إجراءات التحري في جرائم المعلوماتية: دراسة تقويمية

د.خديجة يوسف محمد نور[1]

المستخلص

جاءت هذه الدراسة بعنوان إجراءات التحري في جرائم المعلوماتية. وتنبع أهمية الدراسة من أن موضوع إجراءات التحري في جرائم المعلوماتية من المواضيع الجديدة والمهمة جداً، التي تحتاج إلى فقه يتعامل معها وقانون ينظمها. فهو يعد من المقدمات الضرورية التي تظهر مدى كفاءة الدول في التعامل مع تكنولوجيا المعلومات ومدى تواصلها مع معادلة التطوير والتطبيق على السواء. واستخدمت منهج الدراسة الاسلوب الوصفي التحليلي والاستنباطي استعرضت الباحثة في دراستها الموسومة بإجراءات التحري في جرائم المعلوماتية مفهوم جرائم المعلوماتية من تعريف جرائم المعلوماتية، وأنواعها وخصائصها. وتناولت فتح الدعوى الجنائية والتحري في جرائم المعلوماتية وذلك بفتح الدعوى الجنائية، ماهية التحري، وإجراءات التحري في جرائم المعلوماتية. وتوصلت الدراسة إلى أن هناك قصوراً في الكثير من التشريعات الجنائية الإجرائية في مواجهة جرائم المعلوماتية، وجود عدة صعوبات تكتنف إجراءات الجريمة المعلوماتية، منها التكاليف العالية التي تكتنف عمليات التحري عبر الإنترنت. وأوصت بضرورة قيام المشرّع السوداني بوضع تشريع خاص لمكافحة مثل هذه الجرائم يبين فيه الإجراءات الخاصة لمتابعة وتحري ومحاكمة المرتكبين، محاولة التنسيق مع الجهات والهيئات الدولية لإصدار تشريعات موحدة تكفل إمكانية تتبع بعض أنواع الجرائم وخاصة التي تمس بأمن الدولة.

[1] استاذ مساعد- قسم القانون العام، كلية القانون، جامعة الجزيرة

Procedures for investigating information crimes: An Assessment

Abstract

This study entitled the procedures of investigation in the informatics crimes, the significance of the study appear that the subject of investigation procedures in the informatics crimes is from the newest and important subjects that need to a jurisprudence deal with it and a law organize it, it is considered from the necessary introductions that demonstrate to what extent the state can deal with the informatics technology and tow what extent it can communicate with the application and development equation as equally. The study used the descriptive, analytic, inductive method, the researcher presented investigation procedures in the informatics crime by defining the informatics crimes, its types and specifications. The study presented the opening of the criminal claim and investigation in the informatics crime; therefore by opening the criminal claim, what is investigations, and the procedures in the Informatics crime. The study revealed that, there is a shortage in many of the procedural criminal legislations in encountering the informatics crime, existing of many obstacles embarrassed the procedures of the informatics crime, such as the high cost of the investigations processes via internet. The study recommends the Sudanese legislative by stating a special legislation to combat such these crimes, clarifying with it the allocated procedures to follow, investigate and sentencing the incurred, state security crimes.

مقدمة:

تشهد الحياة اليومية تطوراً متسارعاً في مجال تقنية المعلومات والتي بدأت تصبح جزء رئيساً من حياة الأفراد وتدخل جوانب حياتهم المختلفة الاقتصادية، إنّ الجريمة سابقة لوجودها على وجود القانون فإنّ التشريعات المختلفة مازالت متخلفة عن مواكبة السرعة والتطور المضطرد الذي يسير به المجرمون، إلا أنّ هذه التشريعات متفاوتة في مقدار الحماية التشريعية والتغطية القانونية الخاصة لمواكبة الجريمة، ظهرت العديد من التحديات الجديدة والمشاكل القانونية التي تواجه اجراءات التحري في جرائم المعلوماتية.

فقد ظهرت تقنيات جديدة في ارتكاب الجرائم التقليدية، كالاستيلاء على الأموال عن طريق الاحتيال ألمعلوماتي أو كإرسال بريد إلكتروني يتضمن تهديد بالقتل. كما ظهرت جرائم مستحدثة، كاختراق شبكات المعلومات. وهذا ما جعل القانون الجنائي أمام قصور في مواجهة هذه الجرائم، لذلك وضع المشرع السوداني قانون لتلك الجرائم وهو قانون جرائم المعلوماتية لسنة 2007م. وأيضاً أثرت على قانون الإجراءات الجنائية، وأهم وما اثرت علية التحري في جرائم المعلوماتية .

أهداف الدراسة:

1. التعريف بجرائم المعلوماتية وتحديد أنواعها وخصائصها.
2. إيجاد الحلول القانونية لتحقيق التوازن بين مصلحة المجتمع في الاستفادة من المستحدثات العلمية، وحماية المصالح والحقوق التي تولدت عنها.
3. التعريف بصعوبة إجراءات التحري في جرائم المعلوماتية، وضع الحلول القانونية لمكافحة تلك النوعية من الجرائم.

4. تحديد إجراءات التحري لجرائم المعلوماتية.

أهمية الدراسة:

يعتبر موضوع إجراءات التحري في جرائم المعلوماتية من المواضيع الجديدة والمهمة جداً، التي تحتاج إلى فقه يتعامل معها وقانون ينظمها. فهو يعد من المقدمات الضرورية التي تظهر مدى كفاءة الدول في التعامل مع تكنولوجيا المعلومات.

أنّ جرائم المعلوماتية من الجرائم المستحدثة التي تستعمل فيها التقنية العالية، ونظراً لكونها من الجرائم العابرة للحدود، فإنّ المشرع لابد أن يعيد النظر في كثير من المسائل الإجرائية، لأنّ هذا النوع من الجرائم جعل موضوع إجراءات التحري في مأزق حقيقي، إذ ظهرت جملة من الصعوبات والإشكالات العملية التي تعرقل وتقف كحجر عائق أمام أجهزة العدالة، إذ أصبحت هذه تواجه مشاكل إجرائية أثناء مباشرتها لواجباتها في الكشف عن هذا النوع من الجرائم وملاحقة مرتكبيها وتقديمهم للمحاكمة.

مشكلة الدراسة:

تبدأ المشكلات الإجرائية في نطاق الجرائم المعلوماتية بتعلقها في كثير من الأحيان ببيانات معالجة اليكترونية وكيانات منطقية غير مادية، وبالتالي يصعب كشف هذه الجرائم من ناحية، ويستحيل من ناحية أخرى في بعض الأحيان جمع الأدلة بشأنها، ومما يزيد من صعوبة إجراءات التحري سرعة ودقة تنفيذ الجرائم المعلوماتية وإمكانية محو آثارها، وإخفاء الأدلة المتحصل عنها عقب التنفيذ مباشرة، ويواجه التفتيش وجمع الأدلة صعوبات كثيرة في هذا المجال، وقد يتعلقان ببيانات مخزنة في أنظمة أو شبكات الكترونية موجودة في دول مختلفة ،

ويثير مسألة الدخول إليها ومحاولة جمعها وتحويلها إلى الدولة التي يجري فيها التحقيق .

و من المشكلات الإجرائية للتحري التي يثيرها هذا النوع من الجرائم مدى التزام الشهود أو المشتبه فيهم في كشف الرموز أو الأرقام أو كلمات السر المتعلقة بالبيانات أو البرامج ذات الصلة بالجريمة.

منهج الدراسة:

المنهج التحليلي ، والمنهج الاستقرائي والمقارن

الدراسات السابقة:

1) **دراسة مصعب مالك(2008)** بعنوان جرائم الحاسب الآلي بين الفقه الإسلامي والقانون - جامعة الزعيم الأزهري/ماجستير- هدفت إلى تحقيق التوازن الضروري بين مصلحة المجتمع في الاستفادة بهذه التقنية الحديثة،و مصلحة الإنسان في حمايته من الاستخدام غير السليم لهذه التقنية، وتوصلت إلى عدم ملاحقة النظم القانونية سواء على المستوى الوطني أو الدولي، للتطور المتزايد لتكنولوجيا الحاسب والاتصالات، وتأثيرها على مختلف نواحي الحياة، وإنّ الشريعة الإسلامية قد عالجت جريمة الاستنساخ غير المشروع باهتمامها الواضح بالعلم والابتكار، وأعطت الشريعة الحق بالاهتمام في منع التعدي عليها للمصلحة العامة للمجتمع، بالحفاظ على حقوق المبدعين وتشجيعهم، وكذلك أعطت الشريعة الحق للإمام في وضع العقوبات التعزيرية على المخالفين، ويأخذ السودان في مكافحة الاستنساخ غير المشروع لبرامج الحاسب الآلي ،بقانون حماية حق المؤلف والحقوق المجاورة، الذي تأخذ به معظم دول العالم، اقتصرت الدراسة على جريمة واحدة من جرائم الحاسب الآلي، وهي

جريمة الاستنساخ غير المشروع، أما الدراسة الحالية تناولت إجراءات التحري لكل الجرائم الواردة في قانون جرائم المعلوماتية لسنة 2007م .

2-**دراسة عثمان الصديق (2006)** بعنوان: الجرائم الإلكترونية في القانون السوداني- جامعة الخرطوم، رسالة ماجستير

هدفت الدراسة إلى معالجة الظاهرة الناجمة عن استخدام الحاسوب التي بدأت جلية وظاهرة داخل الأنشطة العامة، رغم أن تداولها مازال في طي الكتمان، خاصة في قطاع الأنشطة المالية والاقتصادية والبنوك، توصلت الدراسة إلى أن غالبية الدراسات البحثية والقانونية في الآونة الأخيرة، اتجهت إلى وصف عصرنا الحاضر بعصر المعلومات،ومن المعلوم أن كل فتح جديد واختراع للوجود يترب علية جملة من الآثار،لم تكن متصورة من قبل، وأفرزت تقنية المعلومات على وجه التحدي شبكة الإنترنت آثاراً عظيمة، على الهيكل الإداري والاقتصادي والسياسي والاجتماعي والثقافي والقانوني.

هذه الدراسة اقتصرت على دراسة الجريمة الإلكترونية في السودان،ولم تفصل في أنواع الجرائم الإلكترونية المختلفة،وكذلك لم تتعرض للمجرم ألمعلوماتي،ولم تبين أساليب وكيفية ارتكاب الجريمة،حيث أنها خلت من الإشارة إلى الجوانب المتعلقة بالإجراءات الجنائية مثل هذه الدراسة الحالية، أنها شملت مفهوم الجريمة المعلوماتية وإجراءات التحري فيها.

هيكل الدراسة: قسمت هذه الدراسة إلى ثلاث مباحث على النحو التالي:

المبحث الأول: مفهوم جرائم المعلوماتية

المبحث الثاني: التعريف بالتحري

المبحث الثالث: إجراءات التحري في جرائم المعلوماتية

المبحث الأول : مفهوم جرائم المعلوماتية

المطلب الأول: تعريف جرائم المعلوماتية

ويمكن تعريفها بأنها جرائم يتم ارتكابها بواسطة الحاسب الآلي عن طريق شبكة الإنترنت, وبواسطة شخص ذو دراية فائقة بها، عبدالله (عبد الكريم،2007م)، وعرفت أيضاً بأنهاالأنشطة أو الأفعال الإجرامية التي تصدر عن إرادة جنائية, والتي يستخدم فيها الحاسوب وشبكاته لأجل الاعتداء على أموال وأنفس أو عرض ,أو أي حق يحميه القانون ,ويصف الاعتداء عليه بأنه جريمة يقرر لها عقوبة أو تدبيراً احترازيا.(الحسن ،2009)

وعرفت أيضاً كل فعل ضار يأتيه الفرد أو الجماعة عبر استعمال الأجهزة الإلكترونية ويكون لهذا الفعل اثر ضاراً على غيره من الأفراد، وعرفت أيضاً بأنّها: تلك الجرائم العابرة للحدود والتي تقع على شبكة الإنترنت أو بواسطتها من قبل شخص على دراية فائقة بها (هروال، 2013م)

وترى الباحثة أن الجريمة المعلوماتية هي كل فعل يعاقب عليه, بموجب أحكام قانون جرائم المعلوماتية, يقع بواسطة أو على نظم وشبكات ووسائل المعلومات, والبرمجيات والحواسيب والإنترنت والأنشطة المتعلقة به.

المطلب الثاني: خصائص جرائم المعلوماتية

وأهم خصائص الجريمة المعلوماتية:

1) تقع الجريمة في بيئة المعالجة الآلية للبيانات,حيث تستلزم لقيامها التعامل مع بيانات مجمعة ومجهزة للدخول للنظام المعلوماتي .

(2) إثبات تلك الجرائم يحيط به كثير من الصعوبات التي تتمثل في صعوبة اكتشاف هذه الجرائم, لأنّها لا تترك أثراً خارجياً .

(3) إحجام الشركات والمؤسسات في المجتمع عن الإبلاغ.

(4) هذه الجرائم لا تعرف الحدود بين القارات على النظام المعلوماتي (الملط،2006م)

(5) تعتبر جرائم الحاسب الآلي من أكثر الجرائم التي تثير مشكلات الاختصاص على المستوى المحلى والدولي

ثانياً: صفات المجرم المعلوماتية

تعريف الصفة لغة:

هي الاسم الدال على بعض أحوال الذات ، وذلك نحو طويل وقصير وعاقل وأحمق، وغيرها وهي الأمارة اللازمة بذات الموصوف الذي يعرف بها. (الجرجاني، 1998م) الصفة الأمارة الْقَائمة بذات الْموصوف(الأنصاري، 1520م)

الصفة الدولية اصطلاحاً:

هي أي حاله اجتماعيه أو قانونيه يكون عليها الناس أو المجتمع أو الدولة والدول.

تعرف الدولة أو الدول بأنها،شعب أو شعوب مستقره على إقليم معين،وخاضع لسلطة سياسية

معينة، وهذا التعريف يتفق علية أكثر الفقهاء (حسن، بدون تاريخ) .

الصفة الدولية في القانون:

هي جماعة مستقلة من الأفراد يعيشون بصفة مستمرة على أرض معينة بينهم طبقة حاكمة وأخرى محكومة.

وهي أيضاً: شعوب منظمة خاضعة للقانون يقطنون أراضي معينة. (يوسف حسن، بدون تاريخ).

وصفات المجرم المعلوماتي كثيرة أهمها:

(1) المجرم المعلوماتي مجرم متخصص.

(2) المجرم المعلوماتي ,مجرم أخرى عائد إلى الإجرام.

(3) المجرم المعلوماتي, مجرم محترف.

(4) المجرم المعلوماتي, مجرم غير عنيف, ذلك إنه ينتمي إلى جرائم الحيلة.

(5) المجرم المعلوماتي من النوابغ ,يذكر عادة أن الأجرام المعلوماتي هو أجرام الأذكياء مقارنة التقليدي.(بيومي، 2009م).

المبحث الثاني: التعريف بالتحري

المطلب الأول: تعريف التحري لغة

القصد والارتقاء كقول القائل أتحرى مسرتك أي أطلب مرضاتك ومنه قوله تعالى: (ي ي) (سورة الجن، الآية 14) أي قصدوا طريق الحق وتوخوه ومنه حديث النبي صلى الله عليه وسلم "تحروا ليلة القدر في الوتر الأخير (البخاري، بدون تاريخ، الرازي، 1999م) **التحري:**

طلب أحرى الأمرين وأولاهما (الجرجاني، بدون تاريخ)

المطلب الثاني: تعريف التحري قانوناً

هو مجموعة من الإجراءات تستهدف التنقيب عن الأدلة بشأن جريمة ارتكبت وتجميعها ثم تقديرها لتحديد مدى كفايتها لإحالة المتهم إلى المحاكمة (يس و الفاضل، 2011م)

أما التحري عبر شبكة الإنترنت هو عمل أمني وقانوني يقوم به المتحري عبر شبكة الإنترنت بواسطة التقنية الإلكترونية الرقمية تحت تغطية للحصول على بيانات ومعلومات تعريفية أو توضيحية عن الأشخاص أو الأماكن أو الأشياء حسب

طبيعتها للحد من الجرائم الإلكترونية أو ضبطها لتحقيق الأمن الإلكتروني أو لأي غرض آخر. (موسى، 2005م)

مكان التحري: هو المكان الذي تمارس فيه النيابة, والشرطة التحري ثم مكان المحاكمة هي الحدودالجغرافية، والحدود المكانية, اختلفت المذاهب الفقهية والتشريعية في العالم في قواعد الاختصاص (قانون الإجراءات الجنائية، 1991م).

وفي جرائم المعلوماتية في السودان ينعقد الاختصاص لمحكمة الملكية الفكرية

المبحث الثالث: إجراءات التحري في جرائم المعلوماتية

تشمل تدريب الكوادر والاستعانة بالخبرة الفنية والمعاينة والتفتيش والضبط والشهادة والاستجواب وسوف نتناول كل إجراء بالتفصيل فيما يلى:

المطلب الأول: تدريب الكوادر والاستعانة بالخبرة الفنية

لاحتمال ارتباط الجرائم المعلوماتية بمختلف أنواع الجرائم فإن إجراءات التحري فيها تأخذ بجميع عناصر التحري الجنائي المتكامل وتمر بذات المراحل الفنية والشكلية. وتعد إجراءات التحري الجنائي العام هي الأساس في التحري في الجرائم المعلوماتية تماماً كما هو الحال في الجرائم الأخرى، أما عناصر التحري الجنائي الأخرى من معملية وفنية ونفسية وغيرها, فإن استخدامها يتوقف على ظروف كل جريمة, إلا أننا نؤكد أن إجراءات التحري في الجريمة المعلوماتية تتميز ببعض الخصوصية (البشرى، 2007م)، بصورة تستدعي بأن يتم تطوير أساليب التحري الجنائي بصورة تتلاءم مع هذه الخصوصية,حتى نمكن رجل الشرطة والمحقق من كشف الجريمة المعلوماتية والتعرف على مرتكبيها بالسرعة والدقة اللازمين, ولتحقيق ذلك يجب تدريب الكوادر التي تباشر التحريات والتحقيقات مع الاستعانة بذوي الخبرة الفنية المتميزة في هذا المجال فضلاً عن تطوير الإجراءات

الجنائية, لتحقيق المطلوب, وهو ما بدأت التشريعات منذ بضع سنوات في تحقيقه ومنها القانون البلجيكي الصادر في23|11|2000م.

وترى الباحثة إن المستوى الثقافي المتدني في علوم الحاسوب، لرجال الأمن والمتحريين العاملين الآن في مجال مكافحة الجريمة المعلوماتية هو خير معين لمرتكبي جرائم الحاسب الآلي.

أولاً: تدريب الكوادر:

إنّ طبيعة جرائم المعلوماتية تقتضي معرفة متميزة بنظم الحاسبات وكيفية تشغيلها ووسائل إساءة استعمال من قبل مستخدميها, ولن تتحقق هذه المعرفة التقنية, إلا باتخاذ التدابير التالية:

1) تعليم رجال الأمن مبادئ علوم الحاسب الآلي وأسلوب التعامل مع أجهزة الحاسب الآلي.
2) العمل على تخصيص وحدات خاصة لديها الإلمام الكافي بتقنيات الحاسب الآلي للعمل في المواقع ذات الصلة بالحاسب الآلي والتي يمكن أن تكون مستهدفة, مثل: البنوك التجارية –المؤسسات المالية –الشركات التجارية –البريد والبرق والهاتف مركز المعلومات القومية –أسواق أجهزة الحاسب الآلي –أسواق بيع البرامج وقطع الغيار –أماكن الصرف الآلي –أماكن التحويلات الالكترونية – معارض السيارات وتجار الجملة –المصالح الحكومية .
3) التواجد في الدورات التدريبية التي تنظمها المعاهد الخاصة والشركات في مجال الحاسب الآلي, وتكوين علاقات قوية مع المتدربين والمدربين
4) رصد حركة هواة الحاسب الآلي من الشباب (البشرى، 2007م)

وعند الحديث عن المهارات الفنية التي ينبغي أن يكتسبها المحقق في الجرائم المعلوماتية فإنّنا لا نقصد بها المهارات التقليدية التي يجب أن يتمتع بها كل متحري فهي مهارات أساسية يفترض بداهة توافرها في المتحري بالضرورة, فمهارات التعامل مع مسرح الجريمة والتحفظ على الأدلة ومناقشة الشهود وغيرها, تعتبر من أساسيات التحقيق التي يتوقع أحد عدم توافرها لدى المحقق. وعلية فإن التركيز هنا سينصب على تلك المهارات التي تتسم بالجدة والحداثة وتعتبر إفراز للتطور الإنساني في مجال تقنية الاتصالات والحوسبة وأمراً مستجد في من يتعامل مع هذه الجرائم المستحدثة وهي:

1) التعرف على المكونات المادية للحاسب الالكتروني والتعامل المبدئي معها: المهم هنا أن يتمكن المحقق من معرفة الشكل المميز للحاسب الالكتروني وملحقاته ومسمى كل منهم, والهدف من استخدامه وما هي احتمالات توظيفه لارتكاب أي من الجرائم المعلوماتية،حيث أن عدم تعرفه عليها قد يودي إلى إهمالها أو حتى إتلافها بدون قصد أو تعديل البيانات الموجودة فيها نتيجة الجهل بها, ولابد أن يلم المحقق بكيفية التعامل مع تلك المكونات من أجهزة وملحقات ووسائط تخزين بصفتها أدلة محتملة .
2) معرفة أساسيات عمل شبكات الحاسب الالكتروني وأهم مصطلحاته: الكثير من الجرائم المعلوماتية يتم ارتكابها من خلال شبكة الإنترنت, وبالتالي فإن المحقق بحاجة إلى معرفة مبادئ الاتصال الشبكي وأنواعه المختلفة وكيفية انتقال البيانات من جهاز إلى آخر على شكل حزم, ومبادئ البرتوكولات الرئيسية الخاصة بالشبكة

وتبرز أهمية فهم المحقق لمبادئ عمل الشبكات في كونها ضرورة لتصور كيفية ارتكاب الفعل الإجرامي في قضاء الانترنت من اختراق للشبكات والحاسبات واعتراض حزم البيانات أثناء انتقالها عبر الشبكة والتجسس عليها وتحويل مسارها.

3) تمييز أنظمة تشغيل الحاسب الالكتروني المتمثلة والتعامل المبدئي معها: يجب أن يكون لدى المحقق على الأقل فهم مبدئي بأنواع الأنظمة التشغيلية لأجهزة الحاسب الالكتروني وخصائص ومميزات كل نظام وأبجديات أنظمة الملفات التي يعتمد عليها,حتى يشارك في متابعة وفحص وتفتيش مسرح الجريمة.الالكتروني وخصائص ومميزات كل نظام وأبجديات أنظمة الملفات التي يعتمد عليها,حتى يشارك في متابعة وفحص وتفتيش مسرح الجريمة (عدنان،2006 م)

ثانياً: الخبرة الفنية

تعريف الخبرة:

أ) تعريف الخبرة لغة :الخبرة بمعنى والخبير من أسماء الله عز وجل بمعنى العالم بما كان وما يكون على حقيقته، والخابر المختبر المجرب والخبرة: العلم بالشيء (ابن منظور، بدون تاريخ).

ب) تعريف الخبرة اصطلاحاً:عرفها الفقهاء بأنها وسيلة من وسائل الإثبات التي تهدف إلى كشف بعض الدلائل أو الأدلة أو تحديد مدلولها بالاستعانة بالمعلومات العلمية (ابن قدامة،بدون تاريخ).

ج) الخبرة في القانون: أورد المشرع السوداني في المادة (30) من قانون الإثبات السوداني لسنة 1991م: إذا اقتضى الفصل في الدعوى استيعاب مسائل

فنية, كالطب, والهندسة والمحاسبة, والخطوط والأثر وغيرها من المسائل الفنية, فيجوز للمحكمة الاستعانة برأي الخبراء فيها, وتندب لذلك خبيراً أو أكثر, مالم يتفق الخصوم على اختيارهم. (قانون الإثبات،1994م)

منذ بدء ظهور الجرائم ذات الصلة بالحاسب الالكتروني، تستعين الشرطة وسلطات التحقيق أو المحاكمة بأصحاب الخبرة الفنية المتميزة في مجال الحاسب الآلي الالكتروني، وذلك بغرض كشف غموض الجريمة أو تجميع أدلتها والتحفظ عليها أو مساعدة المتحري في إجراء جوانب الغموض في العمليات الالكترونية الدقيقة ذات الصلة بالجريمة مجال التخصص بل يجب ان يضاف إليها سنوات من أعمال الخبرة في المجال بل يجب أن يضاف إليها سنوات من أعمال الخبرة في المجال الذي يتميز فيه، وعلى وجه الخصوص لجرائم المعلوماتية، فقد يتعلق الأمر بتزويد المستندات أو بالتلاعب في البيانات أو الغش أثناء نقل أو بث البيانات أو جريمة من جرائم الأموالأو الاعتداء على حرمة الحياة الخاصة، أو عرض صور أو أفلام مخلة بالآداب العامة (عدنان، 2011م).

وتلاحظ الباحثة أن امهر مبرمجي نظم التشغيل حتى الآن اغلبهم لم يكن مستواهم العلمي لا يتجاوز شهادة ثانوية، وكذلك الأمر ينطبق على عتاة الهكره ومحترفي الأنظمة، فأعمارهم لا تتجاوز مرحلة التعليم الثانوي والسنوات الجامعية الأولى في أحسن الأحوال، وترى الباحثة شهادة الخبير تعتبر طريق من طرق إثبات جرائم المعلوماتية بالإضافة إنّها إجراء يتبعه المتحري للوصول إلى التعرف على المتهم أو الجريمة التي ارتكبت.

المطلب الثاني: المعاينة

المعاينة: هي الانتقال، وهو عمل مادي يقصد به تغيير محل إجراءات التحقيق، فالأصل أن إجراءات التحقيق تتم بمكتب المحقق، إلا أن النظام أجاز للمحقق أن ينتقل إلى أي مكان لمباشرة أي إجراء من إجراءات جمع الأدلة، أو التحقيق عند الاقتضاء.(قايد،1998م)

وقد جاء النص على المعاينة في قانون الإجراءات الجنائية السوداني في المادة 48 "على الضابط المسئول بعد رفع محضر التحري أن يتخذ الإجراءات الفورية التالية: إذا كانت طبيعة الجريمة تقتضي ذلك، وأن ينتقل فوراً لمكان الوقائع ليتحري فيها (قانون الإجراءات الجنائية، 1991م)

إلا أن الغرض من الانتقال ليس دائماً المعاينة، بل قد يكون الانتقال لمباشرة أي إجراء من إجراءات جمع الأدلة كالتفتيش، أو سماع الشهود، أو استجواب المتهم (طنطاوي،1990م) أو يرد المحقق من الانتقال إلى المكان الذي ارتكبت فيه الجريمة، قد يسهل له سماع الشهود فور وقوع الحادث قبل أن يخضعوا لمؤثرات خارجية، فضلاً عن أنه يطلع على أدلة الجريمة ويثبتها قبل أن تزول آثارها، أو تتغير معالمها. (ابوالعلاء، بدون تاريخ)

الملاحظ أن المعاينة قد تكون بقرار من المحكمة من تلقاء نفسها، أو بناء على طلب احد الخصوم، والمحكمة تثبت انطباعاتها وأرائها الخاصة، وهذا ويجوز للمحكمة أن تستعين بأحد الخبراء في المعاينة، ولها أن تسمع من ترى سماعه من الشهود.

لا تتمتع المعاينة في مجال كشف الجريمة بنفس الدرجة من الأهمية التي تلعبها في مجال الجريمة التقليدية, ومرد ذلك :

1) أن الجرائم التي تقع على نظم المعلومات قلما يترتب على ارتكابها آثار مادية.
2) إن عدداً كبير من الأشخاص قد يتردد على مكان أو صرح الجريمة,خلال الفترة الزمنية التي تتوسط عادة ارتكاب الجريمة واكتشافها، مما يهيئ الفرصة لحدوث أو إتلاف أو عبث بالآثار المادية(منصور، 2000م)
3) إمكانية التلاعب في البيانات عن بعد, أو محوها عن طريق التدخل, من خلال وحدة طرفية من قبل الجاني (هروال، 2013م)

حتى يكون للمعاينة في الجرائم المعلوماتية فائدة في كشف الحقيقة عنها وعن مرتكبها ينبغي مراعاة عدة قواعد وإرشادات فنية أبرزها ما يلي:

1) تصوير جهاز الحاسب الآلي والأجهزة الطرفية المتصلة به والمحتويات والأوضاع العامة لمكانة.
2) العناية البالغة بملاحظة الطريقة التي تمت بها إعداد النظام والآثار الكترونية الخاصة بالتسجيلات الالكترونية التي تتزود بها شبكات المعلومات بموافقة موقع الاتصال ونوع الجهاز الذي تم عن طريقة الولوج إلي النظام أو الموقع .
3) ملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يمكن إجراء عملية المقارنة والتحليل عند عرض الأمر فيما بعد على القضاء .
4) وضع مخطط تفصيلي للمنشاة التي وقعت بها الجريمة مع كشف تفصيلي بالمسئولين بها ودور كل واحد منهم .
5) عدم نقل أي معلومة من مسرح الجريمة إلا بعد التأكد من خلو المحيط الخارجي لموقع الحاسب الالكتروني من أي مجال مغناطيسي يمكن أن تسبب في محو البيانات المسجلة (علي عدنان، 2011م).

6) القيام بحفظ المستندات الخاصة بالإدخال وكذلك مخرجات الحاسوب الورقية ذات الصلة بالجريمة.

7) ربط الأقراص الكمبيوترية التي ربما تحمل الأدلة مع جهاز يمنع الكتابة أو التسجيل عليها, مما ينتج للتحقيق قراءة بياناتها دون تغيرها (بنت قارة' بدون تاريخ).

يختلف مسرح الجريمة المعلوماتية عن مسرح الجرائم الأخرى, لأنّه يتميز بوجود الأدلة الالكترونية ذات الطبيعة غير المرئية ,لذلك ينبغي تعاملاً خاصاً معه ويكون ذلك من خلال أتباع عدة قواعد فنية قبل الانتقال إلى مسرح الجريمة المعلوماتية, أبرزها ما يلي:

1) توفير معلومات مسبقة عن مكان الجريمة, ونوع وعدد خطة الأجهزة المتوقع مداهمتها, وشبكات الاتصال الخاصة.

2) إعداد فريق التفتيش من المختصين, على أن يكون الفريق مرفقاً بالأمر القضائي اللازم للقيام بالتفتيش (البشرى، 2007م)

مسرح الجريمة الالكترونية: عند تلقي بلاغ إحدى الجرائم الالكترونية, وبعد التأكد من البيانات الضرورية, تتخذ إجراءات التحرك إلى مسرح الجريمة ومسرح الجريمة هنا يختلف عن جريمة القتل أو الاغتصاب مثلاً. وفي الغالب تكون الجريمة تكون الجريمة الالكترونية جريمة مستمرة. خاصة إذا كانت جريمة اقتصادية. وقد يكون مسرح الجريمة الالكترونية مثل مسرح الجرائم الأخرى عندما يكون الهدف منها التخزين أو إتلاف البرامج أو تزوير المستندات والوثائق أو المباني والمنشات، ففي الحالة الأولى عندما يكون التحرك لمسرح الجريمة بقصد المداهمة وضبط الأدلة على حالتها الطبيعية. أما الحالة الثانية, والتي يتم فيها

التحرك بعد وقوع الجريمة وتحقيق نتائجها التخريبية فالنجاح فيها مرهون بتوافر اعترافات المتهمين, وشهادات الشهود والقرائن وكلا الحالتين تتبع الخطوات التالية قبل التحرك لمعاينة مسرح الجريمة :

1) توفير معلومات مسبقة عن مكان الجريمة،نوع وعدد الأجهزة المتوقع مداهمتها وشبكاتها.
2) إعداد خريطة للموقع الذي تتم الإعارة علية وتفاصيل المبنى أو الطابق من المبنى موضع البلاغ, وتحديد مواقع الأجهزة والخزائن والملفات, ويتم ذلك عبر مصادر المعلومات السرية .
3) تحديد عدد وأنواع الأجهزة المحتمل تورطها في الجريمة لتحديد إمكانات التعامل معها فنياً من حيث الضبط والتأمين وحفظ المعلومات (البشرى، 2007م).
4) الحصول على الاحتياجات الضرورية من أجهزة وبرامج صعبة ولينة للاستعانة بها في الفحص والتشغيل.
5) إعداد فريق التفتيش من المتخصصين وفق قائمة تحدد الأسماء والاختصاصات والمهام الموكولة لكل بدقة
6) اخطار أعضاء الفريق قبل وقت كاف من التحرك لمسرح الجريمة لتمكينهم من إعداد خططهم الخاصة.
7) كتابة بيانات بالمهام المطلوبة من كل عضو في الفريق وتوزيعها على الجميع لضمان الانجاز مع التدخل .

8) إعداد خطة الهجوم بحيث تكون الخطة واضحة ومفهومة لدى أعضاء الفريق, على أن تكون الخطة موضحة بالرسومات وتتم مراجعتها مع أعضاء الفريق قبل التحرك .

9) إعداد الأمر القضائي اللازم للتفتيش حسب الأصول لأن الجرائم الالكترونية غالباً ما تكون داخل أمكنة لها خصوصيتها.

10) الاحتفاظ بسرية المكان حتى نهاية التفتيش إذ أن المعلومات التي يتم البحث عنها يمكن إتلافها بسهولة من قبل المتهمين أو المتورطين في الجريمة

11) تأمين التيار الكهربائي بحيث لا يتم التلاعب أو التخزين عن طريق قطع التيار أو تعديل الطاقة الكهربائية (البشرى، 2007م).

بعد وصول الفريق إلى مسرح الجريمة يتم التأمين والسيطرة على المكان والبدء في التفتيش على النحو التالي:

- السيطرة على المناطق المحيطة بمسرح وذلك عن طريق إغلاق الطرق والمداخل.
- تأمين مسرح الجريمة والسيطرة على جميع أركانها ومنافذها والتحفظ على الأشخاص الموجودين.
- تحديد أجهزة الحاسب الآلي الموجودون في الموقع, وتحديد مواقعها بأسرع فرصة ممكنة. اختيار مكان لمقابلة المتهمين والشهود على أن يكون المكان بعيداً عن أجهزة الحاسب الآلي.

ترى الباحثة: أن المعاينة في الجريمة المعلوماتية، تختلف عن المعاينة الجريمة التقليدية, لأنّ المعاينة في الجريمة التقليدية غالباً مسرح الجريمة يكون محتفظاً بآثاره المادية من بصمات وآثار دماء أو غير ذلك. ولكن مسرح الجريمة التقليدية غالباً مايكون في مكان الجاني أو المجني عليه, أما مسرح الجريمة

المعلوماتية قد يكون بعيداً جداً, فمثلاً قد ترتكب جريمة في أمريكا ويكون الجاني في السعودية, والمجني علية في السودان, وهذا ما يشكل على مبدأ تطبيق القانون.

المطلب الثالث: التفتيش

هو أيضاً إجراء من إجراءات التحقيق يستهدف البحث عن الحقيقة في مستودع السر, لذلك يعتبر من أهم إجراءات التحقيق في كشف الحقيقة, لأنّه ما ينتج عنة أدلة تؤيد نسبة الجريمة إلي المتهم (بنت قارة، بدون تاريخ)

ويري الباحث إن تفتيش نظام الحاسوب والإنترنت من أخطر المراحل حال اتخاذ الإجراءات الجنائية ضد مرتكب الجريمة الالكترونية، لكون محل التفتيش في الحاسوب ولان آثار الجريمة المعلوماتية صعب العثور عليها.

وقد نظم قانون الإجراءات الجنائية السوداني لسنة 1991م موضوع التفتيش في (86-95), التي تقابل هذه المواد الفصل السادس كل قانوني 1974م-1983م.

المطلب الرابع: الضبط

الغاية من التفتيش ضبط شيء يتعلق بالجريمة ويفيد في التحقيق الجاري بشأنها سواء أكان هذا الشيء أدوات استعملت في ارتكاب الجريمة أو شيئاً نتج عنها أو غير ذلك مما يفيد في كشف الحقيقة. وهذا من السهل الحديث عنه في كشف الحقيقة في حالة الأدلة المادية لمكونات الحاسوب ولكن المشكلة التي مازالت تظهر هي ضبط البيانات والبرمجيات.

يقصد به في قانون الإجراءات الجنائية وضع اليد على شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبها ومن حيث طبيعية القانونية قد يكون من إجراءات الاستدلال أو التحقيق والضبط بطبيعته وغايته لا يرد إلا على الأشياء أما الأشخاص فلا يصحون محلاً للضبط بالمعنى الدقيق (عدنان،2011م).

المطلب الخامس: الشهادة

نص المادة 23من قانون الإثبات السوداني لسنة 1994م على أن : الشهادة هي البينة الشفوية لشخص عن إدراكه المباشر لواقعة تثبت لغيره مسئولية مدعى بها على آخر أمام المحكمة (قانون الإثبات،1994م) وقد جاءت السوابق القضائية، في شأن الاستماع للشهادة في مرحلة التحري في سابقة حكومة السودان ،ضد زكري سيدهم بولس،م ع|م ك|42|1975م"لا يجوز قبول الشهادة، التي يدلي بها الشاهد على اليمين، في مرحلة التحري، إلا إذا كانت الشهادة، قد أخذت في إجراءات قضائية (مجلة الأحكام القضائية،1975م)

وأيضاً جاءت سابقة حكومة، ضد جابر ضو النعيم،م ع،م ك،98|1977م المتهمون، الذين يطلق سراحهم في مرحلة التحريات لعدم وجود جريمة ضدهم، لا يعتبروا شركاء، لكن يجب أن ينظر بشهادتهم، بحذر، ويكون الاعتماد عليها في نفس مستوى الاعتماد،على بينة الشريك (مجلة الأحكام القضائية، 1977م).

الشاهد في الجريمة المعلوماتية هو الفني صاحب الخبرة والتخصص في تقنية وعلوم الحاسب الالكتروني والذي تكون لدية معلومات جوهرية أو هامة لازمة للولوج في نظام المعالجة الآلية للبيانات إذا كانت مصلحة التحقيق تقتضي التنقيب عن أدلة الجريمة داخلة ويطلق على هذا النوع من الشهود مصطلح الشاهد ألمعلوماتي وذلك تمييزاً له عن الشاهد التقليدي (حسين، بدون تاريخ)

المطلب السادس: الإستجواب

يعتبر الاستجواب من أهم إجراءات التحقيق المستخدمة في كشف الحقيقة .

الاستجواب: هو التحقيق مع الأفراد، بتوجيه الأسئلة إليهم, وطلب الجواب عنها. وهو مناقشة المتهم, تفصيلاً في الأدلة, والبينات القائمة ضده, ومطالبة بالرد عليها،

إما بإنكارها, وإثبات فسادها، وأما بالتسليم بها، وما يتبعه, من اعتراف بالجريمة (نجيب، بدون تاريخ) وهو أيضاً إجراء من إجراءات التحقيق تتم فيه مناقشة المتهم فيما هو منسوب إليه من جرم ويطلب منه الرد على الأدلة القائمة ضده أما بتنفيذها أو التسليم به(ممدوح،2010م).

طبيعة الاستجواب: يعتبر الاستجواب، إجراء ذا طبيعة مزدوجة، فهو إجراء من إجراءات التحقيق، ومن ناحية أخرى إجراء من إجراءات الدفاع، أي أنه، إجراء أساسي لكل من سلطة التحقيق والمتهم، فبوصفه إجراء من إجراءات التحقيق لجمع أدلة الإثبات, يعتبر واجباً على المحقق، وبوصفه من إجراءات الدفاع يعتبر للمتهم، ويترتب على هذا, بوصفة من إجراءات التحقيق، يجوز للمحقق الالتجاء إليه في أي لحظة ،خلال التحقيق ،كما يجوز للمحقق أيضاً، إعادة استجواب المتهم ،كلما رأى ذلك ضرورياً ،وباعتباره من إجراءات الدفاع، يجب على المحقق أن يستجوب المتهم، في كل تحقيق يجريه طالما كان ذلك ممكناً (بلال،1990م).

الخاتمة والتوصيات: هنالك نتائج توصلت إليها الدراسة ثم توصيات أوصت بها وذلك على النحو التالي:

أهم النتائج:

1) ومما سبق يظهر لنا هنالك عدة صعوبات تكتنف إجراءات الجريمة المعلوماتية والتي تتمثل في عدة أمور منها:

_ سهولة محو الأدلة وتدميرها.

_ واستعمال وسائل مختلفة للتحايل وإخفاء الأدلة بوسائل حماية وبرمجيات خاصة.

_ التكاليف العالية التي تكتنف عمليات التحري عبر الانترنت والأجهزة المتخصصة.

_ ومسائل الاختصاص وهذه المسائل من أهم المعيقات التي تسبب بالامتناع عن الملاحقة أحياناً.

_ أحياناً تكون المواقع والبرمجيات معده بأساليب أو لغات برمجية خاصة لا يمكن للمتعاملين العاديين بل وحتى بعض المتخصصين التعامل معها.

2) أن الخطأ في إجراء التفتيش وضبط الأدلة قد يؤدي إلى فوات فرصة كشف الجريمة أو فوات الإدانة حتى مع معرفة الجاني.

3) هناك قصوراً في الكثير من التشريعات الجنائية الإجرائية في مواجهة ظاهرة الإجرام الإلكتروني، فما زال الكثير منها يخضع هذه الجرائم للنصوص التقليدية.

4) في السودان تم تشكيل الأجهزة المختصة في جرائم المعلوماتية "شرطة، نيابة، محكمة".

5) أن المعاينة في الجريمة المعلوماتية لا تتمتع بنفس الدرجة من الأهمية التي تتمتع بها في مسرح الجريمة التقليدية وذلك للأسباب التالية: قلة الآثار المادية المتخلفة عن جرائم الإنترنت، وإمكانية حدوث تغيير أو تلفيق أو عبث بآثار الجريمة أو إمكانية زوال بعضها، نتيجة تردد عدد كبير من الأشخاص على مسرح الجريمة.

6) أن هناك جرائم إنترنت يشترط لتحريك الدعوى الجنائية فيها تقديم شكوى من قبل المجني عليه أو وكيله الخاص، كما هو الحال في جرائم النشر التي تتم عن طريق الإنترنت.

أهم التوصيات:

1) توسعة الإطار التشريعي لمكافحة مثل هذه الجرائم يبين فيه الإجراءات الخاصة والجهات ألتحقيقيه والقضائية الخاصة لمتابعة وتحري ومحاكمة المرتكبين.

2) يجب أن يشمل التعديل في النصوص الجديدة، نظم الحاسوب والإنترنت بالأشياء التي يتم ضبطها وتعديل النصوص المتعلقة بصلاحيات المدعي العام .
3) استحداث وحدة خاصة في النيابة العامة تتكفل بمهمة التحقيق والتحري في الجرائم المعلوماتية وتوفير الأجهزة والأدوات اللازمة وإعداد أفرادها بالصورة الكافية.
4) محاولة التنسيق مع الجهات والهيئات الدولية لإصدار تشريعات موحده تكفل إمكانية تتبع بعض أنواع الجرائم وخصوصاً تلك التي يتجاوز وقوعها المستوى الفردي أو تلك التي تمس بأمن الدولة سواء الداخلي أو الخارجي وإيجاد آليات للتنسيق فيما يخص التحري والملاحقة.
5) ضرورة إعداد كوادر من النيابة للبحث والتحري والمحاكمة في نطاق الجرائم المعلوماتية مع استحداث قواعد مناسبة في مجال الإجراءات الجنائية بشأن التحري الجنائي.
6)توعية وتشجيع المجني عليهم بالإبلاغ عن أي جريمة إليكترونية فور ملاحظتها.

المصادر والمراجع

القرآن الكريم- كتب الحديث وشروحه:

1- البخاري، فتح الباري صحيح البخاري تحقيق محمد فؤاد عبد الباقي دار المعرفة بيروت 4/ 259

كتب اللغة العربية:

2. الحدود الأنيقة والتعريفات الدقيقة، 823 - 926 هـ = 1420 - 1520 م .

3. ابن منظور, جمال الدين محمد بن مكرم الأنصاري المصري، لسان العرب, المتوفى سنة 711هـ-دار صادر, ط1

4. أبو يحيى: زكريا بن محمد بن أحمد بن زكريا الأنصاري السنيكي المصري الشافعيّ.

5. الرازي، مختار الصحاح: زين الدين أبو عبد الله محمد بن أبي بكر بن عبد القادر الحنفي الرازي، المحقق: يوسف الشيخ محمد، المكتبة العصرية، الدار النموذجية، بيروت، صيدا- ط5 1420هـ / 1999م

كتب الفقه الإسلامي:

6. ابن قدامه, أبي محمد علي بن علي بن سعيد ابن حزم ابن قدامه المتوفى سنة 356هـ المغني, دار الفكر, بيروت

كتب القانون وشروحه:

10. محمد الأمين بشرى, مرشد التحريات الجنائية لرجال الشرطة والنيابة, ط1,2007م.

11. علي عدنان الفيل, إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية, المكتب الجامعي الحديث,2011، علي عدنان الفيل, المكتب الجامعي الحديث,2011م

12. أسامة عبد الله قايد، محمد علي كومان، نظام الإجراءات في المملكة العربية السعودية، دار النهضة العربية، ط 1419هـ- 1998م .

13. إبراهيم حامد طنطاوي، التحقيق الجنائي من الناحيتين النظرية والعملية، ط 1، 1999 دار النهضة العربية القاهرة.

14. الشحات إبراهيم محمد منصور، الجرائم الإلكترونية في الشريعة الإسلامية والقوانين الوضعية, الناشر دار النهضة العربية بالقاهرة،مطبعة البحيرة, 2002م د ط.

15. عائشة بنت قارة، الدليل الإلكتروني،بدون تاريخ

16. محمد الأمين البشرى،التحقيق في جرائم الحاسب الآلي والإنترنت، بدون تاريخ

17. عبد الله حسين علي محمود, سرقة المعلومات المخزنة في الحاسب, بدون تاريخ.

18. محمود نجيب حسني, شرح قانون الإجراءات الجنائية, دار النهضة العربية، القاهرة، ط2.

19. خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، 2010 .

20. أحمد عوض بلال، الإجراءات الجنائية في المملكة العربية السعودية، دار النهضة العربية،1411هـ-1990.

21. محمد أبو العلا عقيدة، وشرح الإجراءات الجناية،بدون تاريخ.

22. عزه علي محمد الحسن، الجريمة المعلوماتية في القانون السوداني, الزيتونة للطباعة, د ط,دن, 2009م.
23. مركز دراسات المجتمع، جرائم المعلوماتية، قدم من خلال ورشة عمل شارك فيها عدد من المختصين والباحثين والخبراء في مجال جرائم المعلوماتية.
24. نبيلة هبة هروال،الجوانب الإجرائية لجرائم الإنترنت،دار الفكر الجامعي،2013م.
25. أحمد خليفة الملط , الجريمة المعلوماتية , دار الفكر الجامعي, ط2 (2006).
7. عبد الفتاح بيومي حجازي, نحو نظرية عامة في علم الجريمة والمجرم ألمعلوماتي, مطبعة بهجات, ط1 , 2009م ,
8. يس عمر يوسف.،شرح قانون الإجراءات الجنائية 1991م عبد الله الفاضل عيسى، شرح قانون الإجراءات الجنائية 1991م ط8، 2011م
9. مصطفي محمد موسى, دليل التحري عبر شبكة الإنترنت, دار الكتب القانونية, مصر المحلة الكبرى, 2005م

القوانين:

26. قانون الإثبات 1994م السوداني المادة 23.
27. قانون الإجراءات الجنائية السوداني لسنة 1991.
28. قانون جرائم المعلوماتية السوداني لسنة 2007م.

المجلات القضائية:

29. مجلة الأحكام القضائية السودانية 1975م.
30. مجلة الأحكام القضائية السودانية 1977م.
31. المجلة العربية للدراسات الأمنية والتدريب،تصدر عن أكاديمية نائف للعلوم الأمنية، العدد الثلاثون، رجب،1421هـ،2000.