مظاهر التقاضي في جرائم المعلوماتية وتطبيقاتها المعاصرة

أمير محمد كافي*

مستخلص البحث:

يتصل هذا البحث الموسوم بمظاهر التقاضي في جرائم المعلوماتية وتطبيقاتها المعاصرة بالأسباب المتعلقة بوجود القصور التشريعي في الكشف عنها وطرق إثباتها خاصة في ظل تباين طرق ارتكابها، لذلك يعد هذا الموضوع بمثابة مقوم رئيس لأهمية بيان إجراءات التقاضي في جرائم المعلوماتية لذلك المشرع القانوني لابد أن يعيد النظر في كثير من المسائل والإجراءات الجنائية. فنظراً لخصوصية جرائم المعلوماتية فإنها تثير تساؤلات عديدة منها ما يتعلق بما مدى قابلية الإجراءات الجنائية للجرائم التقليدية للتطبيق على جرائم المعلوماتية وذلك بمنهج استقرائي وصفي تحليلي يوضح مخرجاته العلمية على النحو الآتي:

أولاً: النتائج:

1 صعوبة الكشف عن جرائم المعلوماتية.

2 يؤدي الخطأ في إجراءات التفتيش وضبط الأدلة إلى فوات فرص الإدانة حتى مع معرفة الجاني.

ثانياً: التوصيات:

1 ضرورة تأهيل القضاة على التعامل مع هذه الجرائم بصورة متخصصة.

2 ضرورة الإبلاغ عن أي جريمة إلكترونية فور ملاحظتها.

* الأستاذ المساعد ورئيس قسم القانون بكلية الشريعة والقانون– جامعة أم درمان الإسلامية

Abstract

This theses which entitled by judicial Aspects in intellectual crimes and contemporary Application by the conditions which related which the existence of legislature insufficiency in disclosing these armies, and the ways of improving it particularly with in rarity of the ways of committing it, so this topic is appear as inessential element in explaining judicial procedures in intellectual crimes this the legislator must stating these procedures – inspite of intellectual crimes privacy it raises many questions related by criminal procedures for traditional crimes placation through, deduituie, inductive , analytical methods which achieve the following findings.

I- Results:

1- Its difficult to disclose the intellectual crimes.
2- The inaccuracy in inspecting and Adjustment of evidence to convicte even the wrong door.

II- Recommendations:

1- Necessary to entitle the judges for cleanly with these crimes with specialized from.
2- Necessary to about the intellectual crime instantly.

مقدمة:

الحمد لله رب العالمين والصلاة والسلام على رسول الله الأمين وعلى آله وصحبه الأكارم الطيبين ومن اهتدى بهديه إلى يوم الدين.

وبعد:

فإن الحياة اليومية تشهد تطوراً متسارعاً في مجال تقنية المعلومات والاتصالات والتي صارت جزءاً رئيسياً من حياة الأفراد وتدخل جوانب حياتهم المختلفة الاقتصادية أو الأعمال اليومية التقليدية، وبما أن هذه البيئة لها رواد كثيرون جداً وجد المجرمون في هذه البيئة التقنية مرتعاً خصباً لهم وخاصةً أن طبيعتها توفر لهم الكثير من الضمانات التي تدعوهم إلى اعتقاد صعوبة الوصول إليهم أو البرمجيات التي يستخدمونها، وكما هو معروف إن الجريمة سابقة لوجودها على وجود القانون فإن التشريعات المختلفة ما زالت متخلفة عن مواكبة السرعة والتطور المضطرد الذي يسير به المجرمون، إلا أن هذه التشريعات متفاوتة في مقدار الحماية التشريعية والتغطية القانونية الخاصة لمواكبة الجريمة فبعضها يملك أسساً قانونية خاصة حول مثل هذا النوع من الجرائم ومتطورة بشكل مستمر حيث تعدل كلما ظهرت مستجدات تستوجب ذلك، ولكن بعضها الآخر لا يملك في الأصل تشريعات ناظمة لمثل هذا النوع من الجرائم التي تعرف بـ"جرائم المعلوماتية" وأمام هذا الوضع الخطير، ظهرت العديد من التحديات الجديدة والمشاكل القانونية التي تواجه القانون الجنائي بشقيه الموضوعي والإجرائي.

أولاً: أسباب اختيار الموضوع:

1. تعد الجرائم المعلوماتية من المواضيع المعاصرة.

2. لوجود القصور التشريعي في الإجراءات التي تتبع في الجرائم المعلوماتية.

3. لإثراء المكتبة القانونية بإجراءات التقاضي.

ثانياً: أهمية الموضوع:

1. يعتبر موضوع الإجراءات الجنائية لجرائم المعلوماتية من المواضيع الجديدة في ميدان الدراسات القانونية المقارنة فهو يعد من المقدمات الضرورية التي تظهر مدى كفاءة الدول في التعامل مع تكنولوجيا المعلومات ومدى تواصلها مع معادلة التطوير والتطبيق على السواء.

2. أن جرائم المعلوماتية من الجرائم المستحدثة التي تستعمل فيها التقنية العالية.

3. فإن المشروع لابد أن يعيد النظر في كثير من المسائل الإجرائية، لأن هذا النوع من الجرائم جعل موضوع الإجراءات الجنائية في مأزق حقيقي، إذ ظهرت جملة من الصعوبات والإشكالات العملية التي تعيق الأجهزة العدلية.

ثالثاً: مشكلة البحث:

ظهرت الحاجة لدراسة هذا النوع من الجرائم والتنظيم القانوني لها في محاولات لكشف الخلل التشريعي ولابد من صدور تشريعات خاصة بالجرائم المعلوماتية ولحث المشرعين على إصدار مثل هذه القوانين، لوجود العديد من المشكلات الإجرائية.

وتبدأ المشكلات الإجرائية في نطاق الجرائم المعلوماتية بتعلقها في كثير من الأحيان ببيانات معالجة إلكترونية 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 الإجراءات سرعة ودقة تنفيذ الجرائم المعلوماتية وإمكانية محو آثارها، وإخفاء الأدلة المتحصل عليها عقب التنفيذ مباشرة، ويواجه التفتيش وجمع الأدلة صعوبات كثيرة بما يتعلقان ببيان مخزنة في أنظمة، أو شبكات إلكترونية موجودة في دول مختلفة، ويثير مسألة الدخول إليها ومحاولة جمعها وتحويلها إلى الدولة التي يجري فيها التحقق.

رابعاً: أسئلة البحث:

نظراً لخصوصية جرائم المعلوماتية فإنها تثير العديد من الأسئلة أهمها:

1. ما مدى قابلية الإجراءات الجنائية للجرائم التقليدية للتطبيق على جرائم المعلوماتية؟
2. هل توجد أجهزة عدلية متخصصة في مكافحة الجرائم الإلكترونية؟
3. ما مدى قابلية تطبيق القواعد التقليدية للتفتيش والضبط في مثل هذه البيئة الافتراضية؟
4. كيف يتلقى المتحري البلاغات حول وقوع تلك الجرائم؟
5. كيف تكون محاكمة هذا النوع من المجرمين؟

خامساً: أهداف البحث

يهدف البحث إلى تحقيق المقاصد العلمية الآتية:

1. بيان طبيعة الجرائم الإلكترونية وإجراءات التقاضي فيها.
2. الدفع برؤية علمية تستهدف المراحل التي تمر بها الدعوى المعلوماتية.
3. استعراض أسس المحاكمة في الجرائم المعلوماتية.

سادساً: منهج البحث:

اعتمدت على عناصر منهج البحث الوصفي، الاستقرائي والتحليلي بأسلوب مقارن.

سابعاً: خطة البحث:

يتكون البحث من مقدمة وثلاثة مباحث.

يهتم المبحث الأول ببيان طبيعة الجرائم الإلكترونية من واقع تعريفها، وأنواعها وخصائصها.

ويناقش المبحث الثاني إجراءات فتح الدعوى الجنائية والتحري في الجرائم المعلوماتية على نحو يوضح طريقة فتح الدعوى الجنائية وحقيقة التحري.

ويعالج المبحث الثالث إجراءات التحري في الجرائم المعلوماتية.

ويتناول المبحث الرابع المحاكمة في الجرائم المعلوماتية من واقع تعريف المحاكمة والتطبيقات القضائية المعاصرة.

المبحث الأول

طبيعة الجرائم المعلوماتية

المطلب الأول: تعريف الجرائم المعلوماتية

لم يتفق الفقهاء على وضع تعريف محدد لجرائم المعلوماتية، فالبعض يطلق عليها جرائم الحاسب الآلي، والآخر يطلق عليها الغش المعلوماتي، وآخرون يطلقون عليها جرائم الإنترنت، وأيضاً يطلق عليها جرائم المعلوماتية.

ويمكن تعريفها بأنها جرائم يتم ارتكابها بواسطة الحاسب الآلي عن طريق شبكة الإنترنت، وبواسطة شخص ذو دراية فائقة بها[1].

وعرفت أيضاً بأنها الأنشطة 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 احترازياً[2].

لم يعرف قانون جرائم المعلوماتية السوداني لسنة 2007م الجريمة المعلوماتية وإنما عرف المعلوماتية، وعرف البيانات والمعلومات بأنها الأرقام والحروف والرموز وكل ما يمكن تخزينه ومعالجته وتوليده وإنتاجه ونقله بالحاسوب، أو أي وسائط إلكترونية أخرى[3].

ويمكن القول أن الجريمة المعلوماتية هي كل فعل يعاقب عليه، بموجب أحكام قانون جرائم المعوماتية لسنة 2007م، يقع بواسطة أو على نظم وشبكات ووسائل المعلومات، والبرمجيات والحواسيب والإنترنت والأنشطة المتعلقة به.

المطلب الثاني: أنواع جرائم المعلوماتية:

أولاً: جرائم النظم ووسائط وشبكات المعلومات:

1/ جريمة دخول المواقع وأنظمة المعلومات المملوكة للغير:

أورد المشرع السوداني في قانون جرائم المعلوماتية لسنة 2007م في المادة(4):

– كل من يدخل موقعاً أو نظام معلومات دون أن يكون مصرحاً ويقوم بالاطلاع عليه أو نسخه يعاقب بالسجن مدة لا تتجاوز سنتين، أو بالغرامة، أو العقوبتين معاً.

– بإلغاء بيانات، أو معلومات ملكاً للغير، أو حذفها، أو تدميرها، أو إفشائها أو إتلافها، أو تغيرها أو إعادة نشرها، أو تغيير تصاميم الموقع، أو إلغائه، أو شغل عنوانه يعاقب بالسجن مدة لا تتجاوز أربع سنوات، أو بالغرامة، أو بالعقوبتين معاً[4].

يتضح من خلال النص أعلاه أن أركان هذه الجريمة كما يلي:

– أن يقوم الجاني بدخول موقع نظام معلومات.

– أن لا يكون مصرحاً للجاني بدخول الموقع أو نظام المعلومات.

– أن يقوم الجاني بالاطلاع على الموقع أو نسخه أو إلغاء بيانات أو معلومات مملوكة للغير، أو حذف هذه المعلومات، أو تدميرها، أو تغييرها، أو إعادة نشرها، أو تغيير تصاميم الموقع، أو شغل عنوانه[5].

وشرح هذه المادة يتطلب التعرض لتعريف الموقع وأنظمة المعلومات عرف قانون جرائم المعلوماتية لسنة 2007م الموقع في المادة (3):

يقصد به مكان إتاحة المعلومات على شبكة المعلومات من خلال عنوان محدد[6].

وعرف قانون جرائم المعلوماتية لسنة 2007م شبكة المعلومات في المادة (3) بأنها أي ارتباط بين أكثر من نظام معلومات للحصول عليها أو تبادلها[7].

وعرف قانون جرائم المعلوماتية نظام المعلومات بأنه: مجموعة البرامج والأدوات والمعدات لإنتاج وتخزين ومعالجة البيانات، أو المعلومات، أو إدارة البيانات أو المعلومات[8].

2/ الاعتداء على سلامة البيانات:

يعد هذا الفرع من الجرائم المعلوماتية من أشدها خطورة وتأثيراً وأكثرها حدوثاً وتحقيقاً للخسائر ويتمثل هذا النوع من الجرائم في الدخول إلى محتوى الحاسب الآلي، واعتداء على البيانات والمعلومات الموجودة بصورة إلكترونية على الحاسبات الآلية المتصلة، أو غير المتصلة بشبكات المعلومات، والقيام بتعديلها، أو إلغاءها أو محوها أو تعطيلها بصورة ينتج عنها تعطيل أداء البرامج أو قيامه بوظائف غير تلك التي أعد لها وإتلافها [9] والمقصود بالإتلاف الذي يوجه للجانب المعنوي في الحاسب الآلي.

3/ الاعتداء على سلامة النظم والاتصالات:

من أمثلة نظم المعلومات والتقنيات الخاصة:

- نقل البيانات عبر الحدود.
- نقل الصوت والصورة إلى مسافات بعيدة عن طريق الألياف البصرية[10].
- حفظ الصورة واسترجاعها.
- نقل وتبادل المعلومات الإلكترونية.
- الإنترنت والوسائل المتعددة[11].

– الإنجاز الآلي للأعمال المصرفية.

– التسويق الإلكتروني.

وقد أدت هذه النظم إلى تقارب هائل بين الشعوب، ليس فقط في المسافات حيث أصبح العالم أو كاد يصبح قرية كونية بل أيضاً إلى تقارب الثقافات والنظم.

4/ الاعتراض غير القانوني:

ذهبت المادة (6) من قانون جرائم المعلوماتية 2007م إلى تجريم واقعة الاعتراض العمدي للرسائل بدون تصريح من النيابة العامة أو الجهة المتخصصة أو الجهة المالكة للمعلومة، عن التنصت أو التقاط أو اعتراض الرسائل، من خلال الوسائل الفنية في مكان الوصول إلى المنشأ أو داخل النظام المعلوماتي كل من يتنصت لأي رسائل عن طريق شبكة المعلومات أو أجهزة الحاسوب وما في حكمه أو يلتقطها أو يعترضها، دون تصريح بذلك من النيابة العامة أو الجهة المالكية للمعلومة، يعاقب بالسجن مدى لا تتجاوز ثلاثة سنوات أو بالغرامة أو العقوبتين معاً[12].

ثانياً: الجرائم الواقعة على الأموال والبيانات والاتصالات:

نص قانون جرائم المعلوماتية السوداني لسنة 2007م على الجرائم الواقعة على الأموال والبيانات والاتصالات على التالي:

1) التهديد أو الابتزاز: جاءت المادة (10) من قانون جرائم المعلوماتية لسنة 2007م:(كل من يستعمل شبكة المعلومات أو أحد أجهزة الحاسوب أو ما في حكمها، في تهديد أو ابتزاز شخص آخر، لحمله على القيام بفعل أو الامتناع مشروعاً، يعاقب السجن مدة لا تتجاوز سنتين أو بالغرامة أو بالعقوبتين معاً)[13].

أركان الجريمة:

– أن يستعمل الجاني شبكة المعلومات أو ما في حكمها في الآتي:

تهديد شخص أو ابتزازه بغرض حمله على القيام بفعل أو منعه من القيام.

يستوى أن يكون الفعل أو الامتناع مشروعاً أو غير مشروع وقد حددت المادة أن يكون بعث الخوف بغرض حمل الشخص على أن يؤدي عملاً تحت هذا التخويف أو يمتنع عن أدائه، ولا فرق بين أن يكون الفعل أو الامتناع عن الفعل مشروعاً أو غير مشروع ومثال ذلك أن يهدد الشخص لعمله أو غيابه عنه في الأيام العادية هي أفعال مشروعة في حد ذاتها ويكون الفعل غير مشروع مثل إجبار الشخص على إفشاء أسرار خاصة بعمله[14].

2) الاحتيال أو انتحال الشخصية أو صفة غير صحيحة:

الاحتيال هو كل تظاهر أو إيحاء يكون صالحاً لإيقاع المجني في الغلط، بطريقة تؤدي إلى الاقتناع المباشر بالمظهر المادي الخارجي أي أن المجني عليه في جريمة الاحتيال هو من جازت عليه حيلة الجاني، فانخدع بها وسلمه ماله [15]. نص قانون جرائم المعلوماتية في المادة (11) كل من يتوصل عن طريق شبكة المعلومات أو أحد أجهزة الحاسوب أو ما في حكمها عن طريق الاحتيال أو استخدام اسم كاذب أو انتحال صفة غير صحيحة بغرض الاستيلاء لنفسه أو لغيره على مال أو سند أو توقيع للسند، يعاقب السجن لمدة لا تتجاوز أربع سنوات أو بالغرامة أو العقوبتين معاً[16].

أركان الجريمة:

– أن يتوصل الجاني لخداع شخص آخر عن طريق الاحتيال أو استخدام اسم كاذب أو انتحال صفة غير صحيحة.

– أن يكون ذلك بغرض الحصول على مال لنفسه أو لغيره على مال أو سند أو توقيع السند.

– أن يتم ذلك عن طريق شبكة الحاسوب أو ما في حكمها[17].

الاحتيال هو الغش والخداع، وقد عرفه القانون الجنائي السوداني لسنة 1999م في المادة 178 منه بأنه التوصل لخداع الشخص بأي وسيلة بغرض الحصول على كسب غير مشروع لنفسه أو تسبيب خسارة غير مشروعة للمجني عليه أو لغيره[18]. إما انتحال الشخصية ينقسم إلى قسمين:

– انتحال شخصية الفرد وهو من الجرائم القديمة.

– انتحال شخصية المواقع ويعتبر هذا حديثاً نسبياً ويتم ذلك ضمن نظم الاتصال[19].

وعناصر جريمة الاحتيال هي:

– أن يمارس الجاني الخداع بأي طريقة.

– أن يتم بناء على ذلك الخداع تسليم مال.

– أن يتم تسليم المال بناء على رضاء المجني ولكن رضا معيباً.

– القصد الجنائي[20].

ظهر نوع جديد من أنواع الاحتيال في كثير من القضايا يكيف ضمن القضايا المدنية ولكن هنالك رأي لمولانا محمد الطيب سرور [21] أنها من ضمن القضايا الجنائية وأدرجه تحت المادة (11) وقال أنها تسويق هرمي وليس شبكي.

ج) الحصول على أرقام بطاقات الائتمان:

تعريف بطاقة الائتمان: هي عبارة عن بطاقة مستطيلة من البلاستيك المقوى تحمل اسم المؤسسة المصدرة لها، وشعارها وتوقيع حاملها بشكل بارز على وجه الخصوص رقمها واسم المصدرة لها، وشعارها وتوقيع حاملها، ورقم حسابه وتاريخ انتهاء صلاحيتها [22]. والبطاقات الائتمانية لها أنواع متعددة هي:

- بطاقات السحب الآلي، وهي تخول لحاملها إمكانية سحب مبالغ نقدية من حسابه بحد أقصى متفق عليه من خلال أجهزة الحسب الآلي للنقود.

- **بطاقة الشيكات:** وبمقتضاها يتعهد البنك مصدر الشهادة بأن يضمن سداد الشيكات وبمقتضاها يتعهد البنك مصدر الشهادة بأن يضمن سداد الشيكات التي يحررها العميل من هذا البنك وفقاً لشروط إصدار هذه البطاقة.

- **بطاقة الوفاء:** وهي بطاقة تخول لحاملها الحق في الحصول على تسهيل ائتماني مقابل سداد قيمة السلع والخدمات التي يحصل عليها من بعض المحالات التجارية يوجب اتفاق خاص مع الجهات المصدرة لها[23].

جاء في قانون جرائم المعلوماتية السوداني لسنة 2007م المادة (12) كل من يستخدم شبكة المعلومات أو أحد أجهزة الحاسوب وما في حكمها للوصول إلى أرقام أو بيانات البطاقات الائتمانية أو ما في حكمها بقصد الحصول إلى بيانات الغير أو أموالها وما تتيحه تلك البيانات والأرقام من خدمات يعاقب بالسجن مدة لا تتجاوز خمس سنوات أو بالغرامة أو العقوبتين معاً[24] فالاستيلاء على بطاقات الائتمان أمر ليس بالصعوبة بمكان إطلاقاً.

فلصوص بطاقات الائتمان عبر الإنترنت مثلاً يستطيعون الآن سرقة مئات الألوف من أرقام البطاقات في يوم واحد من خلال شبكة الإنترنت،

ومن ثم بيع هذه المعلومات للآخرين، وقعت بالفعل عدة حوادث ومن ذلك حادثة شخص ألماني قام بالدخول غير المشروع إلى أحد مزود الخدمة بإفشاء أرقام تلك البطاقات ما لم يستلم فدية وقد تمكنت الشرطة الألمانية من القبض عليه.

ويتعدى الأمر المخاطر الأمنية التي تتعرض لها بطاقات الائتمان فنحن في ثورة نقدية تعرف باسم النقود الإلكترونية التي يتنبأ لها إن تكون مكملة للنقود الورقية والبلاستيكية (بطاقات الائتمان) وأن يزداد الاعتماد عليها والثقة بها كما أن هناك الأسهم والسندات الإلكترونية المعمول بها في دول الأوربية والتي أقر الكونجرس الأمريكي التعامل بها في 1990م. وبالتالي فإن التعامل معها من خلال الإنترنت سيواجه مخاطر أمنية ولا شك في ذلك[25].

الأساليب الإجرامية للاستيلاء على أرقام بطاقات الائتمان:

من صور استخدام هذه البطاقات ما يلي: التلاعب في مبالغ قسائم أو تقديم الخدمة بزيادتها عن المطلوب وذلك باستغلال عدم معرفة الأجنبي باللغة التي تكتب بها الإشعارات.

تزوير وتزيف بطاقات الائتمان وهو أسلوب يقوم به غالباً الأجانب القادمون من خارج البلاد، وذلك من خلال تزييف بعض بياناتها خصوصاً في النوع العادي من البطاقات[26].

وعليه يمكن القول إن جرائم السطو على البطاقات الائتمانية محرمة شرعاً وقانوناً حيث تصنف ضمن جرائم السرقات، فالشريعة ترغب في

المحافظة على أموال الناس وصيانتها من كل اعتداء غير مشروع يهدد الأمن والاستقرار.

د) الانتفاع دون وجه حق بخدمات الاتصالات:

أورد المشرع السوداني في المادة (13) من قانون جرائم المعلوماتية لسنة 2007م: كل من ينتفع دون وجه حق بخدمات الاتصال عن طريق شبكة المعلومات أو أحد أجهزة الحاسوب أو ما في حكمها، ويعاقب بالسجن مدة لا تتجاوز أربع سنوات أو بالغرامة أو بالعقوبتين معاً[27].

هذه المادة تجرم الانتفاع غير المشروع بخدمات الاتصال عن طريق شبكة المعلومات أو ما في حكمها، ويشمل الانتفاع غير المشروع الهاتف السيار سواء عن طريق سرقة البطاقات نفسها أو تخمين الأرقام وتدوينها وإرسالها للشركة فإذا كان التخمين صحيحاً تم إدخال القيمة تلقائياً هو أمر صعب ولكنه ممكن الحدوث كما يمكن تصور أن يتم الحصول الأرقام من عامل بالشركة المعينة فإذا قام ببيعها لآخرين وكانوا على علم بذلك يكونوا قد ارتكبوا هذه الجريمة وتعتبر مخالفة للمادة 23 والتي جاءت تحت عنوان التحريض أو الاتفاق أو الاشتراك، كما يشمل هذه الانتفاع غير المشروع بخدمات القنوات القضائية المشفرة، فضلاً عن خدمات الإنترنت[28].

ثالثاً: جرائم النظام العام والآداب:

أدى انفتاح الإنترنت على المستوى العالمي إلى ظهور مساحة لممارسة مختلف أنواع الجرائم الممكنة والمحتملة، ومنها المتعلقة بالآداب العامة والأخلاق.

من جرائم الآداب عبر الإنترنت:

1. المواقع الإباحية: ويندرج تحت هذا البند ارتياد المواقع الإباحية وأصبحت مشكلة مدمرة ولا تقتصر على مجتمع من دون الآخر وهي من المحظورات الشرعية التي حرص الشرع على تحريمها، لقد أمرنا بغض البصر وحرم النظر إلى المحرمات.

2. إشانة السمعة: أورد قانون جرائم المعلوماتية في المادة (17) كل من يستخدم شبكة المعلومات أو أحد أجهزة الحاسوب أو ما في حكمها لإشانة السمعة يعاقب بالسجن مدة لا تتجاوز سنتين أو بالغرامة أو بالعقوبتين معاً[29].

تحكم هذه المادة إشانة السمعة عن طريق شبكة المعلومات أو ما في حكمها ولم يحدد النص معيار إشانة السمعة على خلاف القانون الجنائي لسنة 1999م حيث نصت المادة 159 منه يحدد إشانة السمعة تكون بأن: ينقل الشخص أو يروى لآخر وقائع منسوبة لشخص آخر بقصد الإساءة لسمعته، ووضعت المادة استثناءات لا تجعل الفعل في سياق إجراءات قضائية بقدر ما تفتضيه أو كنشر لتلك الإجراءات، أو كانت له أو لغيره شكوى مشروعة يعبر عنها أو مصلحة مشروعة يحميها وكان ذلك لا يتم بإسناد تلك الوقائع للشخص المعني، أو إذا كان الفعل في شأن من يرشح نفسه لمنصب عام أو يتولاه تقويماً لأهليته أو أدائه بقدر ما يقتضيه الأمر، أو أن يكون الفعل في سياق النصيحة لصالح من يريد التعامل مع ذلك الشخص أو للصالح العام، أو إسناد الوقائع بحسن نية لمن اشتهر بسلوك معين وغلب عليه أو كان مجاهراً به، في حين جاء نص المادة معمماً بدون أي تفرقة بين فعل وآخر، وهذا يعني خضوع الفعل للتقييم من قبل المحكمة للتفتيش عن القصد الجنائي للمتهم عند نشره للوقائع لمعرفة ما إذا كان القصد[30].

رابعاً: جرائم التحريض أو الاتفاق أو الاشتراك:

نصت المادة 1/23 من جرائم المعلوماتية لسنة 2007م "يعد مرتكباً جريمة التحريض كل من حرض أو ساعد أو اشترك أو اتفق مع الغير على ارتكاب جريمة من الجرائم المنصوص عليها في هذا القانون، وإن لم تقع الجريمة يعاقب بنصف العقوبة المقدرة لها"[31].

وأركان جريمة التحريض هي:

- أن يحصل اعتداء أو اتفاق أو مساعدة.
- يكون موضوعه جريمة.
- القصد الجنائي[32].

خامساً: جرائم التجسس الإلكتروني:

تطورت عمليات التجسس طبقاً لما يسود في المجتمع من تطورات علمية وتكنولوجية، فمثلاً اختراع الإنسان جهاز ليتجسس على أعدائه، ومعرفة كافة تحركاتهم، ثم حدث تطور كبير وهو اختراع الأقمار الصناعية، التي تقوم بتصوير الإنسان والآلات الحديثة والمدنية، وكل ما هو فوق الأرض، يتم تصويره كل فترة زمنية معينة لمعرفة التحركات التي تتم الآن، وفي ظل التطور التقني الهائل الذي نعيشه، فقد أصبح هناك ما يعرف بالتجسس الإلكتروني [33]. والملاحظ أن جرائم التجسس الإلكتروني أخطر الجرائم لأن التجسس يكون في الخفاء.

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، لأنها لا تترك أثراً خارجياً.

3. إحجام الشركات والمؤسسات في المجتمع عن الإبلاغ.

4. هذه الجرائم لا تعرف الحدود بين القارات على النظام المعلوماتي[34].

5. تعتبر جرائم الحاسب الآلي من أكثر الجرائم التي تثير مشكلات الاختصاص على المستوى المحلي والدولي.

الاختصاص وتبادل الأدلة الجنائية وتسليم المجرمين. إن الأمر في حاجة إلى قوانين جنائية أكثر مرونة تواكب التعامل بالحاسب الآلي في مختلف مناحي الحياة[35].

المبحث الثاني

فتح الدعوى الجنائية والتحري فيها

المطلب الأول: فتح الدعوى الجنائية:

أولاً: تعريف فتح الدعوى الجنائية: الفت لغة: نقيض الإغلاق ويقال فتح الباب أزال قلقه[36].

فتح الدعوى الجنائية في القانون: وأورد المشرع السوداني في المادة (33): تفتح الدعوى الجنائية بناءً على علم لدى شرطة الجنايات العامة، أو وكيل النيابة، أو بناءً على ما يرفع إلى أيهما من بلاغ أو شكوى[37].

كيفية البلاغ عن جرائم الإنترنت:

لا نجد اختلافاً كبيراً عما هو الحال في الجرائم التقليدية، وإن كان يتمتع بنوع من الخصوصية تتماشى مع طبيعة هذه الجرائم.

فبمجرد تلقى مأمور الضبط القضائي أو جهة التحقيق المختصة بلاغاً يشير إلى ممارسة شخص معروف أو غير معروف أنشطة تندرج ضمن جرائم الإنترنت في مكان معروف وعلى أجهزة محددة وفق لغات برمجية معلومة، كتلقيه بلاغاً مثلاً فيه معلومات عن نشر فيروسات تخزينية عبر شبكة الإنترنت، أو بث صور إباحية عبر تلك الشبكة أو عن وجود مواقع أو صفحات خادعة أعدت للاحتيال على الناس، فإنه حينئذ تنعقد له جملة الاختصاصات السابقة.

والبلاغ هنا يتم عن طريق الإنترنت أي ما يسمى بالبلاغ الرقمي، وذلك إما عن طريق إرسال رسالة إلكترونية إلى عنوان البريد الإلكتروني للجهات المختصة بالتحقيق والتحري لإبلاغها عن وجود صفحات أو مواقع غير مشروعة، كإرسال رسالة إلكترونية مثلاً تتضمن التبليغ عن وجود موقع منشور فيه صور للاستغلال الجنسي للأطفال إلى عنوان البريد الإلكتروني للدرك الوطني الفرنسي باعتبار الجهة المختصة بالتحقيق والتحري عن تلك الجرائم في فرنسا أو على موقع شرطة إدارة مكافحة جرائم الحاسبات وشبكات المعلومات المخصص لتلقي البلاغات والشكاوي، وشبكات المعلومات المخصصة لتلقي البلاغات والشكاوي كالموقع الرسمي للإنترنت الأحداث الذي يوفر استمارة بيانات رقمية، للتبليغ عن مواقع أو خدمات أخرى للإنترنت (كالبريد الإلكتروني، منتديات الحوار والدردشة).

رابعاً: أوجه الاختلاف بين البلاغ عن الجرائم التقليدية والبلاغ عن جرائم المعلوماتية وبالرغم من أن البلاغ عن تلك الجرائم يتشابه في نقاط كثيرة مع البلاغ عن الجرائم التقليدية، إلا أن جرائم المعلوماتية لا تصل عادة إلى علم السلطات المعنية بالصورة العادية وذلك لصعوبة اكتشافها بواسطة

الأشخاص العاديين، فهي كثيراً ما تبقى مستترة، وخصوصاً عندما تقع على أموال المؤسسات المالية، والشركات المالية، والشركات التجارية، إذا ترددت هذه الأخيرة في التبليغ عنها خوفاً على سمعتها.

الجهات المختصة بتلقي البلاغ عن جرائم الإنترنت والإجراءات الشرطية التي تتبع ذلك البلاغ.

الجهة المختصة في السودان هي نيابة التحقيقات الجنائية والجرائم المستحدثة.

الشكوى في جرائم المعلوماتية:

لا تختلف أحكام الشكوى في الجرائم التقليدية عن تلك الجرائم المعلوماتية، إذ لا يجوز للجهات المختلفة تحريك الدعوى العمومية في تلك الجرائم إلا بعد تقديم شكوى من المجني عليه أو المتضرر منها أو وكيلة الخاصة ضد المتهم.

فإنه كثيراً ما يصعب تحديد الجاني أو المتهم شخصياً في هذا النوع من الجرائم. وهذا ما أدى ببعض الفقه إلى ترتيب مسئولية مزود الدخول أو خدمات الإنترنت عن تلك الجرائم مستندين في ذلك على مبدأ افتراض مسؤولية الغير[38].

المطلب الثاني: تعريف التحري:

هو مجموعة من الإجراءات تستهدف التنقيب عن الأدلة بشأن جريمة ارتكبت وتجميعها ثم تقديرها لتحديد مدى كفايتها لإحالة المتهم إلى المحاكمة[39].

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[40].

مكان التحري: هو المكان الذي تمارس فيه النيابة، والشرطة التحري ثم مكان المحاكمة هي الحدود الجغرافية، والحدود المكانية، اختلفت المذاهب الفقهية والتشريعية في العالم في قواعد الاختصاص[41].

المبحث الثالث

إجراءات التحري في الجريمة المعلوماتية

المطلب الأول: تدريب الكوادر والاستعانة بالخبرة الفنية:

أولاً: تدريب الكوادر:

إن 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 الإلكترونية – 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[42].

ثانياً: الخبرة الفنية:

1/ تعريف الخبرة:

أ. تعريف الخبرة لغة: الخبرة بمعنى كلام ناقص والخبير من أسماء الله عز وجل بمعنى العالم بما كان وما يكون على حقيقته، والخابر المختبر المجرب والخبرة: العلم بالشيء[43].

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[44].

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، ما لم يتفق الخصوم على اختيارهم[45].

التي يجب استيعابها وفهمها واستخلاص النتائج منها للفصل في الدعوى عند الاقتضاء لذلك، فيجوز للحكمة الاستعانة بشهادة الخبرة وآراء

الخبراء وتندب لذلك الغرض من يقوم بهذه المهمة من الخبراء، ويكون تحديدهم بواسطة المحكمة، غير أنه يجوز للخصوم في الدعوى الاتفاق على اختيارهم.

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

المطلب الثاني: المعاينة:

أولاً: تعريف المعاينة:

من العين والعين حساسة البصر والرؤية، وتكون للإنسان وغيره من الحيوان [46] قال ابن سيدة [47] العين الذي يبعث لتجسس الخبر والمعاينة النظر، وقد عاينه معاينة وعياناً[48].

المعاينة قانوناً: 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[49].

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 تقتضى ذلك، وأن ينتقل فوراً لمكان الوقائع ليتحرى فيها..."[50].

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[51] 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 وثبتها قبل أن تزول آثارها، أو تتغير معالمها[52].

نص المادة 61 من قانون الإثبات السوداني لسنة 1994م، على الآتي:(يجوز للمحكمة من تلقاء نفسها أو بناء على طلب أحد الخصوم، أن تقرر الانتقال لمعاينة الشيء المتنازع فيه، ويجوز لها أن تستعين بمن ترى لزوماً لسماع من الخبراء أو الشهود).

تحدد المحكمة محضراً تبين فيه جميع ملاحظاتها، دون أن تثبت انطباعاتها عن المعاينة أو رأيها الخاص.

يعتبر محضر المعاينة جزءً من البينة التي تؤسس عليها المحكمة حكمها[53].

يرى الباحث أن المعاينة هي أقوى وسائل إثبات هذه الجرائم الخطيرة التقنية تجرى الملاحظة والفحص المباشر لمكان الجريمة المتعلقة بالإنترنت، ويتطلب ذلك سرعة الانتقال مكان الجريمة، حتى لا يتطرق الشك إلى الدليل المستفاد منها حتى لا يتمكن الجاني من إزالة بعض الآثار المادية، التي تفيد في كشف الحقيقة وبعد معاينة مسرح الجريمة تقوم المحكمة بحجز الأقراص الصلبة الخاصة بالخصم، ويجوز للنيابة الانتقال والمعاينة ثم سماع الشهود بعد ذلك، وكل هذا يتطلب أن يكون من يقوم بهذه الإجراءات ملماً بالكمبيوتر والإنترنت ومتعلقاتها، وأن يكون مع المحكمة أو النيابة أو الشرطة خبير[54].

ثانياً: المعاينة في جرائم المعلوماتية:

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 لمكانه.

2. العناية البالغة بملاحظة الطريقة التي تمت بها إعداد النظام والآثار الإلكترونية الخاصة بالتسجيلات الإلكترونية التي تتزود بها شبكات المعلومات بموافقة موقع الاتصال ونوع الجهاز الذي تم عن طريقة الولوج إلى 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 للمنشأة 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 الإلكتروني من أي مجال مغناطيسي يمكن أن تسبب في محو البيانات المسجلة[55].

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[56].

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

– توفير معلومات مسبقة عن مكان الجريمة، ونوع وعدد خطة الأجهزة المتوقع مداهمتها، وشبكات الاتصال الخاصة.

– إعداد فريق التفتيش من المختصين، على أن يكون الفريق مرفقاً بالأمر القضائي اللازم للقيام بالتفتيش[57].

ثالثاً: مسرح الجريمة الإلكترونية: عند تلقي بلاغ إحدى الجرائم الإلكترونية، 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 الإلكترونية جريمة مستمرة. خاصة إذا كانت جريمة اقتصادية. وقد يكون مسرح الجريمة الإلكترونية مثل مسرح الجرائم الأخرى عندما يكون الهدف منها التخزين أو إتلاف البرامج أو تزويد المستندات والوثائق أو المباني والمنشآت، 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.

يرى الباحث أن المعاينة في الجريمة المعلوماتية، تختلف عن المعاينة في الجريمة التقليدية، لأن المعاينة في الجريمة التقليدية غالباً مسرح الجريمة يكون محتفظاً بآثاره المادية من بصمات وآثار دماء أو غير ذلك. ولكن مسرح الجريمة التقليدية غالباً ما يكون 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 عليه 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، لأنه ما ينتج عنه أدلة تؤيد نسبة الجريمة إلى المتهم[58].

ويرى الباحث إن تفتيش نظام الحاسوب والإنترنت من أخطر المراحل حال اتخاذ الإجراءات الجنائية ضد مرتكب الجريمة الإلكترونية، لكون محل التفتيش في الحاسوب ولأن 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.

ويمكن تعريف تفتيش نظم الحاسوب: بأنه إجراء من إجراءات التحقيق يهدف إلى البحث في داخل نظام حاسوبي معين بأذن قضائي مسبق، سواء كان هذا النظام مكوناً من حاسوب واحد أو عدة حواسيب مرتبطة فيما بينها بشبكة في محل له حرمة منحه إياه القانوني، والعرض استخراج أدلة معلوماتية متمثلة بالمعلومات أو البيانات والتي تساعد في كشف الحقيقة في جريمة وقعت وجاد التحقيق فيها[59].

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 ما زالت تظهر هي ضبط البيانات والبرمجيات.

يقصد به قانون الإجراءات الجنائية وضع اليد على شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبيها ومن حيث طبيعية القانونية قد يكون من إجراءات الاستدلال أو التحقيق والضبط بطبيعته وغايته لا يريد إلا على الأشياء أما الأشخاص فلا يصحون محلاً للضبط بالمعنى الدقيق[60].

المطلب الخامس: الشهادة:

نص المادة 23 من 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[61].

الشاهد في الجريمة المعلوماتية هو الفني صاحب الخبرة والتخصص في تقنية وعلوم الحاسب الإلكتروني والذي تكون لديه 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 المعلوماتي وذلك تمييزاً له عن الشاهد التقليدي[62].

المطلب السادس: الاستجواب:

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، والبنيات القائمة ضده،

ومطالبة بالرد عليها، إما بإنكارها، وإثبات فسادها، وأما بالتسليم بها، وما يتبعه، من اعتراف بالجريمة [63] وهو أيضاً إجراء من إجراءات التحقيق تتم فيه مناقشة المتهم فيما هو منسوب إليه من جرم ويطلب منه على الأدلة القائمة ضده أما بتنفيذها أو التسليم بها[64].

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[65].

المبحث الرابع

المحاكمة في جرائم المعلوماتية

المطلب الأول: مفهوم المحاكمة:

هي آلية تهدف إلى الفصل في براءة المتهم أو إدانته وفقاً للأصول القانونية. والمحكمة المختصة في جرائم المعلوماتية هي محكمة الملكية الفكرية.

مقابلة قاضي محكمة جرائم المعلوماتية[66]:

إن محكمة جرائم المعلوماتية هي واحدة في السودان ومقرها في الخرطوم وهي أول محكمة في أفريقيا وفي الوطن العربي وأنشئت في 2015/2/26م، وتم تعيين لها قاضي مختص بقرار من المحكمة العليا، وأكثر القضايا هي جريمة إشانة السمعة وجرائم النشر الإلكتروني.

وأيضاً ظهرت جريمة جديدة جداً هي جريمة التسويق الشبكي وتدرج في المادة (11) من قانون جرائم المعلوماتية لسنة 2009م وهي في الأصل جرائم تسويق هرمي.

المطلب الثاني: التطبيقات القضائية المعاصرة لجرائم المعلوماتية:

أولاً: بعض الأحكام القضائية في جريمة إشانة السمعة

محمد التاي أحمد المصطفى – قرية الدوينب / الحصاحيصا ضد عز الدين علي أحمد الجاك الصراف – قرية الدوينب / الحصاحيصا.

تتلخص الوقائع في أن الشاكي أبلغ النيابة بموجب عريضة أن صاحب دكان ود النعيم ومجموعته التي تسمى مجموعة التغيير وهي مجموعة معارضة لكل تعرضوا إلى بالإساءة الشخصية ووصفوني بالخداع والتطرق والعمالة وانعدام الضمير والدكتاتورية والفساد بالجنة الشعبية لقرية الدوينب.

فقد أفاد الشاكي أن هناك خلاف سياسي بيني وبين المتهمين وسموا أنفسهم مجموعة التغيير بقيادة المتهم الأول والخلاف كان هدفه تغيير رئيس اللجنة الشعبية[67].

وقام المجلس التشريعي بمحلية الحصاحيصا بحل اللجنة للخلاف وتم عمل انتخابات وتم انتخابي رئيساً، وبعد اختياري رئيساً أصبحت هذه المجموعة تقود عمل مضاد إساءة لسمعتي وتجريمي من خلال تواجدهم في دكان النعيم (المتهم الثالث) وكتابة المنشورات على صفحة التواصل الاجتماعي (الفيس بوك) الموقع الأول باسم عز الدين علي (المتهم الأول) والموقع الثاني باسم أبناء قرية الدوينب بالمملكة العربية السعودية والموقع الثالث باسم الدوينب نيوز وموقع غريب الدنيا[68].

وصدر الحكم كالآتي:

أ. تشطب الدعوى الجنائية في مواجهة المتهم عز الدين علي أحمد لسبق محاكمة في نفس موضوع هذه الجريمة.

ب. إدانة المتهم محمد الحاج الصراف بالمادة 159 من القانون الجنائي.

بعد مراعاة للظروف المخففة والمشددة استناداً لنص المادة (39) من القانون الجنائي ثم الحكم المتهم بالسجن شهر مع وقف التنفيذ وعليه المتهم يعول أسرة كبيرة ومغترب وليس لديه سوابق والشاكي والمتهم من قرية واحدة وعليه أرى تطبيق عقوبة السجن مع استعمال سلطاتنا بموجب المادة بموجب المادة 17 من قانون الإجراءات الجنائية وإيقاف العقوبة[69].

محاكمة/سراج الدين النعيم وآخر

النمرة: م.ع/ط.ج/2014/234م

الحكم

هذا طعن بالنقض مقدم من الأستاذ محمد الطيب نيابة عن الطاعن "الشاكي" في مواجهة حكم محكمة استئناف الخرطوم بالرقم 60/تجاري

2013م بتاريخ 2014/1/6م والذي علم به الطاعن بتاريخ 2014/1/29م وقدم هذا الطعن بتاريخ 2014/2/8م وخلال القيد الزمني الوارد في نص المادة 184 من قانون الإجراءات الجنائية لسنة 1991م.

موجز الوقائع أن الشاكي أبلغ يفيد بأن المتهم الأول الكاتب الصحفي بجريدة الدار وبصحيفة النيلين الإلكترونية أشان سمعة أسرته وتم القبض علي المتهم الأول وقادت التحريات إلى المتهم الثاني والذي كان زوج لأحد أخوات الشاكي وبعد اكتمال التحريات ووضع الأوراق أمام المحكمة للمحاكمة سمعت قضية الاتهام واستجوبت المتهمين وأصدرت أمراً قضي بشطب الدعوى الجنائية وأمرت بالإفراج عن المتهمين وعند الطعن لدى محكمة الاستئناف أيدت قضاء محكمة الموضوع وكان هذا الطعن الماثل.

ينعى محامي الطاعن على قضاء محكمة الموضوع المؤيدة بواسطة محكمة الائتناف مخالفته للقانون ووزن البيانات حيث أوضح أن المتهم الثاني طليق شقيقة الشاكي وتوعد بفضحها ويرى أن سوء النية متوفر. والنشر تم بعبارات واضحة الدلالة والمقصود منها هو شقيقة الشاكي ولهذا طالب بإلغاء قضاء المحاكم الأدنى.

وجرائم المعلوماتية تحاكم بموجب قانون جرائم المعلوماتية لسنة 2007م حيث كل من يستخدم شبكة المعلوماتية أو أحد أجهزة الحاسوب أو ما في حكمها في إشانة سمعة أي شخص يرتكب جريمة ويحاكم بموجب المادة (17) من جرائم المعلوماتية لسنة 2007م.

ومن خلال الاطلاع على النشر الذي تم اتضح أن النشر لم يكن يقصد به الشاكي إنما أنصب على شقيقة الشاكي وجاءت الإشارة إلى أن الشاكي شقيقها وفي الخدمة الشرطية.

ومن أقوال الشاكي أوضح أن الضرر واقع على الأسرة وليس لديه توكيل من الأسرة للمقاضاة وبالتالي تنعدم الصفة في فتح الدعوى الجنائية، ولم يثبت في النشر إشانة لسمعة الشاكي وجاء شطب الدعوى الجنائية تطبيقاً صحيحاً للقانون ولم أجد أي مخالفة للقانون في قضاء محكمة الموضوع المؤيد بواسطة محكمة الاستئناف ويتعين شطب الطعن[70].

ثانياً: أحكام قضائية في جريمة التسويق الشبكي:

مرتضى الحاج عبدالله ضد محمد عباس القاسم

تتلخص وقائع القضية في الشاكي مرتضى الحاج عبدالله بفتح هذا البلاغ بموجب عريضة من النيابة مضمون شكواه أن المتهم محمد عباس القاسم قد احتال عليه واخذ منه مبلغ (7 ألف جنيه) مقابل إشراكه هو ونسيبه حمزة أحمد في شركة تسمى (ماي رأيت) بعد اكتمال التحري أحيلت الدعوى للفصل بعد أن وجهت تهمة للمتهم أعلاه بموجب المادة (11) من قانون جرائم المعلوماتية لسنة 2007م: كل من يتوصل عن طريق شبكة المعلومات أو أحد أجهزة الحاسوب وما في حكمها عن طريق الاحتيال أو استخدام اسم كاذب أو انتحال صفة غير صحيحة، بغرض الاستيلاء لنفسه أو لغيره على مال أو سند أو توقيع للسند، يعاقب بالسجن مدة لا تتجاوز أربع سنوات أو بالغرامة أو بالعقوبتين معاً [71] المتهم لم يذكر استلامه المبلغ أعلاه من الشاكي نظير اشتراك الشاكي ونسيبه في شركة ماي رايت وهو أي المتهم هو الذي شرح للشاكي كيفية الدخول في الشركة ومشاهدة الإعلانات والحصول على إرباح نظير تلك المشاهدة.

بعد اكتمال مناقشة عناصر مادة الاتهام تقرر إدانة المتهم محمد عباس القاسم دون أدنى شك معقول بموجب المادة (11) من قانون جرائم المعلوماتية لسنة 2007م.

بالنسبة للتعويض لم يتم سداد الرسوم وبالتالي تحتفظ المحكمة للشاكي في المطالبة به مدنياً لاحقاً[72].

محاكمة/ إبراهيم حسن إبراهيم وآخر

النمرة: م.ع/ط.ج/2014/739م.

الحكم:

أدين المتهم أعلاه أمام محكمة جنايات كرري ومعه المتهم الثاني حسن علم الدين حسن بموجب المادة 178 من القانون الجنائي لسنة 1991م وحكمت على كل واحد منهما بالجسن لمدة عام مع وقف التنفيذ استناداً للمادة 170 من قانون الإجراءات الجنائية لسنة 1991م ووضعها تحت اختبار حسن السير والسلوك لمدة ستة أشهر اعتباراً من 2014/4/30م مع إلزامهما بأن يدفعا بالتضامن والانفراد للشاكية نهي طه فتح الرحمن مبلغ أثنا عشر ألف جنيه يحصل بالطريق المدني.

استؤنف هذا الحكم أمام محكمة استئناف أم درمان فأصدرت حكمها بالنمرة م ع/ ا س ج/ 783 / 2014م بتأييد الحكم ومن ثم كان هذا الطعن بالنقض المقدم لنا من الأستاذ/ عوض بشير أحمد بابكر المحامي نيابة عن المحكوم عليهما فنقبله شكلاً لتقديمه خلال التقيد الزمني المنصوص عليه في المادة 184 من قانون الإجراءات الجنائية لسنة 1991م ونلخص أسبابه في الآتي:

1. وقائع الدعوى تدخل تحت مسمى التسويق الشبكي وهو عبارة عن تجارة عبر الإنترنت والشبكات العنكبوتية وقد أنشأت له الدولة وزارة تنظيم العمل فيه (وزارة العلوم والاتصال) وأصدرت قانوناً يحمى العمل فيه ويعاقب مرتكبي الجرائم عن طريقه (قانون جرائم المعلوماتية 2007م بل أنشأت كذلك له نيابة متخصصة للتحري في المخالفات التي ترتكب بشأنه وصدرت أحكام من المحاكم الجنائية العامة شطبت الأحكام الصادرة من المحاكم الأدنى درجة وكذلك من المحكمة العليا.

2. تجاهل الحكم المطعون فيه تفسير وفهم قانون جرائم المعلوماتية لسنة 2007م مع عدم الاختصاص حيث جاء في مذكرة الحكم، أن المدانين لم يذكرا أن هذا العمل يندرج تحت قانون جرائم المعلوماتية وهذا فهم خاطئ.

3. لم تستطع المحكمة تكييف القانون في فعل المدان الثاني حيث لم يثبت أنه له أي دور تجاه الشاكية ولم تتهمه بأي شيء خلاف أنه المسئول الأول ولم تقم البينة على ذلك.

4. ما ورد في الحكم بأن الشركة شركة وهمية وغير مسجلة، يدل على ضعف الحكم وعدم مواكبته لتطورات القوانين في التوسع في استخدام التقنية الإلكترونية وما تسعى إليه الدولة في تأسيس الحكومة الإلكترونية.

خلص الأستاذ من هذه الأسباب إلى إلغاء الحكم المطعون فيه والعقوبة الصادرة بموجبه ورد مبلغ الكفالة المالية.

قبل الخوض في الموضوع، أرى أن الخص وقائع الدعوى الجنائية في الآتي:

الشاكية نهلة طه فتح الرحمن وهي محامية كانت قد قبلت دعوة وجهت لها من المدعو محمد إبراهيم حاج الطيب الذي يعمل سائقاً ويمت بصلة

قرابة للمتهم الأول إبراهيم حسن إبراهيم للانضمام لعضوية شركة تسمى T.V.I Express تي.في.أي اكسبريس تعمل في مجال التسويق الشبكي عبر الأجهزة الإلكترونية وأنها بناء على هذه الدعوة والعرض المقدم إليها، سلمت الشاكية مبلغ (12) ألف جنيه لشاهد الاتهام محمد إبراهيم الذي قام بدوره بتسليم المبلغ للمتهم الأول الذي قام بتسليمه للمتهم الثاني والمتهمان الأول والثاني يقران باستلام المبلغ الذي دفعته الشاكية للمدعو محمد إبراهيم وأن المبلغ قد أودع في حساب الشركة تي. في. أي اكسبريس T.V.I Express كما مدون بأقوالهما بالمحضر على الصفحات من 49-57 بالنسبة للمتهم الأول ومن ص 58-61 للمتهم الثاني وعلى ضوء ذلك حركت الشاكية إجراءات هذا البلاغ وقدم للمحاكمة بعد الفراغ من التحريات فكانت الأحكام المشار إليها في مقدمة المذكرة.

أعود للموضوع وأقول أنه من إطلاعي على الأوراق وأسباب الطعن، يوجد ضمن الأوراق المرافقة مع الطعن حكم صادر من المحكمة القومية العليا بالنمرة م ع/ ط ج / 743 / 2013م بتاريخ 2013/11/12م قد الغي الحكم الصادر من محكمة أم درمان الجنائي لسنة 1991م وحكم عليها بالسجن لمدة سنة اعتباراً من 2013/4/17م مع وقف التنفيذ إعمالاً لنص المادة 170 من قانون الإجراءات الجنائية لسنة 1991م والغرامة مبلغ مئتي جنيه وبالعدم السجن لمدة شهر وأن تدفع المدانة للشاكية مبلغ 26ألف جنيه يحصل بالطريق المدني وذلك لأن وقائع الدعوى تشير إلى جرائم المعلوماتية وأن الشارع قد أفراد لمثل هذه الجرائم قانوناً خاضاً هو قانون جرائم المعلوماتية لسنة 2007م وشكل له محكمة ونيابة خاصة وبالتالي يخرج

اختصاص نظر هذه الجرائم أمام المحكمة الجنائية رغم أن القانون الجنائي قد نص على عقوبة جريمة الاحتيال.

وحيث إن وقائع هذه الدعوى مشابهة للدعوى التي أمامنا، وحتى لا تصدر أحكام متباينة من المحكمة القومية العليا، واستناداً إلى هذه السابقة، أرى إلغاء الحكم الصادر من محكمة الموضوع المؤيد من محكمة الاستئناف بالحكم محل هذا الطعن وأن تحال الأوراق للنيابة المختصة بالخرطوم لإحالتها للمحكمة المختصة بالخرطوم.

عليه وتأسيساً على هذه الأسباب، أرى إذا وافق الزميلان المحترمان أن يكون قرارنا هو إلغاء الحكم المطعون فيه المؤيد لحكم محكمة الموضوع وأن تحال الأوراق للمحكمة المختصة بالخرطوم لنظر الدعوى وفق موجهات هذا الحكم[73].

الخاتمة:

الحمد لله رب العالمين الذي وفقني لإكمال الترتيبات العلمية لمظاهر التقاضي في الجرائم الإلكترونية والتي تبدو معالمها واضحة من خلال المخرجات الآتية:

أولاً: النتائج:

1/ مما سبق يظهر لنا وجود عدة صعوبات تكتنف إجراءات الجريمة المعلوماتية والتي تتمثل في عدة أمور منها:

– سهولة محو الأدلة وتدميرها.

– استعمال وسائل مختلفة للتحايل وإخفاء الأدلة بوسائل حماية وبرمجيات خاصة.

– التكاليف العالية التي تكتنف عمليات التحري عبر الإنترنت والأجهزة المتخصصة.

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

– أحياناً تكون المواقع والبرمجيات معدة 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/ أظهر البحث أن هناك قصوراً في الكثير من التشريعات الجنائية الإجرائية في مواجهة ظاهرة الإجرام الإلكتروني، فما زال الكثير منها يخضع هذه الجرائم للنصوص التقليدية.

4/ يتميز البلاغ في جرائم الإنترنت بأنه يقيد في الغالب ضد مجهول.

5/ في السودان تم تشكيل الأجهزة المختصة في جرائم المعلوماتية "شرطة، نيابة، محكمة".

6/ أن المعاينة في الجريمة المعلوماتية لا تتمتع بنفس الدرجة من الأهمية التي تتمتع بها في مسرح الجريمة التقليدية وذلك للأسباب التالية: قلة الآثار المادية المختلفة 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.

7/ 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.

8/ أن المراقبة الإلكترونية على الشبكات هي وسيلة لضبط المراسلات الإلكترونية عبر الإنترنت واعتراض البيانات التي تمر من خلال الشبكة، وإنها تحتاج إلى خبرة فنية للقيام بها.

ثانياً: التوصيات:

1/ ضرورة قيام المشرع السوداني بوضع تشريع خاص لمكافحة مثل هذه الجرائم يبين فيه الإجراءات الخاصة والجهات التحقيقية والقضائية الخاصة لمتابعة وتحري ومحاكمة المرتكبين، وخصوصاً حين نعلم أن عدم وجود مثل هذه التشريعات تمنع الأفراد عن التبليغ عن مثل هذا النوع من الجرائم.

2/ الممكن عدم إصدار قوانين جديدة ولكن تعديل النصوص الموجودة ولكن يجب في هذه الحالة شمول نظم الحاسوب والإنترنت بالأشياء التي يتم ضبطها وتعديل النصوص المتعلقة بصلاحيات المدعي العام.

3/ العمل على تأهيل القضاء على التعامل مع هذه الجرائم بصورة متخصصة وإفراد قضاة متخصصين بالقضايا الإلكترونية والمعلوماتية.

4/ استحداث وحدة خاصة في السلطة القضائية تتكفل بمهمة التحقيق والتحري في الجرائم المعلوماتية وتوفير الأجهزة والأدوات اللازمة وإعداد أفرادها بالصورة الكافية.

5/ محاولة التنسيق مع الجهات والهيئات الدولية لإصدار تشريعات موحدة 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.

6/ ضرورة إعداد كوادر قضائية للبحث والتحري والمحاكمة في نطاق الجرائم المعلوماتية مع استحداث قواعد مناسبة في مجال الإجراءات الجنائية بشأن التحري الجنائي.

7/ توعية وتشجيع المجني عليهم بالإبلاغ عن أي جريمة إلكترونية فور ملاحظتها.

هوامش البحث:

(1)جرائم المعلوماتية والإنترنت، عبدالله عبدالكريم، منشورات الحلبي الحقوقية، ط1، 2007م، ص17.

(2)الجريمة المعلوماتية في القانون السوداني، عزة علي محمد الحسن، الزيتونة للطباعة، د.ط، د.ن، 2009م، ص4.

(3)قانون جرائم المعلوماتية السودانية لسنة 2007م، المادة (4).

(4)قانون جرائم المعلوماتية السوداني لسنة 2007م المادة (4).

(5)شرح قانون جرائم المعلوماتية السوداني لسنة 2007م، إبراهيم قسم السيد، ط1، 2013م، ص8.

(6)قانون جرائم المعلوماتية السوداني لسنة 2007م، المادة (3).

(7)قانون جرائم المعلوماتية السوداني لسنة 2007م، المادة (3).

(8)قانون جرائم المعلوماتية السوداني لسنة 2007م، المادة (3).

(9)قانون جرائم المعلوماتية، عزة علي محمد الحسن، ص51.

(10)ألياف بصرية: تقنية لتصنيع خطوط لنقل إشارات الاتصالات تحل محل الخطوط المصنوعة من الأسلاك النحاسية. معجم مصطلحات الحاسب، المهندس علي يوسف، ص282.

(11)قانون جرائم المعلوماتية، عزة علي حسن، ص51.

(12)قانون جرائم المعلوماتية لسنة 2007م، المادة 6.

(13)قانون جرائم المعلوماتية السوداني لسنة 2007، المادة 10.

(14)شرح قانون جرائم المعلوماتية السوداني، إبراهيم قسم السيد، ص20.

(15)ثورة المعلومات وانعكاساتها على قانون العقوبات، د. محمد سامي الشواء، ص123.

(16)قانون جرائم المعلوماتية السودانية لسنة 2007، المادة 11.

(17)شرح قانون جرائم المعلوماتية السوداني، إبراهيم قسم، مرجع سابق، ص27.
(18)القانون الجنائي السوداني لسنة 1991م، المادة 178.
(19)أشهر جرائم الكمبيوتر والإنترنت، يوسف أبو الحجاج، دار الكتاب العربي، دمشق، القاهرة، ط1، 2010م، ص55.
(20)شرح القانون الجنائي السوداني لسنة 1991م، يس عمر يوسف، مرجع سابق، ص512.
(21)قاضي محكمة جرائم المعلوماتية بالسودان.
(22)الجرائم المعلوماتية، أحمد خليفة الملط، مرجع سابق، ص192.
(23)جرائم الكمبيوتر والإنترنت، عبدالفتاح بيومي، مرجع سابق، ص135.
(24)قانون جرائم المعلوماتية السوداني لسنة 2007م، المادة 12.
(25)أشهر جرائم الكمبيوتر والإنرتنت، يوسف أبو الحجاج، مرجع سابق، ص142 – 143.
(26)أساليب إجرامية بالتقنية ماهيتها – مكافحتها، مصطفى محمد موسى، دار الكتب القانونية، 2005م، مصر، 164.
(27)قانون جرائم المعلوماتية لسنة 2007م، المادة 13.
(28)شرح قانون جرائم المعلوماتية السوداني، إبراهيم قسم السيد، مرجع سابق، ص26.
(29)قانون جرائم المعلوماتية لسنة 2007م، المادة (17).
(30)شرح قانون جرائم المعلوماتية السوداني، إبراهيم قسم السيد، ص32–33.
(31)قانون جرائم المعلوماتية لسنة 2007م، المادة 23.
(32)النظرية العامة للقانون الجنائي السوداني لسنة 1991م، يس عمر يوسف، ص208.

(33)جرائم الإنترنت والحاسب الآلي وسائل مكافحتها، منير محمد الجنبيهي، ممدوح محمد الجنبيهي، مرجع سابق، ص86.

(34)الجريمة المعلوماتية، أحمد خليفة الملط، مرجع سابق، ص93-94.

(35)المجلة العربية للدراسات الأمنية والتدريب، تصدر عن أكاديمية نائف للعلوم الأمنية، العدد الثلاثون، رجب 1421هـ، 2000م، المجلد15، ص374.

(36)لسان العرب، ابن منظور، 461/2.

(37)قانون الإجراءات الجنائية لسنة 1991م، المادة (33).

(38)الوسيط في شرح قانون الإجراءات الجنائية، أحمد فتحي سرور، دار النهضة العربية، ط7، 1966م، ص491.

(39)شرح قانون الإجراءات الجنائية 1991م يس عمر يوسف سرور، دار النهضة العربية، ط7، 1966م، ص491.

(40)دليل التحري عبر شبكة الإنترنت، مصطفى محمد موسى، دار الكتب القانونية، مصر المحلة الكبرى، 2005م، ص22.

(41)قانون الإجراءات الجنائية، المادة 29.

(42)مرشد التحريات، محمد الأمين البشرى، ص144.

(43)لسان العرب، ابن منظور 10/5.

(44)المغني، ابن قدامة، 158/9.

(45)قانون الإثبات لسنة 1994م، المادة (30).

(46)لسان العرب، ابن منظور، مادة (عين)، ص301-302.

(47)ابن سيدة: هو عبدالله بن عبدالرحمن بن علي بن صابر،أبو المعالي الدمشقي، سير أعلام النبلاء، الذهبي، 1960/2.

(48)قانون الإثبات السوداني لسنة 1994م المادة 61.

(49)شرح قانون الإجراءات لمحمد ابوالعلا عقيدة، ط 2001م، دار النهضة العربية، القاهرة، ص426. شرح قانون الجنائية، محمد عيد الغريب، ط 2، 1996–1997م، دون ناشر، 794/1. نظام الإجراءات الجنائية، جلال ثروت، 2002م، دار الجامعة الجديدة القاهرة، ص 427. التحقيق الجنائي من الناحيتين العلمية والعملية، إبراهيم حامد طنطاوي، دار النهضة العربية، القاهرة، ط 1، سنة 1999م، ص165، نظام الإجراءات في المملكة العربية السعودية، أسامة عبدالله قايد، محمد علي كومان، دار النهضة العربية، ط1419هـ–1998م، ص195.

(50)قانون الإجراءات الجنائية السوداني لسنة 1991م، المادة 48.

(51)شرح قانون الإجراءات الجنائية، محمد عيد الغريب، مرجع سابق، ص 795. والتحقيق الجنائي من الناحيتين النظرية والعملية، إبراهيم حامد طنطاوي، ط1، 1999م، دار النهضة العربية، القاهرة، ص794.

(52)شرح قانون الإجراءات الجنائية محمد عيدالغريب، مرجع سابق، ص 795، وشرح الإجراءات الجنائية، محمد أبو العلا عقيدة، ص 426–427.

(53)قانون الإثبات السوداني لسنة 1994م، المادة 61.

(54)شرح قانون الإثبات السوداني لسنة 1994م، حاج آدم حسن الطاهر، مركز شريح القاضي للدراسات القانونية، السودان، ط10، 2009م، ص267–268.

(55)إجراءات التحري في الجرائم المعلوماتية، علي عدنان، ص 33–34.

(56)الدليل الإلكتروني، عائشة بنت قارة، ص154.

(57)التحقيق في جرائم الحاسب الآلي والإنترنت، محمد الأمين البشرى، ص357.

(58)الدليل الإلكتروني، عائشة بنت قارة، ص87.

(59)التفتيش في الجرائم المعلوماتية، سامي جلال فقهي حسين، دار الكتب القانونية، مصر، دار شتات، ص51.

(60)إجراءات التحري وجمع الدليل والتحقيق الابتدائي في الجريمة المعلوماتية، على عدنان، مرجع سابق، ص54-55.

(61)مجلة الأحكام القضائية السودانية 1975م، ص449.

(62)مجلة الأحكام القضائية السودانية 1977م، ص22.

(63)شرح قانون الإجراءات الجنائية، محمود نجيب حسني، دار النهضة العربية، القاهرة، ط2، ص678.

(64)فن التحقيق الجنائي في الجرائم الإلكترونية، خالد ممدوح إبراهيم، دار الفكر الجامعي، 2010م، ص241.

(65)الإجراءات الجنائية في المملكة العربية السعودية، أحمد عوض بلال، دار النهضة العربية، 1411هـ-1990م، ص439-440.

(66)مولانا محمد الطيب سرور المقابلة في المحكمة بتاريخ 2016/2/7م.

(67)سابقة غير منشورة.

(68)محمد الطيب محمد الخير سرور قاضي المحكمة العامة، محكمة الجرائم المعلوماتية 2015/3/31م.

(69)السابقة غير منشورة.

(70)قانون جرائم المعلوماتية لسنة 2007م المادة 11.

(71)صلاح سعيد علي، محكمة حقوق الملكية الفكرية، الدرجة الأولى ، 2014/9/2م.

(72)السابقة غير منشورة، القاضي مولانا محمد الطيب سرور.