوسع في مفهوم الوثيقة مطروحة في الفقه الجنائي قبل ظهور جرائم المعلوماتية، فإن هذا التوسع يبدو أكثر إلحاحاً في ظل الفراغ التشريعي لمواجهة جرائم التزوير المرتكبة بواسطة الحاسب الآلي، إلا أن هذا الاتجاه واجه نقداً شديداً، حيث ذهب جانب من الفقه الفرنسي قبل صدور القانون رقم 19 لسنة 1988 الخاص بالغش المعلوماتي إلى رفض اعتبار التعبير الواقع

[1] حسن صادق المرصفاوي – المرصفاوي في أصول الإجراءات الجنائية – منشأة المعارف – الإسكندرية – ١٩٩٦م.

على الاسطوانات الممغنطة تزويراً، استناداً إلى اعتبارين، **أولهما :** انتفاء الكتابة، لأن التغيير انصب على نبضات إلكترومغناطيسية.[1]

والثاني هو عدم التيقن من صلاحيتها في الإثبات. يؤيد هذا الرأي قياس ذلك على انتفاء التزوير في التغيير الذي يطرأ على الصوت المسجل، والعلة هي انعدام عنصر الكتابة، بالإضافة إلى أن النبضات الإلكترومغناطيسية تمثل جزءاً من ذاكرة الآلة أو برنامج تشغيلها، وهو ما يمكن أن يتحقق معه الإتلاف أو التقليد إذا توافرت شروطهما، وقد بدأ الفكر القانوني الحديث يقبل فكرة الوثيقة الإلكترونية استناداً إلى أن المادة التي تصنع منها الوثيقة ليست عنصراً فيها.[2]

إن مجاراة التقدم العلمي والتكنولوجي تتطلب تجاوز المفهوم التقليدي للوثيقة، أو حصره في الورق المكتوب. ويمكن لنا في هذه الحالة أن نجد سنداً لهذه الفكرة ومنطلقاً لها، أن المشرع المدني في الأصل، رغم أخذه بمبدأ سيادة الدليل الكتابي على غيره من طرق الإثبات، إلا أنه أورد عليه بعض الاستثناءات، فقبل الإثبات بالبينة فيما كان يجب إثباتها كتابةً، وهي اتفاق الأطراف على الإثبات بالبينة أو وجود مانع يحول دون الحصول على الدليل الكتابي، فإذا اتفق الأطراف على الإثبات بالبينة، يكون على القاضي أن يعتد بها استناداً إلى عدم تعلق القواعد الموضوعية في الإثبات بالنظام العام، مما

[1] د.نوري حمد خاطر – قراءة في قانون حق المؤلف الأردني رقم (٢٢) لسنة ١٩٩٢م – بحث مقدم لمجلة مؤته للبحوث والدراسات – المجلد ١٢ – العدد ١ تشرين أول – ١٩٩٧م.

[2] Rahardjo, B. (1998). Keamanan Sistem Informasi Berbasis Internet

يمكن القول معه على إمكانية اتفاق الأطراف على الإثبات بالوسائل الإلكترونية، وهو ما يعد إيذاناً ببداية عصر الوثائق الالكترونية.

وقد استجابت العديد من دول العالم إلى الاتجاه السابق، واعترفت بحجية المستندات الإلكترونية في الإثبات، ومن ثم إلى اعتبارها محلاً لجريمة التزوير ، وقد كانت المملكة الأردنية الهاشمية سباقة في ذلك؛ حيث أصدرت قانون الأوراق المالية المؤقت رقم 23 لسنة 1997 الذي نص في المادة (2/24) على أن : تعتبر القيود المدونة في سجلات البورصة وحساباتها، سواء كانت مدونة يدوياً أو إلكترونياً أو أي وثائق صادرة عنها ، دليلاً على تداول الأوراق".[1]

أما بالنسبة لتجريم تزوير الوثائق الإلكترونية، فقد كان القانون الفرنسي رقم 19 الصادر في يناير 1988 أول التشريعات التي جرمت تزوير المستندات المعلوماتية، فنص في المادة (5/462)

على أن : "كل من ارتكب أفعالاً تؤدي إلى تزوير المستندات المعلوماتية أياً كان شكلها بأي طريقة تؤدي إلى حدوث ضرر للغير، فإنه يعاقب بالسجن من سنة إلى خمس سنوات وغرامة لا تقل عن 20.000 فرنك"، وقضت الفقرة السادسة من ذات المادة على معاقبة كل من استخدم المستندات المعلوماتية المزورة طبقاً للفقرة السابقة، ولم يكتف المشرع الفرنسي بذلك، بل نص على

[1] حسن صادق المرصفاوي – المرصفاوي في أصول الإجراءات الجنائية – منشأة المعارف – الإسكندرية – ١٩٩٦م.

إمكانية ارتكاب جريمة التزوير خطأ[1]، لأن التغيير والتحريف للمعلومات المخزنة خطأً وإن كان غير متصور في المستندات والوثائق التقليدية، إلا أنه كثيراً ما يحدث في المجالات المعلوماتية لأن الدخول إلى الأنظمة المعلوماتية لا يحدث دائماً بشكل متعمد ، فمن الممكن أن يحدث بشكل غير معتمد نتيجة الدخول الخاطئ إليه، وهو ما يجب النص عليه في تجريم التزوير في المستندات المعلوماتية .[2]

كما ألزم القانون العربي النموذجي الدول على معاقبة كل من غيّر في البيانات المخزنة في المستندات المعالجة آلياً، أو البيانات المخزنة في ذاكرة الحاسب الآلي، أو على شريط أو اسطوانة ممغنطة، أو غيرها من الوسائط.

تجدر الإشارة إلى أن كل حالات السرقة والاحتيال تتم عن طريق تزوير البيانات، لنجد أننا أمام حالة من حالات تعدد الجرائم ، فالأمثلة التي سبقت الإشارة إليها في الفقرة الخاصة بالسرقة، سواء كانت بتصميم برنامج معد خصيصاً ، أو عن طريق إجراء عمليات تحويل غير مشروعة للأرصدة بخلق حسابات دائنة وهمية كلها لا تتم إلا بتزوير في البيانات المخزنة آلياً، لنجد أن معظم الحالات يتحقق فيها التعدد المعنوي للجرائم، خاصة مثل التلاعب الذي

---

[1] د. حسن بشيت خوين ضمانات المتهم في الدعوى الجزائية – ج ١+٢ – ط ١ – دار الثقافة – عمان – ١٩٩٨م.

[2] د. هشام محمد فريد رستم – الجرائم المعلوماتية – أصول التحقيق الجنائي الفني واقتراح بإنشاء آلية عربية موحدة للتدريب التخصصي – بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت – في (٣-١ مايو) ٢٠٠٠م.

يتم في الأرصدة المصرفية، لأن عمليات التحويل غير المشروعة تتم عن طريق تعديل في البيانات والأسماء، أو تعديل في البرامج المعلوماتية المعالجة لهذه البيانات .[1]

فإذا كان السلوك الإجرامي في هذه الحالة متمثلاً في تعديل البرامج والبيانات يترتب عليه تحويلات مالية غير مشروعة، فإن السلوك أو الفعل يظل واحداً يتحقق به أكثر من نموذج تجريمي في هذه الحالة، وهو ما يوجب تطبيق أحكام التعدد المعنوي والارتباط بين الجرائم.[2]

تجدر الإشارة إلى أن هذا التوسع في تفسير مفهوم الوثيقة لا يغني عن ضرورة تدخل المشرع لمواجهة التزوير المرتكب بالحاسب الآلي على المستندات والوثائق الإلكترونية، لأن المسألة تحتاج أولاً إلى الاعتراف بحجية هذه المستندات الإلكترونية في الإثبات قبل تجريم تحريفها، بالإضافة إلى أن تجريم التعديل في هذه البيانات، يجب أن يخضع لعقوبات أشد من عقوبة التزوير التقليدية، نظراً لاختلاف حجم الضرر والخسائر الناتجة عن تحريف هذه البيانات وتزويرها.

وقد نصت اتفاقية بودابست في المادة السابعة على تجريم أي تبديل أو محو أو إخماد لأي بيانات مخزنة في أي نظام معلوماتي يؤدي إلى إنتاج

[1] د. محمد الأمين البشري – التحقيق في جرائم الحاسب الآلي – بحث مقـدم لمؤتمر القانون والكمبيوتر والإنترنت – جامعة الإمارات العربية – ٢٠٠٠م.

[2] Faiz, M., Umar, R. & Yudhana, A. (2017). Implementation of Live Forensics for Browser Comparison in Email Security. Jesica, 1, 108-114

بيانات غير حقيقية –in authentic data– لغرض استعمالها لأغراض قانونية على أنها صحيحة، وذلك سواء كانت فورية القراءة من عدمها.

وهو ما يقطع الجدل حول قابلية المستند للقراءة بالعين المجردة، واعتبار المستند الإلكتروني وثيقة قابلة للقراءة، مشمولة بالحماية الجنائية .[1]

يتضح لنا أن الجريمة المعلوماتية تثير مشكلات عديدة في تطبيق النصوص القانونية الحالية، فإن وجد النص القانوني وأمكن أعمال المطابقة بينه وبين السلوك المرتكب، فإننا لا نجد العقوبة تتناسب وحجم الخسائر الناتجة عن ارتكاب مثل هذه الجريمة، وإذا أمكن إعمال المطابقة، وكانت العقوبة رادعة، فإننا نواجه عقبة كبيرة في عمليات ضبط هذه الجرائم وإثباتها، لأن القواعد التقليدية للإثبات وضعت لتواجه سلوكاً مادياً يحدث في العالم الفيزيائي، ولا تتناسب لإثبات جريمة مرتكبة في عالم إلكتروني أو فضاء سيبراني افتراضي غير ملموس يتكون من الذبذبات والموجات غير المرئية. وهو ما يحتم ضرورة التدخل التشريعي لتنظيم هذه المسألة عن طريق الاعتراف لقوة[2]

[1] د. محمد سعيد نمور – الأحكام العامة للجرم المشهود في التشريع الأردني – دراسة مقارنة – مجلة مؤته – المجلد ١٦ – العدد ١ – ١٩٩١م.

[2] Montasari, R. (2016). Review and Assessment of the Existing Digital Forensic Investigation Process Models. International Journal of Computer Applications, 147, 41-49

المستندات الإلكترونية في الإثبات، واعتبارها من قبيل الوثائق قبل النص على تجريم تزويرها أو التعديل فيها وتحريفها حسب الأحوال.[1]

رابعاً: جرائم الاعتداء على التجارة الإلكترونية

إن الاعتداء على التجارة الإلكترونية يتمثل في جرائم النصب والاحتيال، وإذا ما كانت جريمة النصب أو الاحتيال جريمة عمدية، فإن الركن المعنوي في صورة القصد الجنائي العام متوافر، بالإضافة إلى القصد الخاص وهو نية التملك، وفي جريمة النصب المعلوماتي يتحقق القصد العام إذا علم المتهم أنه يقوم بارتكاب فعل من شأنه إيقاع المجني عليه في الغلط الذي يحمله على تسليم ماله.[2]

فالجاني هنا يستعمل أسلوباً للإيهام بوجود ائتمان كاذب يتوصل من خلاله إلى الاستيلاء على مال الغير كله أو بعضه متى وقع على فواتير الشراء باسم كاذب، أو استغل صفة كاذبة لتحويل أموال الغير من حساب آلي آخر عن

[1] د. حسن بشيت خوين ضمانات المتهم في الدعوى الجزائية – ج ١+٢ – ط ١ – دار الثقافة – عمان – ١٩٩٨م.

[2] د.نائل عبد الرحمن صالح – واقع جرائم الحاسوب في التشريع الأردني – ورقة عمل مقدمة لمؤتمر القانون والكمبيوتر والإنترنت – جامعة الإمارات العربية المتحدة – العين – في ١-٣/٥/٢٠٠٠م.

طريق التلاعب في البيانات المدخلة، مع توافر علمه بهذه الوقائع، ومع ذلك تنصرف إرادته إليها رغم علمه بهذه الأفعال التدليسية.[1]

وفي جريمة النصب أو الاحتيال، يعتبر الركن المادي "الوسيلة التي يلجأ إليها الجاني في سبيل تحقق الغرض الذي يرمي إليه، وهو الاستيلاء لنفسه أو لغيره على مال منقول أو سند أو توقيع على هذا السند أو إلغائه أو إتلافه أو تعديله، وكذلك من وسائل الاحتيال التصرف في عقار أو منقول غير مملوك للجاني، وبناءً عليه فالوسيلة إما أن تكون بالاستعانة بطريقة احتيالية، أو باتخاذ اسم كاذب، أو صفة غير صحيحة، وإما أن تكون بالتصرف في عقار أو منقول".[2]

ويشترط في الاستعانة بأي من هذه الوسائل أن يكون من شأن ذلك خداع المجني عليه وحمله على تسلم المال المنقول أو السند أو التوقيع عليه أو إلغائه أو إتلافه أو تعديله، وعليه فإنه من المسلم فقهاً وقضاءً أن الكذب المجرد لا يكفي لتوافر الطريقة الاحتيالية مهما كان منمقاً أو مرتباً يوحي بتصديقه، وعليه فإن مجال القضاء لا يتحقق جريمة النصب بمجرد الأقوال والإدعاءات الكاذبة مهما بلغ صاحبها في توكيد صحتها حتى يتأثر بها المجني عليه، بل

---

[1] د. محمد الأمين البشري – الأدلة الجنائية الرقمية – مفهومها ودورها فـــي الإثبات – المجلة العربية للدراسات الأمنية والتدريب – المجلد ١٧-- العدد ٣٣- السنة ١٧ – الرياض – أبريل ٢٠٠٢م.

[2] يونس خالد غرب – جرائم الحاسوب – ندوة الجرائم الناجمة عن التطور التكنولوجي – المنعقدة في عمان – ٢٩-١٩٨٨/١٠/٢٨م.

لابد وأن يصاحبها أعمال مادية أو مظاهر خارجية تحمل المجني عليه على الاعتقاد بصحة ذلك، والتخلي عن حيازة المال موضوع الجريمة وتسليمه إلى الجاني.[1]

وهنا يتوجب أن تتجه الطريقة الاحتيالية إلى المجني عليه ذاته لخداعه وغشه ابتغاء اغتيال ماله، فمن يزعم بقدرته على شفاء الأمراض، أو يوهم الناس بقدرته على الاتصال بالجن وإمكان شفائهم، أو الإرشاد عن مكان مفقود، فإن هذه الوقائع وأمثالها تعد نصباً واحتيالاً، وكذلك في مجال النصب والاحتيال اتخاذ الجاني اسماً كاذباً أو صفة غير صحيحة، وهذه في الحقيقة تعد وسيلة مستقلة من وسائل النصب والاحتيال، وتلغي في حد ذاتها في تكوين الركن المادي في الجريمة؛ فيكفي أن يتسمى الجاني باسم كاذب يتوصل به إلى تحقيق غرضه دون حاجة إلى الاستعانة على إتمام جريمته بأساليب احتيالية أخرى.[2]

وكذلك يدخل في إطار النصب والاحتيال التصرف في عقار منقول غير مملوك للجاني وليس له حق التصرف فيه، وهذه الوسيلة مستقلة بذاتها، ويكفي مجرد القيام بها بتوافر الركن المادي في الجريمة دون اشتراط تأييدها بأشياء

---

[1] Valjarevic, A., & Venter, H. S. (2012). Harmonised digital forensic investigation process model. In 2012 Information Security for South Africa - Proceedings of the ISSA 2012 Conference (pp. 1-10)

[2] د. هشام محمد فريد رستم – جرائم الحاسوب كصورة من صور الجرائم الاقتصادية المستحدثة – مجلة الدراسات القانونية – جامعة أسيوط – العـــــــدد ١٧– ١٩٩٥م.

أخرى خارجية، فزعم الجاني أنه يملك المال أو أن له الحق في التصرف فيه هو في ذاته كافٍ لتحقيق الركن المادي في جريمة النصب.[1]

ويقصد بالتصرف هنا كل تصرف ناقل للملكية، كالبيع والمقايضة والهبة ، أو كل تصرف يقرر على العقار حقاً عينياً كحق الرهن، أما التأخير فلا يعد تصرفاً في جريمة النصب، ويستوي أن يكون محل التصرف عقاراً أو منقولاً، فإذا كان التصرف بالبيع مثلاً وارداً على عقار ، فإن المجني عليه هو المتصرف إليه الذي يسلم المال للجاني، وتقوم وسيلة الاحتيال في هذه الحالة دون أي شبهة.

أما إذا كان محل التصرف معيناً بالذات، كسيارة أو دابة محددة بأوصافها، فإن جريمة الاحتيال تقوم بتمكين الجاني من الاستيلاء على مال المجني عليه، فمن يشاهد سيارة ويتوجه إلى الجاني، معتقداً أنه مالكها يبغي شراءها منه، فيبدي هذا الأخير استعداده لبيعها له مؤكداً أنها ملكه ويتفق معه على تسليمها إليه بعد تحرير عقد البيع وقبض الثمن ،فإن تم هذا واختفى الجانى قبل التسليم ، عند مرتكبا لجريمة النصب .[2]

[1] حسن صادق المرصفاوي – المرصفاوي في أصول الإجراءات الجنائية – منشأة المعارف – الإسكندرية – ١٩٩٦م.

[2] د. محمد الأمين البشري – الأدلة الجنائية الرقمية – مفهومها ودورها فـــى الإثبات – المجلة العربية للدراسات الأمنية والتدريب – المجلد ١٧-- العدد ٣٣– السنة ١٧ – الرياض – أبريل ٢٠٠٢م.

وعليه فكون المال غير مملوك للجانى، أو ليس له حق التصرف فيه ، أو تصرف فيه مع علمه بسبق تصرفه فيه ، فإن كان مملوكا له ، أو له حق التصرف فيه فلا جريمة، فالوكيل الذى يقوم بالتصرف فى مال مملوك لموكله بناء على عقد وكالة يفوضه فيه بالبيع ، لا يرتكب جريمة نصب، حتى ولو ظهر بعد ذلك أن الوكالة كانت قد انتهت أو انقضت ولم يكن الوكيل قد علم بذلك. [1]

ويشترط أن يكون موضوع جريمة الاحتيال أو النصب مالاً منقولاً أو عقاراً مملوكاً لغير الجاني، وليس له حق في التصرف فيه أو تصرف منه منه مع علمه بسبق تصرفه فيه.

ولا أهمية بقيمة المال – عقاراً كان أو منقولاً – في قيام جريمة الاحتيال، كذلك لا عبرة بكون المال له قيمة مادية أو مجرد قيمة أدبية كالخطابات والمذكرات الخاصة، ويستوي في المال موضوع الجريمة أن تكون حيازة المجني عليه له مشروعة أو غير مشروعة، كمن يتوصل بالاحتيال إلى الاستيلاء على مواد مخدرة من آخر يُعد مرتكباً لجريمة النصب، وكذلك من يستولي على سلاح غير مرخص بحيازته.

وعليه **يشير الباحث** إلى أن الاستيلاء على المنفعة فقط بإحدى وسائل الاحتيال لا يكفي لقيام محل جريمة النصب ؛ كمن يتوصل بالحيلة إلى الركوب

[1] د.رضا عبد الحكيم إسماعيل – الوقاية من الجرائم الناشئة عن استعمال الحاسوب – مجلة الاقتصاد الإسلامي – العدد ٢١٨ – السنة ١٩ – أغسطس١٩٩٩م.

في وسائل المواصلات العامة بغير أجر تحت الزعم أنه من رجال الشرطة مثلاً.

وجريمة الاحتيال أو النصب جريمة عمدية، تتطلب توفر القصد الجنائي العام والقصد الخاص، فالقصد الجنائي العام فيها بعلم الجاني يتمثل في الأفعال التي يأتيها، ويعتبرها القانون وسائل احتيال، ومن شأنها خداع المجني عليه وحمله على التسليم، أما القصد الخاص فيتمثل فى انصراف نية الجاني إلى الاستيلاء على الحيازة الكاملة.[1]

1- حماية أموال التجارة الإلكترونية من خلال القواعد العامة لجريمة النصب:

هناك ثلاثة آراء مختلفة اتجهت نحو حماية التجارة الالكترونية من خلال القواعد العامة لجريمة النصب والاحتيال، وهذه الآراء هي:

الرأي الأول: يرى أن جريمة النصب لا تقوم إلا إذا خدع شخصاً مثله، وأن يكون الشخص المخدوع مكلفاً بمراقبة البيانات، وعلى ذلك لا يتصور خداع الحاسب الآلي بوصفه آلة، ومن ثم لا يطبق النص الجنائي الخاص بالنصب والاحتيال، لافتقاده أحد العناصر اللازمة لتطبيقه ، وهذا الاتجاه تبنته التشريعات المصرية والألمانية واليابان والسويد وايطاليا .[2]

[1] د. أحمد السمدان – النظام القانوني لحماية برامج الكمبيوتر – مجلة الحقوق العدد٤ – السنة ١١ – جامعة الكويت – الكويت – ديسمبر – ١٩٨٧م.

[2] يزيد بو حليط، تفتيش المنظومة المعلوماتية وحجز المعطيات في التشريع الجزائري، مجلة التواصل في الاقتصاد والإدارة والقانون، العدد 48، ديسمبر 2016

الرأي الثاني : تبنته دول الأنجلوساكسون، منها بريطانيا واستراليا وكندا، وهذا الاتجاه يوسع من النصوص بالعقاب على جريمة النصب المعلوماتي؛ حيث تدخل المشرع الإنجليزي في العام 1982م، واعتبر خداع الآلة بنية ارتكاب غش مالي هو من قبيل الاحتيال الذي يجب العقاب عليه جنائياً.[1]

الرأي الثالث: وتبنته الولايات المتحدة الأمريكية؛ حيث تطبق النصوص المتعلقة بالغش في مجال البنوك والبريد والتلغراف بغرض الغش على حالات النصب المعلوماتي، كما نرى المشرع الإماراتي في المادة (2) من العقوبات المنصوص عليها في القانون الاتحادي لعام 2006 في شأن مكافحة جرائم تقنية المعلومات قد عاقب على كل فعل عمومي يتوصل فيه بغير وجه حق إلى موقع أو نظام معلوماتي، سواءً بدخول الموقع أو النظام، أو يتجاوز مدخلاً مصرحاً به يعاقب بالحبس وبالغرامة.[2]

[1] د. هلالي عبد اللاه أحمد – التزام الشاهد بالإعلام في الجرائم المعلوماتية – دراسة مقارنة – النسر الذهبي – القاهرة – ٢٠٠٠م.

[2] د. محمد الأمين البشرى– العدالة الجنائية ومنع الجريمة – دراسة مقارنة – ط١– أكاديمية نايف العربية للعلوم الأمنية – الرياض – ١٩٩٧م.

2- الحماية التشريعية لجرائم تقنية المعلومات في دولة الإمارات العربية المتحدة:

هناك العديد من الأسباب التي دعت المشرع الإماراتي إلى سن تشريعات خاصة بجرائم تقنية المعلومات في دولة الإمارات العربية المتحدة، وهذه الأسباب هي:

أ- التوسع في استخدام الانترنت :

على الرغم من حداثة تقديم خدمة الانترنت في دولة الإمارات العربية المتحدة، إلا أن عدد مستخدمي الشبكة وصل إلى أرقام خيالية، ولهذا فإن دولة الإمارات العربية المتحدة تحتل المركز الثاني عربياً، والثامن عشر عالمياً منذ سنة 2000م.[1]

ب – التجارة الإلكترونية

والحديث عن التجارة الإلكترونية في دولة الإمارات العربية المتحدة ذو أهمية بالغة؛ فبالرغم من القفزات الهائلة في هذا المجال، فقد كان للمشرع

[1] د. محمد عبد المحسن المقاطع – حماية الحياة الخاصة للأفراد وضماناتها في مواجهة الحاسوب الآلي – دراسة تحليلية نقدية مقارنة للحق في الخصوصية وتطبيقاته في القانون الكويتي – مطبوعات جامعة الكويت – الكويت- ١٩٩٢م.

الإماراتي دور فعال تجاه هذا التطور السريع، الأمر الذي دفع به بمجاراة هذا التطور بإصدار التشريعات المناسبة التي تحمي هذه التجارة الإلكترونية .[1]

ج – الحكومة الالكترونية

لما لهذا الموضوع من أهمية بالغة، حيث إن جميع القطاعات الحكومية في معظم إمارات الدولة، وخاصة إمارة دبي، قد تحولت إلى النظام الإلكتروني، والمقصود بالنظام الإلكتروني تقديم الخدمات والقيام بالأعمال آلياً، هذا ما هو واقع فعلاً؛ حيث نرى التنافس بين هذه القطاعات لتحقيق السبق في التحول للنظام الآلي من خلال مواقعها على الشبكة، وبالتالي كان لابد من حماية هذه المواقع الحكومية من أي اعتداءات أياً كانت صورة هذا الاعتداء، وهذا ما قرره قانون العقوبات.[2]

الاتحادي الجديد بشأن الجرائم المعلوماتية الصادر عام 2000م ، وكذلك المرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات في دولة الإمارات العربية المتحدة.[3]

[1] د.مصطفى محمد موسى الجهاز الإلكتروني لمكافحة الجريمة – ط١ – الكتاب الأول – سلسلة اللواء الأمنية – القاهرة – ٢٠٠١م.

[2] هـــ.كيت الخصوصية في عصر المعلومات – ترجمة محمد محمود شهاب – ط١– مؤسسة الأهرام – القاهرة – ١٩٩٩م.

[3] يزيد بو حليط، تفتيش المنظومة المعلوماتية وحجز المعطيات في التشريع الجزائري، مجلة التواصل في الاقتصاد والإدارة والقانون، العدد 48، ديسمبر 2016

خامسا: جرائم قرصنة برامج الحاسب الآلى

جرائم قرصنة برامج الحاسب الآلي هي الجرائم الماسة بحقوق الملكية الفكرية لبرامج الحاسوب ونظمه، والتي تشمل نسخ وتقليد البرامج وإعادة إنتاجها وصنعها دون ترخيص، والاعتداء على العلامة التجارية وبراءة الاختراع .[1]

وبإمعان النظر في هذه الطوائف، نجد أن الحدود بينها ليست قاطعة ومانعة، فالتداخل حاصل ومتحقق، إذ إن الاعتداء على معطيات الحاسوب بالنظر لقيمتها الذاتية أو ما تمثله، هو في ذات الوقت اعتداء على أمن المعطيات، لكن الغرض المباشر المحرك للاعتداء انصب على قيمتها أو ما تمثله والاعتداء على حقوق الملكية الفكرية لبرامج الحاسوب، هو اعتداء على الحقوق المالية واعتداء على الحقوق الأدبية (الاعتبار الأدبي)، لكنها تتميز عن الطوائف الأخرى بأن محلها هو البرامج فقط، وجرائمها تستهدف الاستخدام غير المحق أو التملك غير المشروع لهذه البرامج .

هذا من جهة، ومن جهة أخرى، نجد أن الحماية الجنائية للمعلومات في نطاق القانون المقارن وفي إطار الجهود الدولية لحماية معطيات الحاسوب واستخدامه، اعتمدت على نحو غالب، التقسيم المتقدم ؛ فظهرت حماية حقوق الملكية الأدبية للبرامج، وحماية البيانات الشخصية المتصلة بالحياة الخاصة،

[1] مبدر الويس – أثر التطور التكنولوجي على الحريات العامة – منشأة المعارف – الإسكندرية – (د.ت).

وحماية المعطيات بالنظر لقيمتها أو ما تمثله، والذي عرف بحماية (الأموال)، كل في ميدان وموقع مستقل . وهو في الحقيقة تمييز – ليس مطلقاً – بين حماية قيمة المعطيات، وأمنها ، وحقوق الملكية الفكرية. ولا بد لنا من الإشارة إلى أن حماية أمن المعطيات (الطائفة الثانية)[1]

انحصر في حماية البيانات الشخصية المتصلة بالحياة الخاصة، أما حماية البيانات والمعلومات السرية والمحمية، فقد تم تناوله في نطاق جرائم الطائفة الأولى الماسة بقيمة المعطيات، بالنظر إلى أن الباعث الرئيسي للاعتداء . والغرض من معرفة أو إفشاء هذه المعلومات غالباً ما كان الحصول على المال ؛ مما يُعد من الاعتداءات التي تندرج تحت نطاق الجرائم الماسة بقيمة المعطيات التي تتطلب توفير الحماية الجنائية للحقوق المتصلة بالذمة المالية التي تستهدفها هذه الجرائم.[2]

وحول أبرز الأحداث والوقائع الجرمية خلال السنوات الخمس الماضية، وبالاستناد إلى المواد الإخبارية الصحفية وبعض معلومات الدراسة المتقدمة، فقد تعرضت شركة اتصالات الإمارات إلى أنشطة اعتداء أُحيل مرتكبها إلى القضاء .

---

[1] المحامي صبحي المحمصاني – الأوضاع التشريعية في الدول العربية ماضيها وحاضرها ط٣ – دار العلم للملايين – بيروت – ١٩٦٥م.

[2] جورج الخوام – الحواسيب اليوم – ط ١ – منشورات الأمم المتحدة لإغاثة وتشغيل اللاجئين – فينا – ١٩٩٢م.

سادسا: جرائم التجسس والتنصت على البيانات والمعلومات:

إن جرائم التجسس والتنصت على البيانات والمعلومات وجرائم الأسرار التجارية المرتبطة بالكمبيوتر لم يجر النص عليها صراحة، وهو ما يرجع إلى أن بقية النصوص، وتحديداً الطائفة الأولى المتعلقة بالجرائم التي تستهدف سرية وسلامة وتوفر المعلومات، تغطي أنشطة التجسس باعتبارها دخولاً غير مصرح به إلى النظم وكشف للمعلومات المخزنة فيها وإفشاء لها.[1]

وأما عن نصوص المسائل الإجرائية، فإنها تتخذ أهمية قصوى، ذلك أن التدابير التشريعية الإجرائية لم تكن بمستوى التدابير التشريعية الموضوعية، وهي غائبة للآن في الجزء الأكبر من دول الاتحاد الأوروبي، فيما يتعلق بالقواعد الإجرائية الخاصة بجرائم الكمبيوتر والانترنت، وتمثل أحكام اتفاقية بودابست 2001م في هذا الحقل قواعد عامة وتوجيهات عريضة تتطلب تحديداً منضبطاً من المؤسسات التشريعية لدى وضع القوانين الوطنية في هذا الحقل؛ فالاتفاقية أرادت أن تؤكد على حقيقة أن جرائم الكمبيوتر والانترنت تنطوي على خصوصية في ميدان الإثبات والتحري والضبط والتفتيش والمقاضاة والاختصاص، ولهذا سعت لتقديم معايير لضبط هذه العناصر من أجل انسجام الحلول الإجرائية، لكنها منحت هامشاً للدول الأعضاء لاتخاذ تدابير مختلفة، أو على الأقل حلولاً بديلة، أو أخرى غير ما تضمنته وفي نطاق التعاون الدولي

[1] د. محمد الأمين البشرى– العدالة الجنائية ومنع الجريمة – دراسة مقارنة – ط١– أكاديمية نايف العربية للعلوم الأمنية – الرياض – ١٩٩٧م.

لمكافحة جرائم الكمبيوتر جاءت الاتفاقية بأحكام أكثر تفصيلاً، باعتبار الاتفاقية نفسها هي الأداة التشريعية الرئيسية التي ستحكم مسائل التعاون الدولي في أنشطة المكافحة ونكتفي بالقول في هذا المقام إن أبرز ما تنطوي عليه مسائل التعاون الدولي يتمثل بالقواعد المتعلقة بتسليم المجرمين والإنابات القضائية ومسائل الضبط والتفتيش وتحريز الأدلة خارج الحدود .[1]

ولقد كانت الأحكام التي تضمنتها الاتفاقية في هذا الميدان الأكثر إثارة للجدل، والتي واجهت اعتراضات عريضة من جهات عدة، ونحن بدورنا – وبالرغم من أننا من أشد المتمسكين بمقتضيات السيادة الوطنية – إلا أننا نجد جرائم الكمبيوتر تحديداً مما لا يمكن مواجهته دون قواعد مخصوصة تنظم المسائل الحساسة والهامة ، بل لعلها القواعد التي ستحمي السيادة الوطنية باعتبارها تنطبق على كافة دول الأعضاء ضمن المعايير الموضوعية المقررة في الاتفاقية، وبشكل قد يحول دون تدخلات لصالح طرف دون آخر في ظل اختلال موازين القوى .

سابعاً: جريمة إتلاف وتدمير المعطيات:

أدرك المشرع الإماراتي مدى خطورة إتلاف وتدمير المعطيات الإلكترونية، فنص في المادة الثانية من المرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات على أنه: "يعاقب بالحبس

[1] د. أسامة عبد الله قايد – الحماية الجنائية للحياة الخاصة وبنوك المعلومات – دراسة مقارنة – ط ٢ – دار النهضة العربية – القاهرة – ١٩٨٩م.

والغرامة التي لا تقل عن مائة ألف درهم ولا تزيد على ثلاثمائة ألف درهم أو بإحدى هاتين العقوبتين كل من دخل موقعاً إلكترونياً أو نظاماً معلوماتياً إلكترونياً أو شبكة معلومات، أو وسيلة تقنية معلومات، بدون تصريح أو بتجاوز حدود التصريح، أو بالبقاء فيه بصورة غير مشروعة.[1]

تكون العقوبة الحبس مدة لا تقل عن ستة أشهر والغرامة التي لا تقل عن مائة وخمسين ألف درهم ولا تجاوز سبعمائة وخمسين ألف درهم أو بإحدى هاتين العقوبتين إذا ترتب على أي فعل من الأفعال النصوص عليها بالفقرة (1) من هذه المادة إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أي بيانات أو معلومات. وتكون العقوبة الحبس مدة لا تقل عن سنة واحدة والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز مليون درهم أو بإحدى هاتين العقوبتين إذا كانت البيانات أو المعلومات محل الأفعال الواردة في الفقرة (2) من هذه المادة شخصية".[2]

ثامنا الجرائم التقليدية السب والقذف والتشهيـــر:

نص المشرع الاتحادي في المادة (35) من المرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات بدولة الإمارات العربية المتحدة على أنه: "مع عدم الإخلال بالأحكام المقررة في الشريعة

---

[1] أحمد فتحي سرور – الوسيط في قانون الإجراءات الجنائية – ط – دار النهضة العربية – القاهرة –ط ١٩٨٥م– و ١٩٩٣م.

[2] د. أحمد حسام طه تمام – الجرائم الناشئة عن استخدام الحاسب الآلى ــ (الحماية الجنائية للحاسب الآلي – دراسة مقارنة – دار النهضة العربية – القاهرة – ٢٠٠٠م.

الإسلامية، يعاقب بالحبس والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز مليون درهم أو بإحدى هاتين العقوبتين كل من ارتكب عن طريق الشبكة المعلوماتية أو وسيلة تقنية معلومات أو على موقع إلكتروني، إحدى الجرائم التالية:[1]

-الإساءة إلى أحد المقدسات أو الشعائر الإسلامية.

-الإساءة إلى أحد المقدسات أو الشعائر المقررة في الأديان الأخرى متى كانت هذه المقدسات والشعائر مصونة وفقاً لأحكام الشريعة الإسلامية.

- سب أحد الأديان السماوية المعترف بها.

-تحسين المعاصي أو الحض عليها أو الترويج لها.

-واذا تضمنت الجريمة إساءة للذات الإلهية أو لذات الرسل والأنبياء أو كانت مناهضة للدين الإسلامي أو جرحاً للأسس والمبادئ التي يقوم عليها ، أو ناهض أو جرح ما علم من شعائر وأحكام الدين الإسلامي بالضرورة، أو نال من الدين الإسلامي، أو بشر بغيره أو دعا إلى مذهب أو فكرة تنطوي على شيء مما تقدم أو حبذ لذلك أو روج له، فيعاقب بالسجن مدة لا تزيد على سبع (7) سنوات .[2]

---

[1] جورج الخوام – الحواسيب اليوم – ط ١ – منشورات الأمم المتحدة لإغاثة وتشغيل اللاجئين – فينا – ١٩٩٢م.

[2] د.جميل عبد الباقي الصغير – الجوانب الإجرائية المتعلقة بالإنترنت – دار النهضة العربية – القاهرة – ٢٠٠١م.

التفتيش الجنائي على نظم الحاسوب والانترنت

في التشريع المصري والتشريع السعودي

يعد التفتيش من بين الإجراءات الجنائية الأكثر خطورة وتأثيراً على حرية الأفراد، حيث يتعارض مباشرة مع حقوقهم في الخصوصية وحماية سريتهم الشخصية. يمثل التفتيش تقييداً للحرية واستخداماً للسلطة، وهما عناصر من صفات السلطة الاحتياطية، مثل الاعتقال والتوقيف، بالإضافة إلى جمع الأدلة. يعتبر التفتيش إجراءً جنائيًا يتضمن انتهاكًا لحق الإنسان في الاحتفاظ بأسراره وحماية منزله وحياته الشخصية، وتنظمه القوانين لتحقيق مصلحة المجتمع في الوصول إلى أدلة الجريمة وكشف الحقيقة.

ومن هنا، تبرز أهمية موضوع التفتيش الجنائي على أنظمة الحاسوب والإنترنت، والذي يُعَدّ موضوعاً جديداً تماماً في الأردن وجزئيًا في العالم العربي. في الأيام الأخيرة، بدأت الأجهزة الأمنية تواجه عدداً من جرائم الحاسوب والإنترنت. لذا، يتطلب ذلك وجود تعريف للتفتيش والضبط على أنظمة الحاسوب والإنترنت، وتوافقها مع الإجراءات التقليدية المقارنة، وتنسيقها مع المكونات المادية والمعنوية للحاسوب وشبكة الإنترنت. كما يتطلب أيضاً وضع مقترحات لنصوص قانونية تنظم استفادة المتخصصين في هذا المجال العلمي والتقني .[1]

[1] نعيم مغبغب – مخاطر المعلوماتية والإنترنت – المخاطر على الحياة الخاصة وحمايتها – دراسة في القانون المقارن – بيروت – ١٩٩٨م.

وتم وضع التعريفات المفاهيمية للحريات والحقوق الفردية تاريخياً لمواجهة تعدي الدولة على حقوق المواطنين وحرياتهم .وبالتالي ، ظهر مفهوم حق المواطنين في التمتع بحقوق غير قابلة للتقييد بعد معركة طويلة للحد من سلطات الدولة غير المحدودة[1].

المساحة الشخصية ، التي تحدها جدران منزل كل شخص وتمتد بشكل خاص إلى تواصله الشخصي مع الآخرين ، كانت محور مختلف التشريعات والقوانين التي سعت إلى حماية المواطنين من أي تدخل في حياتهم الشخصية .تخضع هذه القوانين للتعديل طوال الوقت ؛ بسبب الاختراق الهائل الذي شهدته تقنيات تخزين البيانات الشخصية .ويصاحب هذا التطور دائماً مخاطر أكبر تتمثل في تعريض مثل هذه البيانات والاتصالات للانتهاك من قبل جهات خارجية وعلى رأسها سلطات الدولة[2].

في ظل التطور الجوهري لوسائل الاتصال الإلكترونية وخاصة الإنترنت وتطبيقاته المختلفة التي لم تعد تقتصر على أجهزة الكمبيوتر الشخصية ، بل توسعت لتشمل الهواتف الذكية ، مما يتيح لنا حفظ أو تخزين معظم بياناتنا إلكترونياً وتبادلها معها الأشخاص والوجهات المختلفة طوال الوقت باستخدام اتصال الشبكة ، أصبح من الضروري حماية خصوصيتنا من أجل الحفاظ

[1] نديم محمد حسن الترزي، سلطات النيابة العامة في الجرائم المعلوماتية، مجلة أندلس للعلوم الاجتماعية والإنسانية، العدد 19، مجلد 15، أبريل 2017

[2] ياكوف ميخايلو فيتش بيلسون – الإنتربول في الصراع ضد الجريمة الجنائية – ترجمة وإعداد : عماد محمود طحينة ومازن محمد نفاع – دار معد للنشر والتوزيع – دمشق – ١٩٩١م.

على هذا القدر من البيانات والاتصالات التي قد تُستخدم لإلحاق الأذى بنا بطريقة أو بأخرى .من ناحية أخرى ، قد تلجأ هيئات الدولة ، في ظل ظروف معينة ، إلى الوصول إلى البيانات الشخصية والمراسلات لجمع الأدلة التي من شأنها أن تساعد في إدانة مرتكبي الجرائم المختلفة أو في الكشف عن خطط لأعمال إجرامية تستهدف الأمن القومي ، وخاصة الجرائم الإرهابية[1] .

الإطار القانوني والدستوري:

ينص الإعلان العالمي لحقوق الإنسان على أن "لكل فرد الحق في الحياة والحرية وسلامة شخصه ، ولا يجوز تعريض أي شخص لتدخل تعسفي في خصوصيته أو أسرته أو منزله أو مراسلاته ."كما تنص على أن "لكل فرد الحق في حماية القانون من مثل هذا التدخل أو الهجمات" ، مع الاعتراف بالحق في نظام اجتماعي ودولي يمكن من خلاله إعمال الحقوق والحريات المنصوص عليها في هذا الإعلان إعمالاً كاملاً[2].

بالإضافة إلى ذلك ، فإن العهد الدولي الخاص بالحقوق المدنية والسياسية ، الذي دخل حيز التنفيذ في مصر منذ عام 1981 ، يؤكد – في المادة 17 منه

[1] د.مصطفى محمد موسى الجهاز الإلكتروني لمكافحة الجريمة – ط١ – الكتاب الأول – سلسلة اللواء الأمنية – القاهرة – ٢٠٠١م.

[2] د. محمود شريف بسيوني ود. عبد العظيم الوزير – الإجراءات الجنائية في النظم القانونية العربية وحماية حقوق الإنسان – ط ١ – دار العلم للملايين – بيروت – ١٩٩١م.

– عدم جواز التدخل في حياة الفرد الخاصة ولا في شؤون أسرته ومنزله ومراسلاته[1].

تنص المادة (17) من العهد الدولي الخاص بالحقوق المدنية والسياسية على ما يلي:

1. لا يجوز تعريض أي شخص لتدخل تعسفي أو غير قانوني في حياته الخاصة أو أسرته أو منزله أو مراسلاته ، ولا لأي هجمات غير قانونية على شرفه وسمعته.

2. لكل فرد الحق في حماية القانون من مثل هذا التدخل أو الهجمات.

كما نص الدستور المصري على حرمة الحياة الخاصة والمراسلات البريدية والبرقية والإلكترونية والمكالمات الهاتفية وغيرها من وسائل الاتصال ، ويحظر مصادرتها أو كشفها أو مراقبتها إلا بحكم قضائي مسبب ولمدة محددة. وفي الحالات التي يحددها القانون (المادتان 57 و 58).

كما نص الدستور على أن لكل شخص الحق في حياة آمنة وأن على الدولة توفير الأمن والطمأنينة للمواطنين وجميع المقيمين على أراضيها[2].

قانون رقم 175 والخصوصية

---

[1] د.محمد فهمي طلبة وآخرون – دائرة المعارف الحاسب الإلكتروني – مجموعة كتب دلتا – مطابع المكتب المصري الحديث – القاهرة – ١٩٩١م.

[2] ياكوف ميخايلو فيتش بيلسون – الإنتربول في الصراع ضد الجريمة الجنائية – ترجمة وإعداد : عماد محمود طحينة ومازن محمد نفاع – دار معد للنشر والتوزيع – دمشق – ١٩٩١م.

أولاً: تعريض خصوصية المواطنين بشكل عام للخطر

تلزم المادة (2) من القانون رقم 2018/175 بشأن مكافحة جرائم الإنترنت وجرائم تكنولوجيا المعلومات "مقدمي الخدمة" ، أي شركات الاتصالات / الإنترنت ، بما يلي:

-1الاحتفاظ ببيانات نظام المعلومات أو أي وسيلة أخرى من وسائل تقنية المعلومات وتخزينها لمدة تقصير 180 يوماً .تتضمن هذه البيانات ما يلي:

1. المعرفات الشخصية (المعلومات التي تحدد مستخدم الخدمة)
2. البيانات الوصفية (البيانات المتعلقة بمحتوى نظام المعلومات)
3. البيانات المتعلقة بحركة الاتصالات.
4. البيانات المتعلقة بأجهزة الاتصالات الطرفية.
5. أي بيانات أخرى تحددها السلطة المختصة

تنتهك هذه المادة حق المواطنين في الخصوصية للأسباب التالية:

1. يلتزم مقدمو الخدمات بالاحتفاظ بالبيانات التي قد تتجاوز ما يحتاجون إليه وتخزينها من أجل إكمال عملهم بكفاءة ، مع ملاحظة أن هذه

البيانات ليست مرتبطة بشركات الاتصالات أو الإنترنت ولا مملوكة لها على الإطلاق ؛ بل هي مملوكة بالكامل لمستخدمي الخدمة[1].

2. يلتزم مقدمو الخدمة بالاحتفاظ بهذه البيانات لفترة طويلة من الزمن ، وكلما طالت هذه الفترة ، زادت تعرض هذه البيانات للتدخل والقرصنة والوصول غير القانوني أو التجاري ، مما قد يؤدي إلى انتهاك خصوصية المواطنين بشكل ما مما يجعل من الصعب تحديد المخالف ؛ سواء كان ضمن نظام معلومات مقدم الخدمة أو خارجه[2].

3. تمنح هذه المادة السلطات الإدارية أو غير التشريعية أو القضائية الحق في تحديد أنواع إضافية من البيانات التي تعتبر غير معروفة وغير محددة وغير محدودة من خلال إلزام مقدمي الخدمة بالاحتفاظ بها وتخزينها .يشكل هذا انتهاكًا جسيماً لحق مستخدم الخدمة في الحصول على المعلومات عندما يكون لمزود الخدمة الحق في الاحتفاظ بالبيانات وتخزينها مسبقًا وبالتفصيل[3].

---

[1] د. هلالي عبد اللاه أحمد – حقوق الدفاع في مرحلة ما قبل المحاكمة بين النمط المثالي والنمط الواقعي – (في فرنسا ومصر والمملكة العربية السعودية) – دار النهضة العربية – القاهرة – ١٩٩٥م.

[2] هشام محمد فريد رستم – الجوانب الإجرائية للجرائم المعلوماتية – دراسة مقارنة – مكتبة الآلات الحديثة – أسيوط – ١٩٩٤م.

[3] نديم محمد حسن الترزي، سلطات النيابة العامة في الجرائم المعلوماتية، مجلة أندلس للعلوم الاجتماعية والإنسانية، العدد 19، مجلد 15، أبريل 2017

ثانياً: الصلاحيات الممنوحة لأجهزة الأمن الوطني

على الرغم من أن القانون يلزم شركات الاتصالات والإنترنت (مزودي الخدمة) بالحفاظ على خصوصية وسرية البيانات المخزنة من خلال إجبارهم على عدم الكشف عنها إلا بموجب أمر قضائي مسبب ، إلا أن قانون الجرائم الإلكترونية يمنح وكالات "الأمن القومي" – والتي تعرفها على أنها: رئاسة الجمهورية ، ووزارة الدفاع ، ووزارة الداخلية ، وجهاز المخابرات العامة ، وهيئة الرقابة الإدارية – الحق في الاستفادة من هذا الأمر القضائي المسبب على النحو التالي[1]:

-للجهات المختصة الوصول إلى المعلومات أو البيانات أو نظم المعلومات أو مصادرتها أو إرفاقها أو تتبعها في أي وسيط أو برنامج إلكتروني أو حاسوب.

-يمكنهم البحث والوصول إلى قواعد بيانات برامج الحاسب وأنظمة المعلومات الأخرى كجزء من الصلاحيات الممنوحة لهم لتحقيق هدفهم.

-يجوز للسلطات أن تأمر مزودي الخدمة بتسليم أي معلومات تتعلق بأنشطة المستخدمين أو بنظام معلومات أو جهاز تقني يكون تحت سيطرته ، وكذلك بيانات مستخدمي خدمته وحركة الاتصالات التي تمت. على هذا النظام أو الجهاز الفني[2].

---

[1] يزيد بو حليط، تفتيش المنظومة المعلوماتية وحجز المعطيات في التشريع الجزائري، مجلة التواصل في الاقتصاد والإدارة والقانون، العدد 48، ديسمبر 2016

[2] أسامة بن غانم العبيدي. نديم محمد حسن الترزي، سلطات النيابة العامة في الجرائم المعلوماتية، مجلة أندلس للعلوم الاجتماعية والإنسانية، العدد 19، مجلد 15، أبريل 2017

المواد المذكورة أعلاه معيبة بشكل أساسي للأسباب التالية:

1. التناقض: تتطلب بعض المواد أمراً قضائياً للوصول إلى البيانات ، بينما تمنح مواد أخرى سلطة تقديرية لهيئة تحقيق غير محددة ، وتعطي مواد أخرى صلاحيات لـــ "أجهزة الأمن القومي" نفسها دون أي متطلبات (سواء الحصول على أمر قضائي أو هيئة تحقيق)[1].

2. لا يحدد القانون أي لوائح فيما يتعلق بالأسباب أو الظروف التي يمكن بموجبها إصدار أمر قضائي للوصول إلى بيانات المستخدم .كما أنه لا يحدد نوع البيانات التي قد يغطيها الأمر القضائي[2].

3. يمنح القانون للمجهول الحق في الطعن في الأمر القضائي ، دون الحاجة إلى إخطار صاحب العلاقة (مستخدم الخدمة) بالموضوع .كما أنه لا يحدد فترة زمنية لتقديم استئناف قبل تنفيذ القرار فعلياً .كما لم ينص القانون على أي وسيلة للتعويض في حال كانت أسباب طلب

[1] د. هلالي عبد اللاه أحمد – حقوق الدفاع في مرحلة ما قبل المحاكمة بين النمط المثالي والنمط الواقعي – (في فرنسا ومصر والمملكة العربية السعودية) – دار النهضة العربية – القاهرة – ١٩٩٥م.

[2] هشام محمد فريد رستم – الجوانب الإجرائية للجرائم المعلوماتية – دراسة مقارنة – مكتبة الآلات الحديثة – أسيوط – ١٩٩٤م.

الوصول إلى البيانات غير كافية أو غير صحيحة مما يتسبب في إلحاق الضرر بمالك البيانات أو تعريض سلامته للخطر[1].

4. أخطر نقطة هي أن المواد المذكورة أعلاه من القانون تسمح لأجهزة الأمن القومي بالوصول إلى جميع بيانات نظام المعلومات ولا تقصر الأمر على مستخدمين معينين قد يتعلق بهم أمر المحكمة (عندما يكون ذلك مطلوباً للحصول على أمر قضائي) ، مما يجعل الوصول إلى بيانات جميع مستخدمي نظام المعلومات متاحاً دون أي مبرر أو لوائح قانونية[2].

ثالثاً: تخويف مقدمي الخدمة

يُحمل القانون مقدمي الخدمة المسؤولية الجنائية في الحالات التالية: عندما يمتنع أي منهم عن تسليم بياناته أو معلوماته ، أو السماح لأجهزة الأمن الوطني بمصادرة أو إرفاق أو تتبع المعلومات أو البيانات أو أنظمة المعلومات بأي وسيلة أو برنامج إلكتروني أو كمبيوتر ، أو البحث والوصول إلى قواعد بيانات برامج الكمبيوتر وأنظمة المعلومات الأخرى.وبالتالي يعاقب مقدمو

[1] هشام محمد فريد رستم – الجوانب الإجرائية للجرائم المعلوماتية – دراسة مقارنة – مكتبة الآلات الحديثة – أسيوط – ١٩٩٤م.

[2] أسامة بن غانم العبيدي. نديم محمد حسن الترزي، سلطات النيابة العامة في الجرائم المعلوماتية، مجلة أندلس للعلوم الاجتماعية والإنسانية، العدد 19، مجلد 15، أبريل 2017

الخدمة بالسجن مدة لا تقل عن ستة أشهر وغرامة لا تقل عن 20.000 جنيه ولا تزيد عن 100.000 جنيه أو بإحدى هاتين العقوبتين[1].

النظام القانوني في مصر:

في السياق المصري، يتم استعراض التشريعات والقوانين ذات الصلة بالتفتيش الجنائي على نظم الحاسوب والإنترنت، ويتم اعتبارها كإطار قانوني للتعامل مع هذه القضية. بعض القوانين المهمة التي يمكن ذكرها على سبيل المثال لا الحصر هي:

1. **قانون العقوبات المصري رقم 58 لسنة 1937:** يحدد الجرائم المرتبطة بالتكنولوجيا الحاسوبية والإنترنت والعقوبات المناسبة لها. يحدد هذا القانون الجرائم والعقوبات المنصوص عليها في حالة ارتكاب جرائم على نظم الحاسوب والإنترنت. يتضمن القانون تصنيفات للجرائم الإلكترونية ويحدد العقوبات المناسبة لكل تصنيف [2]
2. **قانون الإجراءات الجنائية المصري رقم 150 لسنة 1950:** ينظم إجراءات التحقيق في جرائم تتعلق بنظم الحاسوب والإنترنت وصلاحيات الجهات المختصة في جمع الأدلة الرقمية يحدد هذا القانون إجراءات التحقيق الجنائي بشكل عام، بما في ذلك التحقيق في

[1] عربوز فاطمة الزهراء، التفتيش الالكتروني كإجراء للتحقيق في الجرائم المعلوماتية، مجلة جيل الأبحاث القانونية المعمقة، العدد 34

[2] أحمد أسامة حسنية، التفتيش في الجرائم الإلكترونية في التشريع الفلسطيني، دراسة تحليلية مقارنة بالتشريع العُماني، 2016

جرائم تتعلق بنظم الحاسوب والإنترنت. ينص القانون على صلاحيات الجهات المختصة في جمع الأدلة الرقمية واستخدامها في إثبات الجرائم[1]

3. **قانون حماية المعلومات الشخصية في مصر رقم 151 لسنة 2020:** يحمي خصوصية البيانات الشخصية وينظم جمعها ومعالجتها واستخدامها في الأنظمة الحاسوبية والإلكترونية، ويوفر آليات للإبلاغ عن انتهاكات الخصوصية قانون حماية المعلومات الشخصية في مصر: يهدف هذا القانون إلى حماية البيانات الشخصية للأفراد وضمان سرية وخصوصية هذه المعلومات عند جمعها ومعالجتها واستخدامها في سياق الأنظمة الحاسوبية والإلكترونية.[2]

يتضمن القانون إجراءات للتحقق من سلامة النظم الإلكترونية وتوفير آليات للإبلاغ عن انتهاكات الخصوصية .تلك القوانين هي أمثلة على التشريعات المصرية ذات الصلة بالتفتيش الجنائي على نظم الحاسوب والإنترنت. يعتبر

[1] د.فاضل نصر الله عوض – ضمانات المتهم أمام سلطة التحقيق الابتدائي في التشريع الكويتي – دراسة مقارنة بالتشريعيين المصري والفرنسي – مجلة الحقوق – الكويت – ١٩٩٨م.

[2] كامل السعيد – جرائم الكمبيوتر والجرائم الأخرى في مجال التكنولوجيا – بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي – القاهرة – في ٢٥–٢٨/ اكتوبر / ١٩٩٣م.

دراسة وفهم هذه القوانين أساسيًا لضمان التطبيق الصحيح للاجراءات القانونية.[1]

النظام القانوني في السعودية:

في المملكة العربية السعودية، يتم استعراض التشريعات والقوانين ذات الصلة بالتفتيش الجنائي على نظم الحاسوب والإنترنت. يتم اعتبار هذه القوانين كإطار قانوني للتعامل مع هذه القضية. بعض القوانين المهمة ذات الصلة يمكن ذكرها على سبيل المثال لا الحصر:

1. نظام العقوبات السعودي، المعروف رسميًا بـــ "نظام العقوبات العامة"، الصادر بالمرسوم الملكي رقم م/39 وتاريخ 1439/11/19هـــ (الموافق 2018/8/1م): يحدد هذا النظام الجرائم والعقوبات المنصوص عليها في حالة ارتكاب جرائم على نظم الحاسوب والإنترنت. يشمل النظام تصنيفات للجرائم الإلكترونية ويحدد العقوبات المناسبة لكل تصنيف.

2. نظام الإجراءات الجزائية السعودي، الصادر بالمرسوم الملكي رقم م/56 وتاريخ 1400/12/5هـــ (الموافق 1980/6/19م): ينظم هذا النظام إجراءات التحقيق الجنائي بشكل عام، بما في ذلك التحقيق في جرائم تتعلق بنظم الحاسوب والإنترنت. ينص النظام على صلاحيات

[1] كامل السعيد – جرائم الكمبيوتر والجرائم الأخرى في مجال التكنولوجيا – بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي – القاهرة – في ٢٥-٢٨/ اكتوبر / ١٩٩٣م.

الجهات المختصة في جمع الأدلة الرقمية واستخدامها في إثبات الجرائم.

تلك القوانين هي أمثلة على التشريعات السعودية ذات الصلة بالتفتيش الجنائي على نظم الحاسوب والإنترنت. يجب الإشارة إلى أنه قد يتم تحديث وتعديل القوانين بمرور الوقت، لذا ينبغي الرجوع إلى النصوص القانونية الرسمية للحصول على المعلومات الدقيقة والمحدثة[1].

مقارنة التشريعات:

التشريعات المصرية والسعودية المتعلقة بالتفتيش الجنائي على نظم الحاسوب والإنترنت تختلف في عدة جوانب. يتطلب التحليل والمقارنة دقة في عدة جوانب مهمة:

1. **نطاق التفتيش:**

- في مصر، يغطي قانون العقوبات الجرائم المرتكبة على نظم الحاسوب والإنترنت.

يغطي قانون العقوبات المصري الجرائم المرتكبة على نظم الحاسوب والإنترنت. يتضمن القانون تصنيفات للجرائم الإلكترونية ويحدد الأفعال التي

[1] د.فاضل نصر الله عوض – ضمانات المتهم أمام سلطة التحقيق الابتدائي في التشريع الكويتي – دراسة مقارنة بالتشريعيين المصري والفرنسي – مجلة الحقوق – الكويت – ١٩٩٨م.

تعتبر مخالفة قانونية عند ارتكابها على الأنظمة الحاسوبية والشبكات الإلكترونية. يتم تحديد العقوبات المناسبة لكل تصنيف جريمة وفقًا للقانون[1].

- في السعودية، يشمل نظام العقوبات العامة الجرائم ذات الصلة بالحوسبة الجنائية.

في السعودية، يشمل نظام العقوبات العامة الجرائم ذات الصلة بالحوسبة الجنائية. يتضمن النظام تعريفات وتصنيفات للجرائم الإلكترونية ويحدد العقوبات المنصوص عليها لكل جريمة وفقًا للقانون. يتم التعامل مع الجرائم المتعلقة بالحوسبة الجنائية وفقًا لأحكام النظام العقابي العام[2].

بشكل عام، يمكن ملاحظة وجود تباين في نطاق التفتيش على نظم الحاسوب والإنترنت بين البلدين. في مصر، يتم تنظيم الجرائم المرتكبة على نظم الحاسوب والإنترنت بشكل مباشر من خلال قانون العقوبات، بينما في السعودية، تتم معالجة الجرائم المتعلقة بالحوسبة الجنائية في إطار النظام العقابي العام.

[1] ٢ قانون الإجراءات الجنائية المصري رقم ١٥٠ لسنة ١٩٥٠م.

[2] د. هلالي عبد اللاه أحمد – حقوق الدفاع في مرحلة ما قبل المحاكمة بين النمط المثالي والنمط الواقعي – (في فرنسا ومصر والمملكة العربية السعودية) – دار النهضة العربية – القاهرة – ١٩٩٥م.

2. الضوابط والإجراءات:

فيما يتعلق بالضوابط والإجراءات المتعلقة بالتفتيش الجنائي على نظم الحاسوب والإنترنت في مصر والسعودية، يمكن تفصيل الفروقات التالية:

- قانون الإجراءات الجنائية في مصر يحدد إجراءات التحقيق وجمع الأدلة الرقمية.

قانون الإجراءات الجنائية في مصر يحدد الإجراءات التي يتم اتخاذها خلال التحقيق في الجرائم الإلكترونية وجمع الأدلة الرقمية. يشمل ذلك استدعاء المشتبه بهم وشهود العيان وجمع الأدلة الرقمية المتعلقة بالجريمة. يتم اتخاذ الإجراءات وفقًا للأحكام المنصوص عليها في قانون الإجراءات الجنائية.

- في السعودية، نظام الإجراءات الجزائية ينظم الإجراءات الجنائية العامة بما في ذلك التحقيق في الجرائم الإلكترونية.

في السعودية، ينظم نظام الإجراءات الجزائية الإجراءات الجنائية العامة بما في ذلك التحقيق في الجرائم الإلكترونية. يتضمن ذلك استجواب المشتبه بهم وشهود العيان وجمع الأدلة

الرقمية المتعلقة بالجرائم. يتم تطبيق الضوابط والإجراءات الجنائية وفقًا لأحكام نظام الإجراءات الجزائية[1].

باختصار، يمكن ملاحظة وجود تشابه في الأساس بين الضوابط والإجراءات في كلا البلدين، حيث يتم تحديد الإجراءات اللازمة للتحقيق في الجرائم الإلكترونية وجمع الأدلة الرقمية في القوانين الجنائية لكل من مصر والسعودية.[2]

3. حقوق المتهمين:

- كلا النظامين يتعاملان مع حقوق المتهمين ويضمنان حقوقهم خلال التحقيق والمحاكمة.

فى مصر : قانون العقوبات وقانون الإجراءات الجنائية في مصر يضمنان حقوق المتهمين خلال التحقيق والمحاكمة. يشمل ذلك حق المتهم في الحصول على محامٍ لتمثيله والتعبير عن دفاعه، وحقه في الحضور في المحاكمة وسماع الإدعاءات الموجهة ضده، وحقه في إبداء الأدلة والمرافعة، وحقه في عدم إجبار نفسه على الإدلاء بأي اعتراف ضده. يتمتع المتهم بحقوقه الأساسية وفقًا للأحكام القانونية

[1] د. مأمون محمد سلامة – الإجراءات الجنائية في التشريع المصري – ج ١ – دار النهضة العربية – القاهرة – ١٩٨٨م.

[2] د.فاضل نصر الله عوض – ضمانات المتهم أمام سلطة التحقيق الابتدائي في التشريع الكويتي – دراسة مقارنة بالتشريعيين المصري والفرنسى – مجلة الحقوق – الكويت – ١٩٩٨م.

في السعودية : نظام العقوبات العامة ونظام الإجراءات الجزائية يضمنان حقوق المتهمين خلال التحقيق والمحاكمة. يتضمن ذلك حق المتهم في التمثيل القانوني والتعبير عن دفاعه، وحقه في الحضور في المحاكمة وسماع الإدعاءات الموجهة ضده، وحقه في تقديم الأدلة والمرافعة، وحقه في عدم إجبار نفسه على الإدلاء بأي اعتراف ضده. تكفل القوانين حماية حقوق المتهمين وتطبق الإجراءات القانونية المناسبة لضمان عدالة المحاكمة.[1]

باختصار، يمكن القول إن كلا النظامين في مصر والسعودية يضمنان حقوق المتهمين ويتعاملان معها بمنتهى الاحترام والعدالة خلال التحقيق والمحاكمة في قضايا التفتيش الجنائي على نظم الحاسوب والإنترنت.

4. حماية البيانات الشخصية:

- في مصر، قانون حماية المعلومات الشخصية يحمي البيانات الشخصية وينظم جمعها واستخدامها في النظم الحاسوبية والإلكترونية[2].

فى مصر : قانون حماية المعلومات الشخصية في مصر يوفر إطاراً قانونياً لحماية البيانات الشخصية وتنظيم جمعها واستخدامها في النظم الحاسوبية والإلكترونية. ينص القانون على وجوب الحفاظ على سرية البيانات الشخصية

[1] د. عبد الحافظ عبد الهادي عابد – الإثبات الجنائي بالقرائن – دراسة مقارنة – دار النهضة العربية – القاهرة – ١٩٩١م.

[2] عبد الأمير العكيلي – أصول الإجراءات الجنائية في قانون أصول المحاكمات الجزائية – ج ١ – ط ١ – مطبعة المعارف – بغداد – ١٩٧٥م.

وضمان عدم الوصول غير المصرح به إليها أو استخدامها بطرق غير قانونية. يتطلب القانون موافقة صريحة من المستخدمين لجمع ومعالجة بياناتهم الشخصية ويحدد الإجراءات التي يجب اتباعها لضمان الامتثال للمعايير والمتطلبات الأمنية لحماية البيانات الشخصية.

- في السعودية، قد تشمل حماية البيانات الشخصية في قوانين أخرى ذات الصلة.

في السعودية، قد تشمل حماية البيانات الشخصية في قوانين أخرى ذات الصلة بالخصوصية والتقنية والمعلومات، بالإضافة إلى قوانين التفتيش الجنائي والحوسبة الجنائية. تحظى البيانات الشخصية بحماية وتنظيم خاص في هذه القوانين لضمان سرية وخصوصية هذه البيانات ومنع الوصول غير المصرح به إليها أو استخدامها بطرق غير قانونية[1]

باختصار، يتوفر في مصر قانون محدد يحمي البيانات الشخصية وينظم جمعها واستخدامها في النظم الحاسوبية والإلكترونية، بينما في السعودية قد تشمل حماية البيانات الشخصية في قوانين أخرى ذات الصلة بالخصوصية والتقنية والمعلومات. يهدف كل من النظامين إلى ضمان سرية

[1] د. مأمون محمد سلامة – الإجراءات الجنائية في التشريع المصري – ج ١ – دار النهضة العربية – القاهرة – ١٩٨٨م.

5. العقوبات:

- كلا النظامين يحددان العقوبات المنصوص عليها للجرائم المرتكبة على نظم الحاسوب والإنترنت.

كلا النظامين، في مصر والسعودية، يحددان العقوبات المنصوص عليها للجرائم المرتكبة على نظم الحاسوب والإنترنت. يتم تحديد هذه العقوبات في القوانين المعنية بالتفتيش الجنائي على الأنظمة الحاسوبية والإلكترونية

على سبيل المثال، في مصر، قانون العقوبات المصري يحدد الجرائم المرتكبة على نظم الحاسوب والإنترنت ويحدد العقوبات المناسبة لكل جريمة وفقًا لنصوص القانون وبالنسبة للسعودية، نظام العقوبات العامة يشمل الجرائم ذات الصلة بالحوسبة الجنائية ويحدد العقوبات المناسبة لكل جريمة وفقًا لأحكام النظام[1]

هدف تحديد العقوبات في كلا النظامين هو تأديب المرتكبين وردعهم عن ارتكاب جرائم على نظم الحاسوب والإنترنت، وضمان تنفيذ العدالة وحماية المجتمع والأفراد من التهديدات الإلكترونية والاختراقات السيبرانية.

يجب الأخذ في الاعتبار أن هذه المقارنة تقدم نظرة عامة وقد تتطور التشريعات في كلا البلدين بمرور الوقت. [2]

---

[1] عبد الأمير العكيلي – أصول الإجراءات الجنائية في قانون أصول المحاكمات الجزائية – ج ١ – ط ١ – مطبعة المعارف – بغداد – ١٩٧٥م.

[2] د.رؤوف عبيد – مبادئ الإجراءات الجنائية في القانون المصري – ط١٦ دار الجيل – القاهرة – ١٩٨٦م.

الاستنتاج و التوصيات

بناءً على المقارنة والتحليل السابق، يتوصل الدراسة إلى الاستنتاجات القانونية التالية:

1. هناك اختلافات في نطاق التفتيش على نظم الحاسوب والإنترنت بين القوانين المصرية والسعودية. قانون العقوبات المصري يغطي الجرائم المرتكبة على نظم الحاسوب والإنترنت بينما يتناول نظام العقوبات السعودي الحوسبة الجنائية بشكل عام.

2. تختلف الضوابط والإجراءات المنصوص عليها في قوانين الإجراءات الجنائية المصرية والسعودية بشأن التحقيق في الجرائم الإلكترونية. يجب أخذ هذه الاختلافات في الاعتبار عند تنفيذ إجراءات التحقيق وجمع الأدلة الرقمية.

3. يجب الالتزام بحقوق المتهمين في كلا النظامين وضمان حقوقهم أثناء التحقيق والمحاكمة، وذلك وفقاً للقوانين الجاري بها العمل في كل بلد.

4. يجب حماية البيانات الشخصية واحترام الخصوصية في كلا البلدين وفقًا للتشريعات ذات الصلة، مثل قانون حماية المعلومات الشخصية في مصر وقوانين أخرى محتملة في السعودية.

5. يجب تنفيذ العقوبات المنصوص عليها في القوانين المصرية والسعودية لمكافحة الجرائم المرتكبة على نظم الحاسوب والإنترنت، وتطبيقها بشكل مناسب لضمان العدالة والردع الجنائي.

تلك هي الاستنتاجات القانونية الرئيسية التي تم التوصل إليها بناءً على المقارنة والتحليل المذكورين، ومن المتوقع أن تؤثر هذه القوانين على التفتيش الجنائي على نظم الحاسوب والإنترنت في المملكة العربية السعودية وجمهورية مصر العربية.

يتجاهل القانون رقم 175 لسنة 2018 تماماً الضمانات الدستورية وحقوق الإنسان الخاصة بالخصوصية وحرمة الحياة الخاصة .من الناحية العملية ، فإنه يجعل البيانات الإلكترونية لمستخدمي الإنترنت وخدمات الاتصالات متاحة تماماً ويمكن الوصول إليها لأجهزة الأمن القومي ، دون رقابة قضائية أو لوائح واضحة ، ودون توفير وسائل تظلم حقيقية لتجنب الضرر الناتج عن مثل هذا الانتهاك للخصوصية. أو حتى تقديم تعويض عن الضرر في حالة حدوثه.

لذلك ، توصي هذه الدراسة بتعديل القانون 175 لعام 2018 بحيث تتوافق مواده تماماً مع الدستور المصري والمواثيق والعهود الدولية لحقوق الإنسان التي صادقت عليها مصر .يجب أن تشمل التعديلات ما يلي:

1- عدم إلزام أو السماح لمقدمي الخدمة بالاحتفاظ أو تخزين البيانات التي تتجاوز ما يلزم لأداء مهامهم وللمدة اللازمة لأداء عملهم .بمعنى آخر ، يجب أن يحدد القانون صراحة نوع البيانات المطلوب فحصها أو الكشف عنها ، وحصر الحاجة إلى الكشف عن البيانات للسلطات القضائية فقط ، مع ترتيب العقوبات في حالة احتفاظ مقدم الخدمة ببيانات تنتهك الموافقة التي حصلت عليها من مستخدميها.

2-في حال استدعى التحقيق في جريمة معينة الوصول إلى بيانات مستخدم خدمات الاتصالات والإنترنت ، أو الاحتفاظ بالبيانات لفترة محددة ، يجب أن ينص القانون على اللوائح التي يمكن بموجبها تلبية مثل هذا الطلب عند تقديمه. إلى سلطة قضائية مستقلة .يمكن أن تشمل هذه اللوائح: ذكر الشخص (الأشخاص) المطلوب الوصول إلى بياناته والأسباب التي تبرر هذا الطلب ، بالإضافة إلى تحديد نوع البيانات المطلوب الوصول إليها أو الكشف عنها ، وفي حالة الطلب المتعلقة بتخزين البيانات لفترة زمنية محددة (وهو ما يماثل وضع الشخص تحت مراقبة الشرطة) ، يلزم تحديد هذه الفترة والأسباب الكامنة وراء طلب تخزين البيانات.

3-لا ينبغي أن ينص القانون على إلزام مقدمي الخدمة بمنح أي جهة حكومية أو غير حكومية وصولاً كاملاً إلى نظم المعلومات الخاصة بها ، تحت أي ظرف من الظروف .يمكن بالأحرى أن يقتصر ذلك على البيانات التي يحددها أمر قضائي مسبب ولفترة زمنية محددة.

تلك الإجراءات والضوابط تهدف إلى ضمان حماية حقوق المستخدمين والخصوصية فيما يتعلق بالبيانات الشخصية، وتحقيق توازن بين حاجة الدولة إلى التحقيق في الجرائم الإلكترونية وحماية الحقوق الأساسية للأفراد.

قائمة المراجع العربية :

المصادر أولاً: الكتب

- القرآن الكريم

١. إبراهيم صالح المحامي – التعليمات العامة للنيابات في المسائل الجنائية حسب آخر التعديلات – القاهرة – ١٩٩٤م

٢. د. أحمد أبو الروس – التحقيق الجنائي والتصرف فيه والأدلة الجنائية – دار المطبوعات الجامعية – الإسكندرية – ١٩٩٢م.

٣. د. أحمد حسام طه تمام – الجرائم الناشئة عن استخدام الحاسب الآلى ــ (الحماية الجنائية للحاسب الآلي – دراسة مقارنة – دار النهضة العربية – القاهرة – ٢٠٠٠م.

٤. د.أحمد عوض بلال – الإجراءات الجنائية المقارنة والنظام الإجرائي فى المملكة العربية السعودية – دار النهضة العربية – القاهرة – ١٩٩٠م.

ه. د. أحمد عوض بلال – قاعدة استبعاد الأدلة المتحصلة بطرق غير مشروعة في الإجراءات الجنائية المقارنة – دار النهضة العربية – القاهرة – ١٩٩٤م.

٦. د. أحمد فتحي سرور – الشرعية والإجراءات الجنائية – دار النهضة العربية – القاهرة – ١٩٧٧م – وط ١٩٩٥م.

. أحمد فتحي سرور – الوسيط في قانون الإجراءات الجنائية – ط – دار النهضة العربية – القاهرة –ط ١٩٨٥م– و ١٩٩٣م.

٧. أسامة أحمد المناعسة وجلال محمد الزعبي وصايل الهواوشة – جرائم الحاسب الآلي والإنترنت – دراسة تحليلية مقارنة – ط ١ – دار وائل – عمان – ٢٠٠١م.

٩. د. أسامة عبد الله قايد – الحماية الجنائية للحياة الخاصة وبنوك المعلومات – دراسة مقارنة – ط ٢ – دار النهضة العربية – القاهرة – ١٩٨٩م.

١٠. أسامة محمود أبو عباس – رحلة إلى عالم الإنترنت – ط ١– شركة النجار للكمبيوتر والإلكترونيات – الأردن – اربد – ١٩٩٩م.

١١. د. آمال عبد الرحيم عثمان – الإثبات الجنائي ووسائل التحقيق العلمية – دار النهضة العربية – القاهرة – ١٩٧٥م.

١٢. د. آمال عبد الرحيم عثمان – شرح قانون الإجراءات الجنائية – دار النهضة العربية – القاهرة – ١٩٧٥م.

١٣. انتصار نوري الغريب – أمن الكمبيوتر والقانون – دار الراتب الجامعية – بيروت – ١٩٩٤م.

١٤. بيتر كنت – الدليل الكامل إلى الإنترنت – ترجمة سامح الخلف – ط ١ – الدار العربية للعلوم – بيروت – ١٩٩٧م.

١٥. بيل جيتس وآخرين – المعلوماتية بعد الإنترنت طريق المستقبل) – ترجمة أ. عبد السلام رضوان – سلسلة عالم المعرفة – المجلس الوطني للثقافة والفنون الآداب – العدد ٢٣١ – الكويت – مارس ١٩٨٨م.

١٦ . توفيق الشاوي – فقه الإجراءات الجنائية – ط ٢ – ج ١- ج ٢- ١٩٥٤.

١٧. جميل عبد الباقي الصغير – أدلة الإثبات الجنائي والتكنولوجيا الحديثة – (أجهزة الرادار – الحاسبات الآلية – البصمة الوراثية – دراسة مقارنة – دار النهضة العربية – القاهرة – ٢٠٠١م.

١٨. د.جميل عبد الباقي الصغير – الإنترنت والقانون الجنائي – الأحكام الموضوعية للجرائم المتعلقة بالإنترنت – دار النهضة العربية – القاهرة – ٢٠٠١م.

١٩. د.جميل عبد الباقي الصغير – الجوانب الإجرائية المتعلقة بالإنترنت – دار النهضة العربية – القاهرة – ٢٠٠١م.

٢٠. د.جميل عبد الباقي الصغير – القانون الجنائي والتكنولوجيا الحديثة – الكتاب الأول – الجرائم الناشئة عن استخدام الحاسب الآلي – ط١ – دار النهضة العربية – القاهرة – ١٩٩٢م.

٢١. جورج الخوام – الحواسيب اليوم – ط ١ – منشورات الأمم المتحدة لإغاثة وتشغيل اللاجئين – فينا – ١٩٩٢م.

٢٢. جون فورستر – مجتمع التقنية العالية – قصة ثورة تقنية المعلومات – ط١ – ترجمة ونشر مركز الكتاب الأردني – الأردن – ١٩٨٩م.

٢٣. د. حامد راشد – أحكام تفتيش المسكن في التشريعات الإجرائية العربية – دراسة مقارنة – ط ١ – دار النهضة العربية – القاهرة – ١٩٩٨م.

٢٤. حسن الجوخدار – شرح قانون أصول المحاكمات الجزائية – ط٢ – مكتبة دار الثقافة – عمان – ١٩٩٧م.

٢٥. د. حسن بشيت خوين ضمانات المتهم في الدعوى الجزائية – ج ١+٢ – ط ١ – دار الثقافة – عمان – ١٩٩٨م.

٢٦. حسن صادق المرصفاوي – المرصفاوي في أصول الإجراءات الجنائية – منشأة المعارف – الإسكندرية – ١٩٩٦م.

٢٧. حسن صادق المرصفاوي – قانون الإجراءات الجنائية مع تطوراته التشريعية ومذكراته الإيضاحية وأحكام النقض في خمسين عاماً – موسوعة الفقه والقضاء للدول العربية – الجزء (١٤٠) – الدار العربية للموسوعات – بيروت – ١٩٨١م.

٢٨. د.حسني الجندي – الدفع ببطلان التفتيش في ضوء أحكام محكمة النقض دراسة تحليلية تأصيلية – دار النهضة العربية – القاهرة – ١٩٨٨/١٩٨٩م.

٢٩. د.حمودي الجاسم – دراسة مقارنة في أصول المحاكمات الجزائية – ج ١ – مطبعة العاني – بغداد – ١٩٦٢م.

٣٠. د.م.ي. باجا نوف ود. يوم غرو شيفري– شرح الإجراءات الجنائية السوفيتية – ترجمة صالح العبيدي – جامعة بغداد – بغداد – ١٩٩٠م.

٣١. د.رؤوف عبيد المشكلات العملية الهامة في الإجراءات الجنائية – ج ١ – ط ٣ – دار الفكر العربي.

٣٢. د.رؤوف عبيد – مبادئ الإجراءات الجنائية في القانون المصري – ط ١١ – القاهرة – ١٩٧٦م / وط ١٦ – ١٩٨٥م.

٣٣. د.رؤوف عبيد – مبادئ الإجراءات الجنائية في القانون المصري – ط١٦ دار الجيل – القاهرة – ١٩٨٦م.

٤٦. عبد الأمير العكيلي – أصول الإجراءات الجنائية في قانون أصول المحاكمات الجزائية – ج ١ – ط ١ – مطبعة المعارف – بغداد – ١٩٧٥م.

٤٧. د. عبد الحافظ عبد الهادي عابد – الإثبات الجنائي بالقرائن – دراسة مقارنة – دار النهضة العربية – القاهرة – ١٩٩١م.

٤٨. د. عبد الحميد الشواربي – ضمانات المتهم في مرحلة التحقيق الابتدائي – منشأة المعارف – الإسكندرية – ١٩٨٨م.

٤٩. عبد الحميد المنشاوي – المرجع العلمي في إجراءات التحقيق الجنائي – دار الفكر الجامعي – القاهرة – ١٩٩٤م.

٥٠. م.عبد الحميد بسيوني عبد الحميد – شبكات الكمبيوتر – ج ١ – مكتبة ابن سينا – القاهرة – ١٩٩٥م.

٥١. د. عبد الرؤوف مهدي – شرح القواعد العامة للإجراءات الجنائية وفقاً لآخر التعديلات – دار النهضة العربية – القاهرة – ٢٠٠٠م.

٥٢. د. عبد العظيم الوزير – شرح قانون العقوبات – القسم الخاص – جرائم الاعتداء على الأموال – ط ١ – دار النهضة العربية – القاهرة – ١٩٩٣م.

٥٣. د. عبد الفتاح بيومي حجازي – الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت – دراسة متعمقة في جرائم الحاسب الآلي والإنترنت – دار الكتب القانونية – القاهرة – ٢٠٠٢م.

٥٤. د. عبد الفتاح بيومي حجازي – النظام القانوني لحماية التجارة الإلكترونية – ط ١ – دار الفكر الجامعي – الإسكندرية – ٢٠٠٢م.

٥٥. عبد الفتاح مراد – التحقيق الجنائي التطبيقي – القاهرة – ١٩٩٥م.

٥٦. د. عبد الوهاب حومد – الوسيط في الإجراءات الجزائية الكويتية – ط ٢ – جامعة الكويت – الكويت – ١٩٨٢م.

٥٧. د.عصمت عبد المجيد بكر ود صبري حمد خاطر – الحماية القانونية للملكية الفكرية – ط ١ – بيت الحكمة – بغداد – **٢٠٠١م.**

٥٨. د. عفيفي كامل عفيفي – جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون – دراسة مقارنة – (د.ت).

٥٩. د. علاء عبد الرزاق السالمي – تكنولوجيا المعلومات – ط ١ – كحلـــــــــــــــون – عمان – ١٩٩٧م.

٦٠ . علي عبد القادر القهوجي – الندب للتحقيق – دار الجامعة الجديدة للنشر . الإسكندرية – ١٩٩٧م.

٦١. د. عمر السعيد رمضان – مبادئ الإجراءات الجنائية – دار النهضة العربية – القاهرة – ١٩٨٥م.

٦٢. عمر الفاروق الحسيني – المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية – دراسة تحليلية نقدية – ط٢ – القاهرة – ١٩٩٥م.

٦٣. د. عوض محمد – الوجيز في قانون الإجراءات الجنائية – الجزء الأول – دار المطبوعات الجامعية – الإسكندرية (د.ت).

٦٤ . عوض منصور – شبكة إنترنت دليلك السريع للاتصال بالعالم – ط١ – دار البشير – عمان – ١٩٩٦م.

٦٥. د.غنام محمد غنام – الحماية الجنائية لأسرار الأفراد لدى الموظف العام – دار النهضة العربية – القاهرة – ١٩٨٨م.

٦٦. فاروق الكيلاني – محاضرات في قانون أصول المحاكمات الجزائية الأردني والمقارن – ج ٢ – دار الفارابي – عمان – ١٩٨٥م.

٦٧ . فاروق محمد العامري – الشبكة العالمية للمعلومات – الإنترنت – ط ١ – النسر الذهبي للطباعة – القاهرة – ١٩٧٧م.

٦٨. م.فاروق حسين – فيروسات الحاسب الآلي والإنترنت – ط١ – دار هـــــــــلا للنشر – ١٩٩١م.

٦٩. د.فوزية عبد الستار – شرح قانون أصول المحاكمات الجزائية اللبناني – دار النهضة العربية – بيروت – ١٩٧٥م.

٧٠. د. فوزية عبد الستار – شرح قانون الإجراءات الجنائية – دار النهضة العربية – القاهرة – ١٩٨٦م.

٧١. د.قدري عبد الفتاح الشهاوي – أدلة مسرح الجريمة – منشأة المعـــــــــارف – الإسكندرية – ١٩٩٧م.

٧٢. د قدري عبد الفتاح الشهاوي – الحدث الجرمى – منشأة المعارف – الإسكندرية – ١٩٩٩م.

٧٣. قدري عبد الفتاح الشهاوي – ضوابط السلطة الشرطية في التشريع الإجرائي المصري والمقارن – ط ١ – منشأة المعارف – الإسكندرية – ١٩٩٩م.

٧٤. د.كامل السعيد – الأحكام العامة في الاشتراك الإجرامي في قانون العقوبات الأردني – دراسة تحليلية مقارنة – ط ١ – دار مجدلاوي – عمان – ١٩٨٣م.

٧٥. د. كامل السعيد – شرح الأحكام العامة في قانون العقوبات الأردني – دراسة مقارنة – عمان – ١٩٩٨م.

٧٦. كمال كمال الرخاوي – إذن التفتيش فقهاً وقضاء – ط ١ – دار الفكـــــ والقانون – المنصورة – ٢٠٠٠م.

٧٧. د.لؤي جميل حدادين – نظرية البطلان في قانون أصول المحاكمات الجزائية – دراسة مقارنة – ط ا – المؤلف نفسه) – عمان – ٢٠٠٠م.

٧٨. د. مأمون محمد سلامة – الإجراءات الجنائية في التشريع المصري – ج ١ – دار النهضة العربية – القاهرة – ١٩٨٨م.

٧٩. د.مارسيل لوكلير – الوجيز في الشرطة التقنية – تعريب د. بسام الهاشم – ط١ – الدار العربية للموسوعات – بيروت ١٩٨٣م.

٨٠. مبدر الويس – أثر التطور التكنولوجي على الحريات العامة – منشأة المعارف – الإسكندرية – (د.ت).

٨١. المحامي صبحي المحمصاني – الأوضاع التشريعية في الدول العربية ماضيها وحاضرها ط٣ – دار العلم للملايين – بيروت – ١٩٦٥م.

٨٢. د. محمد إبراهيم زيد – تنظيم الإجراءات الجزائية في التشريعات العربية – ج ٢ – المركز العربي للدراسات الأمنية والتدريب – الرياض – ١٩٩٠م.

٨٣. محمد أحمد فكيرين – أساسيات الحاسب الآلي – دار الراتب الجامعية – بيروت – ١٩٩٣ م.

٨٤. د. محمد أمين الميداني – النظام الأوروبي لحماية حقوق الإنسان – دار البشير – عمان – ١٩٨٩م.

٨٥. د. محمد إبراهيم زيد ود. عبد الفتاح الصيفي – قانون الإجراءات الجنائية الإيطالي – دار النهضة العربية – القاهرة – ١٩٩٠م.

٨٦. د. محمد الأمين البشرى– العدالة الجنائية ومنع الجريمة – دراسة مقارنة – ط١– أكاديمية نايف العربية للعلوم الأمنية – الرياض – ١٩٩٧م.

٨٧. د. محمد الجبور – استعانة المتهم بمحام – دراسة مقارنة – ط١ – دار الثقافة – عمان – ٢٠٠٢م.

٨٨. د. محمد الجبور – الجرائم الواقعة على أمن الدولة في القانون الأردني والقوانين العربية – ط ٢ – عمان – ٢٠٠٠م.

٨٩. د. محمد الفاضل – التعاون الدولي في مكافحة الإجرام – بدون دار نشر –(د.ت).

٩٠. د. محمد زكي أبو عامر – الإجراءات الجنائية – ط ٢ – منشأة المعارف – الإسكندرية – ١٩٩٠م.

٩١. د.محمد سامي الشوا – ثورة المعلومات وانعكاساتها على قانون العقوبات الجزء الثاني – دار النهضة العربية – القاهرة – ١٩٩٤م.

٩٢. د. محمد شلال العاني وعلي حسن طوالبه – علم الإجرام والعقاب – ط ١ – دار المسيرة – عمان – ١٩٩٨م.

٩٣. د.محمد صبحي نجم – قانون أصول المحاكمات الجزائية – ط١ – دار الثقافة – عمان –٢٠٠٠م.

٩٤. د.محمد عبد الظاهر حسين – الاتجاهات الحديثة في حماية برامج الكمبيوتر المعلوماتية – دار النهضة العربية – القاهرة – ٢٠٠٠/٢٠٠١م.

٩٥. د. محمد عبد المحسن المقاطع – حماية الحياة الخاصة للأفراد وضماناتها في مواجهة الحاسوب الآلي – دراسة تحليلية نقدية مقارنة للحق في الخصوصية وتطبيقاته في القانون الكويتي – مطبوعات جامعة الكويت – الكويت –**١٩٩٢م.**

٩٦. محمد علي سالم عياد الحلبي – الوسيط في شرح قانون أصول المحاكمات الجزائية – ج ١ – مكتبة دار الثقافة للنشر – عمان – ١٩٩٦م.

٩٧. د.محمد علي عياد الحلبي – الحرية الشخصية أثناء التحري والاستدلال في القانون المقارن – ط ا – منشورات ذات السلاسل – الكويت (د.ت).

٩٨. د. محمد عيد الغريب – الاختصاص القضائي لمأمور الضبط القضائي فى الأحوال العادية والاستثنائية – القاهرة –١٩٩٩ /٢٠٠٠م.

٩٩. د.محمد فهمي طلبة وآخرون – دائرة المعارف الحاسب الإلكتروني – مجموعة كتب دلتا – مطابع المكتب المصري الحديث – القاهرة – ١٩٩١م.

١٠٠.د. محمد كامل إبراهيم – النظرية العامة للبطلان في قانون الإجراءات الجنائية – دار النهضة العربية – القاهرة – ١٩٨٩م.

١٠١.د. محمد محدة – ضمانات المتهم أثناء التحقيق ج 3+٣٢ – ط١ – دار الهدى – الجزائر – ١٩٩٢م.

١٠٢. محمد محمد شتا – فكرة الحماية الجنائية لبرامج الحاسب الآلي – دار الجامعة الجديدة – الإسكندرية – ٢٠٠١م.

١٠٣.د. محمود شريف بسيوني ود. عبد العظيم الوزير – الإجراءات الجنائية في النظم القانونية العربية وحماية حقوق الإنسان – ط ١ – دار العلم للملايين – بيروت – ١٩٩١م.

١٠٤.د. محمود محمود مصطفى – شرح قانون الإجراءات الجنائية – ط٩ – دار النهضة العربية – القاهرة – ١٩٦٦م.

١٠٥.د. محمود نجيب حسني – الدستور والقانون الجنائي – دار النهضة العربية – القاهرة – ١٩٩٢م.

١٠٦.د.محمود نجيب حسني – شرح قانون الإجراءات الجنائية – ط٣ – دار النهضة العربية – القاهرة – ١٩٩٦م /ط٢ – ١٩٨٨م.

١٠٧. د.مدحت رمضان – جرائم الاعتداء على الأشخاص والإنترنت – دار النهضة العربية – القاهرة – ٢٠٠٠م.

١٠٨. د.مدحت محمد الحسيني – البطلان في المواد الجنائية – دار المطبوعات الإسكندرية – ١٩٩٣م.

١٠٩.د.مصطفى محمد موسى الجهاز الإلكتروني لمكافحة الجريمة – ط١ – الكتاب الأول – سلسلة اللواء الأمنية – القاهرة – ٢٠٠١م.

١١٠.د ممدوح خليل البحر – أصول المحاكمات الجزائية الأردني – ط١ – دار الثقافة – عمان – ١٩٩٨م.

١١١.د. نائل عبد الرحمن صالح – محاضرات في قانون أصول المحاكمات الجزائية – ط ١ – دار الفكر العربي – عمان – ١٩٩٧م.

١١٢.د. نعمان الخطيب – الوسيط في النظم السياسية والقانون الدستوري – ط١ – دار الثقافة – عمان – ١٩٩٩م.

١١٣. نعيم مغبغب – مخاطر المعلوماتية والإنترنت – المخاطر على الحياة الخاصة وحمايتها – دراسة في القانون المقارن – بيروت – ١٩٩٨م.

١١٤. د. نواف كنعان – حق المؤلف – النماذج المعاصرة لحق المؤلف ووسائل حمايته – ط ٣ – توزيع دار الثقافة – عمان – ٢٠٠٠م.

١١٥. هـ.كيت الخصوصية في عصر المعلومات – ترجمة محمد محمود شهاب – ط١– مؤسسة الأهرام – القاهرة – ١٩٩٩م.

١١٦. د.هدى حامد قشقوش – الحماية الجنائية للتجارة الإلكترونية عبر الإنترنت – دار النهضة العربية – القاهرة – ٢٠٠٠م.

١١٧.د.هدى حامد قشقوش – جرائم الحاسب الإلكتروني في التشريع المقارن – دار النهضة العربية – القاهرة – ١٩٩٢م.

١١٨ . هشام محمد فريد رستم – الجوانب الإجرائية للجرائم المعلوماتية – دراسة مقارنة – مكتبة الآلات الحديثة – أسيوط – ١٩٩٤م.

١١٩. هشام محمد فريد رستم – قانون العقوبات ومخاطر تقنية المعلومات – ط١ – مكتبة الآلات الحديثة – أسيوط – ١٩٩٢م.

١٢٠. د. هلالي عبد اللاه أحمد – حجية المخرجات الكمبيوترية في الإثبات الجنائي – ط١ – دار النهضة العربية – القاهرة – ١٩٩٧م.

١٢١. د. هلالي عبد اللاه أحمد – حقوق الدفاع في مرحلة ما قبل المحاكمة بين النمط المثالي والنمط الواقعي – (في فرنسا ومصر والمملكة العربية السعودية) – دار النهضة العربية – القاهرة – ١٩٩٥م.

١٢٢.د. هلالي عبد اللاه أحمد – التزام الشاهد بالإعلام في الجرائم المعلوماتية – دراسة مقارنة – النسر الذهبي – القاهرة – ٢٠٠٠م.

١٢٣. د. هلالي عبد اللاه أحمد – تفتيش نظم الحاسب الآلـــى وضمانات المتهم المعلوماتي – دراسة مقارنة – ط١ – دار النهضة العربية – القاهرة – ١٩٩٧م.

١٢٤ . ياكوف ميخايلو فيتش بيلسون – الإنتربول في الصراع ضد الجريمة الجنائية – ترجمة وإعداد : عماد محمود طحينة ومازن محمد نفاع – دار معد للنشر والتوزيع – دمشق – ١٩٩١م.

١٢٥. يوسف أوراها ياقو وعبد الناصر أحمد وحسن نعمة جعفر – المقدمة الغنية في الحاسبات الإلكترونية – مركز الفارابي – بغداد – ١٩٩٨م.

126 .نديم محمد حسن الترزي، سلطات النيابة العامة في الجرائم المعلوماتية، مجلة أندلس للعلوم الاجتماعية والإنسانية، العدد 19، مجلد 15، أبريل 2017

127. هلالي عبد الإله أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، سنة 1997، ص 47.

128. يزيد بو حليط، تفتيش المنظومة المعلوماتية وحجز المعطيات في التشريع الجزائري، مجلة التواصل في الاقتصاد والإدارة والقانون، العدد 48، ديسمبر 2016

129. أسامة بن غانم العبيدي. نديم محمد حسن الترزي، سلطات النيابة العامة في الجرائم المعلوماتية، مجلة أندلس للعلوم الاجتماعية والإنسانية، العدد 19، مجلد 15، أبريل 2017

130 . الشرقي حراث، الدفوع الشكلية في المادة الزجرية، مكتبة الرشاد السطات، الطبعة الأولى، السنة 2012

131 . خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي، الإسكندرية، مصر، الطبعة الأولى، 2009

132 . عربوز فاطمة الزهراء، التفتيش الالكتروني كإجراء للتحقيق في الجرائم المعلوماتية، مجلة جيل الأبحاث القانونية المعمقة، العدد 34

133 . خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2010

134 . هلالي عبد الإله أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، سنة 1997

144 . أحمد أسامة حسنية، التفتيش في الجرائم الإلكترونية في التشريع الفلسطيني، دراسة تحليلية مقارنة بالتشريع العُماني، 2016

145 . نور الدين الواهلي، الاختصاص في الجريمة الإلكترونية، سلسلة ندوات محكمة الاستئناف، الرباط، العدد السابع، 2014

ثانياً: الأبحاث:

١.د. أحمد السمدان – النظام القانوني لحماية برامج الكمبيوتر – مجلة الحقوق العدد٤ – السنة ١١ – جامعة الكويت – الكويت – ديسمبر – ١٩٨٧م.

٢. د. أحمد فتحي سرور – حضور المتهم أثناء التفتيش – مجلة إدارة قضايـــــــــــــا الحكومة – السنة ٣١ – العدد ١ – يناير / مارس – ١٩٥٩م.

٣ . د. أحمد فتحي سرور – مراقبة المكالمات التلفونية – المجلة الجنائية القومية العدد ١ – مارس – ١٩٦٣م. ٤. أنطوان بطرس وآخرون – الإنترنت – ملف خاص – مجلة الكمبيوتر والاتصالات الإلكترونية – المجلد ١٢– العدد ٧ – أيلول ١٩٩٥م.

ه. الرائد كمال أحمد الكركي – النواحي الفنية لإساءة استخدام الكمبيوتر – ورقة عمل مقدمة لندوة الجرائم الناجمة عن التطور التكنولوجي – المنعقدة في عمان بتاريخ ٢٩–١٩٩٨/١٠/٢٨م.

٦. الرائد كمال الكركي – جرائم الحاسوب ودور مديرية الأمن في مكافحتها – ورقة عمل مقدمة إلى ندوة قانون حماية حق المؤلف – نظرة إلى المستقبل – المنعقدة في عمان بتاريخ ١٩٩٩/٧/٥م.

٧. د.رضا عبد الحكيم إسماعيل – الوقاية من الجرائم الناشئة عن استعمال الحاسوب – مجلة الاقتصاد الإسلامي – العدد ٢١٨ – السنة ١٩ – أغسطس١٩٩٩م.

٨. د. عادل رياض محمد – جرائم الحاسوب وأمن البيانات – مجلة العربي – العدد ٤٤٠– السنة ٣٨ – الكويت – يوليو – ١٩٩٥م.

٩. غسان حزين – قصة اختراع البريد الإلكتروني – مجلة العربي – العدد ٥٣٠ – الكويت – يناير – ٢٠٠٣م.

١٠. د.فاضل نصر الله عوض – ضمانات المتهم أمام سلطة التحقيق الابتدائي في التشريع الكويتي – دراسة مقارنة بالتشريعيين المصري والفرنسى – مجلة الحقوق – الكويت – ١٩٩٨م.

١١. كامل السعيد – جرائم الكمبيوتر والجرائم الأخرى في مجال التكنولوجيا – بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي – القاهرة – في ٢٥–٢٨/ اكتوبر / ١٩٩٣م.

١٢ . د. كامل فريد السالك – الجريمة المعلوماتية – مجلة المحامون السورية – العدد (٥–٦) – السنة (٦٦) – أيار وحزيران – ٢٠٠١م.

١٣. د. محمد الأمين البشري – الأدلة الجنائية الرقمية – مفهومها ودورها فـــي الإثبات – المجلة العربية للدراسات الأمنية والتدريب – المجلد ١٧-- العدد ٣٣– السنة ١٧ – الرياض – أبريل ٢٠٠٢م.

١٤. د. محمد الأمين البشري – التحقيق في جرائم الحاسب الآلي – بحث مقـــدم لمؤتمر القانون والكمبيوتر والإنترنت – جامعة الإمارات العربية – ٢٠٠٠م.

١٥. د. محمد سعيد نمور – الأحكام العامة للجرم المشهود في التشريع الأردني – دراسة مقارنة – مجلة مؤته – المجلد ١٦ – العدد ١ – ١٩٩١م.

١٦. مختار محمد أمين – جرائم الحاسب الإلكتروني – مجلة الأمن العام – العدد ٩٠– السنة ٢٣ – القاهرة – ١٩٨٠م.

١٧. د.مدحت رمضان – الأحكام العامة للقانون الجنائي وجرائم الإنترنت – بحث مقدم لندوة الجرائم الناجمة عن التطور التكنولوجي – المنعقدة في عمان بتاريخ ٢٨– ١٩٩٨/١٠/٢٩م.

١٨. د.معتصم مشعشع – استعانة المشتكى عليه بمحام خلال الاســـ تجواب في مرحلة التحقيق الابتدائي – دراسة في القانون الأردني مقارنة مع القانون الفرنسي – مجلة الدراسات – الجامعة الأردنية – المجلد ٢٦ العدد ١ – ١٩٩٩م.

١٩. د.نائل عبد الرحمن صالح – واقع جرائم الحاسوب في التشريع الأردني – ورقة عمل مقدمة لمؤتمر القانون والكمبيوتر والإنترنت – جامعة الإمارات العربية المتحدة – العين – في ١-٢٠٠٠/٥/٣م.

٢٠. د.نوري حمد خاطر – قراءة في قانون حق المؤلف الأردني رقم (٢٢) لسنة ١٩٩٢م – بحث مقدم لمجلة مؤته للبحوث والدراسات – المجلد ١٢ – العدد ١ تشرين أول – ١٩٩٧م.

٢١. د. هشام محمد فريد رستم – الجرائم المعلوماتية – أصول التحقيق الجنائي الفني واقتراح بإنشاء آلية عربية موحدة للتدريب التخصصي – بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت – في (٣-١ مايو) ٢٠٠٠م.

٢٢. د. هشام محمد فريد رستم – جرائم الحاسوب كصورة من صور الجرائم الاقتصادية المستحدثة – مجلة الدراسات القانونية – جامعة أسيوط – العـــــــدد ١٧– ١٩٩٥م.

٢٣. يونس خالد غرب – جرائم الحاسوب – ندوة الجرائم الناجمة عن التطور التكنولوجي – المنعقدة في عمان – ٢٩-٢٨/١٠/١٩٨٨م.

رابعاً: الدساتير والقوانين

الدساتير:

١– الدستور اللبناني لسنة ١٩٢٦م.

٢ – الدستور الأردني لسنة ١٩٥٢م.

٣ – الدستور السوري لسنة ١٩٦٤م.

٤ – الدستور العراقي لسنة ١٩٧٠م.

٥ – الدستور المصري لسنة ١٩٧١م.

٦– الدستور الإماراتي لسنة ١٩٧١م.

٧– الدستور الجزائري لسنة ١٩٧٦م.

القوانين الإجرائية:

١- قانون أصول المحاكمات الجزائية اللبناني لسنة ١٩٤٨م.

٢ قانون الإجراءات الجنائية المصري رقم ١٥٠ لسنة ١٩٥٠م.

٣- قانون أصول المحاكمات الجزائية السوري رقم ١١٢ لسنة ١٩٥٠م.

٤ - قانون الإجراءات الجنائية الليبي لسنة ١٩٥٣م.

ه - قانون المسطرة الجنائية المغربي لسنة ١٩٥٩م.

٦- قانون الإجراءات والمحاكمات الجزائية الكويتي رقم ١٧ لسنة ١٩٦٠م.

٧-قانون أصول المحاكمات الجزائية الأردني رقم ٩ لسنة ١٩٦١م.

٨- قانون الإجراءات الجنائية الصومالي رقم (١) لسنة ١٩٦٣م.

٩ قانون الإجراءات الجزائية الجزائري لسنة ١٩٦٦م.

١٠ - قانون أصول المحاكمات الجزائية البحريني لسنة ١٩٦٦م.

١١ -قانون تنظيم المرافعات الجنائي التونسي لسنة ١٩٦٨م.

-١٢ قانون أصول المحاكمات الجزائية العراقي رقم ٢٣ لسنة ١٩٧١م.

١٣ - قانون الإجراءات الجزائية القطري رقم ١٥ لسنة ١٩٧١م.

١٤ قانون الإجراءات الجزائية الإماراتي (القانون الاتحادي رقم ٣٥ لسنة ١٩٩٢م).

١٥ - قانون الإجراءات الجنائية السوداني رقم ٦٥ لسنة ١٩٩١م.

١٦ - القانون رقم (١٦) لسنة ٢٠٠١م المعدل لقانون أصول المحاكمات الجزائية الأردني.

القوانين الخاصة:

1- قانون الجمارك رقم (٢٠) لسنة ١٩٩٨م.

2- قانون مراقبة المصنفات المرئية والمسموعة رقم (٨) لسنة ١٩٩٧م.

3- قانون حماية حق المؤلف رقم (٢٢) لسنة ١٩٩٢ ، وتعديله قانون رقم (١٤) لسنة ١٩٩٨م ، والقانون المعدل رقم (٢٩) لسنة ١٩٩٩م.

4 – قانون المعاملات الإلكترونية المؤقت رقم (٨٥) لسنة ٢٠٠١م.

المراجع الأجنبية :

مراجع باللغة الإنجليزية :

1. Faiz, M., Umar, R. & Yudhana, A. (2017). Implementation of Live Forensics for Browser Comparison in Email Security. Jesica, 1, 108-114. https://www.researchgate.net/publication/316274410_Implementasi_Live_Forensics_untuk_Perbandingan_Browser_pada_Keamanan_Email
2. Rahardjo, B. (1998). Keamanan Sistem Informasi Berbasis Internet. https://www.researchgate.net/publication/228538128_Keamanan_Sistem_Informasi_Berbasis_Internet
3. Montasari, R. (2016). Review and Assessment of the Existing Digital Forensic Investigation Process Models. International Journal of Computer Applications, 147, 41-49. https://www.researchgate.net/publication/306127931_Review_and_Assessment_of_the_Existing_Digital_Forensic_Investigation_Process_Models

4. Valjarevic, A., & Venter, H. S. (2012). Harmonised digital forensic investigation process model. In 2012 Information Security for South Africa - Proceedings of the ISSA 2012 Conference (pp. 1-10). doi: 10.1109/ISSA.2012.6320441. https://www.researchgate.net/publication/261451453_Harmonised_digital_forensic_investigation_process_model

5. Agarwal, A., Gupta, M., Gupta, Y., Gupta, C. (2011). Systematic digital forensic investigation model. Gupta International Journal of Computer Science and Security, 2011, 118. https://www.researchgate.net/publication/228410430_Systematic_Digital_Forensic_Investigation_Model

6. Ieong, R. (2006). FORZA: A digital forensics investigation framework that incorporates legal issues. Digital Investigation, 3, 29-36.

https://www.researchgate.net/publication/222680703_FORZA_-_Digital_forensics_investigation_framework_that_incorporate_legal_issues

7. Casey, E. (2001). Handbook of Computer Crime Investigation: Forensic Tools and Technology. In E. Casey (Ed.), Handbook of Computer Crime Investigation: Forensic Tools and Technology. https://www.researchgate.net/publication/242391498_Handbook_of_computer_crime_investigation_forensic_tools_and_technology

8. Losavio, M., Adams, J., & Rogers, M. (2006). Gap Analysis: Judicial Experience and Perception of Electronic Evidence. Journal of Digital Forensic Practice, 1, 13-17.

https://www.researchgate.net/publication/220121465_Gap_Analysis_Judicial_Experience_and_Perception_of_Electronic_Evidence

9. Adams, R., Hobbs, V., & Mann, G. (2013). The Advanced Data Acquisition Model (Adam): A Process Model for Digital Forensic Practice. Journal of Digital Forensics, Security and Law
https://www.researchgate.net/publication/313958414_The_Advanced_Data_Acquisition_Model_Adam_A_Process_Model_for_Digital_Forensic_Practice

10. Kamran, A., Arafeen, Q., & Sheikh, A. (2020). Existing Cyber Laws and Their Role in Legal Aspects of Cybercrime in Pakistan. International Journal of Cyber-Security and Digital Forensics, 8, 241-249
https://www.researchgate.net/publication/338885893_Existing_Cyber_Laws_and_Their_Role_in_Legal_Aspects_of_Cybercrime_in_Pakistan

11. Kundi, G. M., Nawaz, A., & Akhtar, R. (2014). Digital Revolution, Cyber Crimes And Cyber Legislation: A Challenge To Governments In Developing Countries. International Journal of Academic Research in Business and Social Sciences, 4.
https://www.researchgate.net/publication/283316038_Digital_Revolution_Cyber-Crimes_And_Cyber_Legislation_A_Challenge_To_Governments_In_Developing_Countries

12. Ieong, R. (2006). FORZA: A Digital Forensics Investigation Framework Incorporating Legal Issues. Digital Investigation, 3, 29-36.

https://www.researchgate.net/publication/222680703_FORZA_-_Digital_forensics_investigation_framework_that_incorporate_legal_issues

13. Cohen, F. (2010). Toward a Science of Digital Forensic Evidence Examination. In IFIP Advances in Information and Communication Technology (Vol. 337, pp. 17-35).. https://www.researchgate.net/publication/221352733_Toward_a_Science_of_Digital_Forensic_Evidence_Examination

14. Cohen, F. (2010). Toward a Science of Digital Forensic Evidence Examination. IFIP Advances in Information and Communication Technology, 337, 17-35.

https://www.researchgate.net/publication/221352733_Toward_a_Science_of_Digital_Forensic_Evidence_Examination

15. Cohen, F. (2010). Toward a Science of Digital Forensic Evidence Examination. IFIP Advances in Information and Communication Technology, 337, 17-35. https://www.researchgate.net/publication/221352733_Toward_a_Science_of_Digital_Forensic_Evidence_Examination

16. Agarwal, A., Gupta, M., Gupta, Mr., Gupta, Y., & Gupta, C. (2011). Systematic Digital Forensic Investigation Model. Gupta International Journal of Computer Science and Security, 2011, 118. https://www.researchgate.net/publication/228410430_Systematic_Digital_Forensic_Investigation_Model

17. Reith, M., Carr, C., & Gunsch, G. (2003). An Examination of Digital Forensic Models. Journal of Digital Forensics, 1.

https://www.researchgate.net/publication/2589967_An_Examination_of_Digital_Forensic_Models

18. Ieong, R. (2006). FORZA: Digital Forensics Investigation Framework That Incorporates Legal Issues. Digital Investigation, 3, 29-36. https://www.researchgate.net/publication/222680703_FORZA_-_Digital_forensics_investigation_framework_that_incorporate_legal_issues

19. Cohen, F. (2010). Toward a Science of Digital Forensic Evidence Examination (Vol. 337). IFIP Advances in Information and Communication Technology. https://www.researchgate.net/publication/221352733_Toward_a_Science_of_Digital_Forensic_Evidence_Examination

20. Mandya, K., & Prosise, C. (2023). Incident Response: Investigating Computer Crime. https://www.researchgate.net/publication/248561279_Incident_Response_Investigating_Computer_Crime

21. Boddington, R., Hobbs, V., & Mann, G. (2023). Validating Digital Evidence for Legal Argument. Australian Digital Forensics Conference. https://www.researchgate.net/publication/49283380_Validating_digital_evidence_for_legal_argument

22. Janes, S. (2000). The Role of Technology in Computer Forensic Investigations. Information Security Technical Report, 5, 43-50. https://www.researchgate.net/publication/257547559_The_Role_of_Technology_in_Computer_Forensic_Investigations

23. Carrier, B., & Spafford, E. (2005). Automated Digital Evidence Target Definition Using Outlier Analysis and Existing Evidence. In Digital Forensic Research Workshop 2005. https://www.researchgate.net/publication/221410306_Automated_Digital_Evidence_Target_Definition_Using_Outlier_Analysis_and_Existing_Evidence

24. Egan, M., & Mathar, T. (2005). The Executive Guide to Information Security: Threats, Challenges, and Solutions. https://www.researchgate.net/publication/220690120_The_executive_guide_to_information_security_-_threats_challenges_and_solutions

25. Whitcomb, C. (2002). An Historical Perspective of Digital Evidence. International Journal of Digital Evidence, 1. https://www.researchgate.net/publication/220542518_An_Historical_Perspective_of_Digital_Evidence

26. Rogers, M., & Meyers, M. (2005). Digital Forensics: Meeting the Challenges of Scientific Evidence. International Federation for Information Processing Digital Library; Advances in Digital Forensics, 194. https://www.researchgate.net/publication/45816110_Digital_Forensics_Meeting_the_Challenges_of_Scientific_Evidence

27. Avizienis, A., Laprie, J.-C., Randell, B., & Landwehr, C. (2004). Basic Concepts and Taxonomy of Dependable and Secure Computing. Dependable and Secure Computing, IEEE Transactions on, 1, 11-33. https://www.researchgate.net/publication/3449335_Basic_Concepts_and_Taxonomy_of_Dependable_and_Secure_Computing

28. Cohen, F. (2009). Two Models of Digital Forensic Examination. In Proceedings of the IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE) (pp. 42-53). https://www.researchgate.net/publication/224084963_Two_Models_of_Digital_Forensic_Examination

ثانياً: باللغة الفرنسية:

1. .Jean Larguier- Procedure Penale -Dolloz- 1991.
2. 2.Merle et vitu: Traite de droit Criminel, paris, 1967.
3. 3.Procedure Penale - Informatique code 1993.
4. 4.Stefani, "L'acted' instruction" in Problems contemporains de procedure penale, paris- 1964.