YAKIN DOĞU ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
KAMU HUKUKU / ANABİLİM DALI

SİBER SUÇLARDA CEZAİ KANITLA İLGİLİ ZORLUKLAR

QAHTAN TAWFEEQ KHALEEL AL WAHB

Yüksek Lisans Tezi

LEFKOŞA
2021

جامعة الشرق الأدنى
معهد الدراسات العليا
كلية الحقوق / قسم القانون العام

صعوبات الإثبات الجنائي في الجرائم الإلكترونية

قحطان توفيق خليل الوهاب

رسالة ماجستير

نيقوسيا
2021

SİBER SUÇLARDA CEZAİ KANITLA İLGİLİ ZORLUKLAR

QAHTAN TAWFEEQ KHALEEL AL WAHB

YAKIN DOĞU ÜNİVERSİTESİ
LISANSÜSTÜ EĞITIM ENSTITÜSÜ
KAMU HUKUKU / ANABILIM DALI

Yüksek Lisans Tezi

DANIŞMAN

PROF .DR. WEADI SULAIMAN ALI

NICOSIA
2021

صعوبات الإثبات الجنائي في الجرائم الإلكترونية

قحطان توفيق خليل الوهاب

جامعة الشرق الأدنى
معهد الدراسات العليا
كلية الحقوق / قسم القانون العام

رسالة ماجستير

بإشراف

الاستاذ الدكتور وعدي سليمان علي

نيقوسيا
2021

KABUL VE ONAY

Qahtan Tawfeeq Khaleel Al Wahb tarafından hazırlanan "Siber suçlarda cezai kanıtla ilgili zorluklar" başlıklı bu çalışma, 28/ 01 /2021 tarihinde yapılan savunma sınavı sonucunda başarılı bulunarak jürimiz tarafından Yüksek Lisans Sanatta Yeterlik Tezi olarak kabul edilmiştir.

JÜRİ ÜYELERİ

.....

Prof. Dr. Weadi Sulaiman Ali (Danışman)
Yakın Doğu Üniversitesi
Hukuk Fakültesi, Kamu Hukuk Bölümü

.....

Yrd.Doç.Dr. Yousif Mostafa Rasul (Başkan)
Yakın Doğu Üniversitesi
Hukuk Fakültesi, Kamu Hukuk Bölümü

.....

Yrd.Doç.Dr. Shamal Husain Mustafa
Yakın Doğu Üniversitesi
İktisadi ve İdari Bilimler Fakültesi, Uluslararası İlişkiler Bölümü

.....

Prof. Dr. K. Hüsnü Can Başer
Lisansüstü Eğitim Enstitüsü
Müdürü

قرار لجنة المناقشة

نحن كأعضاء لجنة مناقشة طالب الماجستير قحطان توفيق خليل الوهاب في رسالته الموسومة بـ " صعوبات الإثبات الجنائي في الجرائم الإلكترونية " نشهد بأننا اطلعنا على الرسالة وناقشنا الطالب في محتوياتها بتاريخ 2021/01/28، ونشهد بأنها جديرة لنيل درجة الماجستير.

أعضاء لجنة المناقشة

.....

الاستاذ الدكتور وعدي سليمان علي (المشرف)
جامعة الشرق الادنى
كلية الحقوق ,قسم القانون العام

.....

الاستاذ المساعد الدكتور يوسف مصطفى رسول (رئيس لجنة المناقشة)
جامعة الشرق الادنى
كلية الحقوق ,قسم القانون العام

.....

الاستاذ المساعد الدكتور شمال حسين مصطفى
جامعة الشرق الادنى
كلية العلوم الاقتصادية والإدارية، قسم العلاقات الدولية

.....

الاستاذ الدكتور كـ. حسنو جان باشير
معهد الدراسات العليا
المدير

BİLDİRİM

Ben **QAHTAN TAWFEEQ KHALEEL AL WAHB** olarak beyan ederim ki **Siber suçlarda cezai kanıtla ilgili zorluklar,** başlıklı tezi '**Prof .Dr. Weadi Sulaiman Ali'** nin denetimi ve danışmanlığında hazırladığımı,tezin tamamen kendi çalışmam olduğunu ve her alıntıya Sosyal Bilimler Enstitüsünün tez yazım kurallarına bağlı kalarak yaptığımı taahhüt ederim. Tezimin kağıt ve elektronik kopyalarının Yakın Doğu Üniversitesi Sosyal Bilimler Enstitüsü arşivlerinde saklanmasına izin verdiğimi onaylarım.

Bu Tez benim kendi çalışmamdır. Bu tezde yer alan tüm iddia, fikir, yorum, öneri ve çevirilerin sorumluluğu yazar olarak bana aittir.

Bağlı olduğum Sosyal Bilimler Enstitüsü hiçbir koşul veya şart altında, tezin içeriğini ve bilimsel sorumluluğunu taşımamaktadır. Yapılan ve yayınlanan çalışmaların tüm sorumlulukları yazar olarak bana aittir.

- ☐ Tezimin tüm içeriğine heryerden erişilebilir.
- ☐ Tezimin içeriğine Sadece Yakın Doğu Üniversitesinde erişilebilir.
- ☐ Tezimin içeriğine iki yıl boyunca hiçkimse tarafından erişilemez, eğer bu sürenin sonunda sürenin uzatılmasını talep etmezsem, sürenin sonunda tezimin tüm içeriğine heryerden erişilebilir.

Tarih : 28/01/2021

İmza :

Adı ve Soyadı: QAHTAN TAWFEEQ KHALEEL AL WAHB

الاعلان

أنا **قحطان توفيق خليل الوهاب،** أعلن بأن رسالتي الماجستير بعنوان **صعوبات الإثبات الجنائي في الجرائم الإلكترونية،** كانت تحت إشراف وتوجيهات **الاستاذ الدكتور وعدي سليمان علي،** ولقد أعددتها بنفسي تماماً، وكل اقتباس كان مقيداً بموجب الالتزامات والقواعد المتبعة في كتابة الرسالة في معهد العلوم الاجتماعية. أؤكد بأنني أسمح بوجود النسخ الورقية والإلكترونية لرسالتي في محفوظات معهد العلوم الاجتماعية بجامعة الشرق الأدنى. هذه الرسالة هي من عملي الخاص، وأتحمل مسؤولية كل الادعاءات والأفكار والتعليقات والاقتراحات والنصوص المترجمة في هذه الرسالة هي مسؤولية المؤلف. معهد العلوم الاجتماعية الذي أنتمي إليه ليس له أي تبعية أو مسؤولية علمية تحت أي ظرف من الظروف، جميع مسؤوليات المصنفات المنشورة المنشورة تخصني كمؤلف.

- المحتوى الكامل لرسالتي يمكن الوصول اليها من أي مكان.
- رسالتي يمكن الوصول اليها فقط من جامعة الشرق الأدنى.
- لا يمكن أن تكون رسالتي قابلة للوصول اليها لمدة عامين (2). إذا لم أتقدم بطلب للحصول على الامتداد في نهاية هذه الفترة، فسيكون المحتوى الكامل لرسالتي مسموح الوصول اليها من أي مكان.

تاريخ:2021/01/28

التوقيع:

الاسم واللقب: قحطان توفيق خليل الوهاب

TEŞEKKÜR

Önce Allah'a hamd ve şükürler olsun, salat ve selam insanların en hayırlısı olan Peygamber'e olsun.

Sonra:

Prof .Dr. Weadi Sulaiman Ali Al-Mizori 'ye, tüm uğraşlarına rağmen önce bu araştırmanın denetimini nezaketle kabul eden ve daha sonra tüm düzenlemesini okuması için zaman ayırdığı için onu onurlandıran ve eksik bırakmayan Profesör Dr. Uday Süleyman Ali Al-Mazouri'ye en içten teşekkürlerimi sunarım. bu tezin başarısı için tavsiye ve rehberlik sağlama konusunda ve tartışma komitesi üyelerine de bu araştırmayı kabul ettikleri için içten teşekkürler.

Yakın Doğu Üniversitesi Hukuk Bölümü'nün tüm hocalarına teşekkürlerimi ve şükranlarımı unutmadan.

Ayrıca bu araştırmanın tamamlanmasında bana yardımcı olan, rehberlik eden ve yakın-uzak katkı sağlayan herkese teşekkür ederim.

شكر وتقدير

الحمد لله والشكر أولاً والصلاة والسلام على المصطفى خير الأنام

أما بعد :

أتقدم بالشكر الخالص للأستاذ الدكتور وعدي سليمان علي المزوري والذي تفضل أولاً بقبول الإشراف على هذا البحث رغم انشـــغالاته ثم تكرمه بوقته من أجل قراءته عبر كامل تحريره, ولم يبخل في تقديم النصـــح والإرشاد من أجل إنجاح هذه الرسالة وبالشكر الخالص ايضاً لأعضاء لجنة المناقشة على قبولهم هذا البحث.

دون أن أنسى شكري وإمتناني لكل أساتذة قسم الحقوق جامعة الشرق الأدنى (Near East).

كما أشكر كل من ساعدني وأرشدني وساهم سواء من قريب أو بعيد في انجاز هذا البحث.

ÖZ

SİBER SUÇLARDA CEZAİ KANITLA İLGİLİ ZORLUKLAR

Günümüzde teknolojik gelişmenin sonuçlarından biri, bilgisayarın kullanımı ile bazı yeni suçların işlenmesi arasında bir korelasyonun varlığı, yani bilgisayarın ister bir özne ister bir elektronik suç aracı olsun, yasadışı eylemleri işlemek için bir araç olarak kullanılmasıdır. Ve siber suç, kanıtlanması büyük bir teknik ve yasal zorluk haline gelen geleneksel suçların aksine, duyular tarafından algılanabilecek fiziksel etkiler bırakmaz. Kanıt, suçun meydana geldiğine ve suçun sanığa kanunun tanımladığı şekilde atfedilmesine ilişkin kanıtların oluşturulmasıdır ve bu nedenle elektronik suçlar alanındaki kanıtlar genel ispat kavramına uygulanır ve burada delil elde etmenin zorluğuyla ilgili birçok sorun ve güçlükle ve dolayısıyla elektronik araçları kullanan faille karşı karşıya kalır. Gerçekleştirilen işin teknik niteliği ile karakterize edilen, istihbarat ve yüksek teknik beceri ile nitelendirilen suçları işlerken, bu nedenle fail bu elektronik araçların işleyişi sırasında gerçekleştirdiği yasadışı eylemleri gizleyebilmekte ve gizleyebilmekte ve o sırada bilginin kaydedildiği elektronik titreşimlerin görünmez manipülasyonunu kullanmaktadır. Bilgisayarda depolanan bilginin soyut doğası kadar, bu tür bilgileri iletme araçlarının somut olmayan doğası da ispat konusunda pek çok sorunu beraberinde getirmekte ve elektronik bilgi sürecinde meydana gelen suçtan kaynaklanan kanıtlar çok zordur. Aynı şekilde, siber suçların tespiti, faillere atfedilmesi ve kovuşturulmasında soruşturma ve soruşturma makamlarında deneyim eksikliği ve elektronik suç karşısında uluslararası işbirliğinin zayıflığı olduğunu görüyoruz. Bu kaynak, siber suçlarda cezai kanıtların zorlukları üzerine yaptığımız araştırmanın konusuydu

Anahtar kelimeler: Elektronik suç, elektronik kanıt, bilgisayar.

ABSTRACT

DIFFICULTIES WİTH CRİMİNAL PROOF İN CYBER CRİMES

One result of the technology development at the present time due to the relativity between the use of committing some new crimes and the computer, that is, the computer employs as a device to commit illegal acts, whether it was a subject or a means for these electronic crimes.

Unlike traditional crime, cybercrime does not leave tangible evidence that can be proved by the senses, which has become a great challenge to prove it legally and technically.

To prove the cybercrime, by the law, and accusing the criminal, needs evidence that is specified by the common concept of evidence. This means facing a lot of problems related to the difficulty of obtaining evidence.

Consequently, the offender who uses electronic means to commit crimes has great measure of intelligence and high technical skills for the work that he performs and is able to conceal and obscure the wrongful acts during the operation of these electronic means and the invisible manipulation of the electronic vibrations through which the information is recorded during the crime. As well as, the intangible nature of, the information stored in the computer and the means used to transmit it, will raise many problems and make them very difficult to prove this type of crimes.

Also there is a lack of experience with the investigative authorities in detecting and referring to cybercrimes and their prosecution, furthermore the weakness of international cooperation in the face of electronic crimes.

This source was the subject of our research on the difficulties of criminal proof in cybercrimes.

Key words: Electronic crime, electronic evidence, computer.

الملخص

صعوبات الإثبات الجنائي في الجرائم الإلكترونية

لقد كانت من نتائج التطور التكنلوجي في الوقت الراهن, وجود علاقة أرتباط بين استخدام الحاسوب الالي وأرتكاب بعض الجرائم المستحدثة, اي أستخدام الحاسوب كأداة لارَتكاب الأفعال الغيرَ المشروعة سواءاً كانت الحاسوب الآلي محلا للجريمة الإلكترونية او وسيلة لها.

والجرائم الإلكترونية لا تترك آثاراً مادية يمكن إدراكها بالحواس على عكس الجرائم التقليدية الأمر الذي اضحى يشكل تحدياً كثيراً من الناحية التقنية والقانونية لإثباتها.

والإثبات هو أقامة الدليل على وقوع الجريمة وتنسيبها الى المتهم, ذلك من خلال الذي حدده القانون, وبالتالي فأن الإثبات في مجال الجرائم الإلكترونية تنطبق عليها مفهوم العام للإثبات, وهنا يواجه العديد من المشاكل والصعوبات التي يتعلق بـ (صعوبة الحصول على الدليل), وبالتالي فأن الجاني الذي يستخدم الوسائل الإلكترونية في ارتكاب جرائم يمتاز بالذكاء والمهارة التقنية العالية بالعمل الذي يقوم بها, والذي يتميز بالطبيعة الفنية, وبالتالي فأن الجاني يتمكن من إخفاء وطمس الأفعال غير المشروعة التي يقوم به اثناء تشغيل لمثل هذه الوسائل الإلكترونية ويستخدم في ذلك الوقت التلاعب غير مرئية في الذبذبات الإلكترونية التي تتم تسجيل المعلومات عن طريقه, وكذلك الطبيعة غير المادية للمعلومات المخزونة بالحاسوب الآلي وكذلك الطبيعة المعنوية لوسائل النقل مثل هذه المعلومات يثير المشكلات عديدة في الإثبات, ويكون الدليلِ الناتج عن الجريمة التي يقع على العملية المعلوماتية (الالكترونية) في غاية الصعوبة.

وكذلك نجد أن نقص في خبرة السلطات التحري والتحقيق في كشف الجرائم الإلكترونية وتنسيبها الى مرتكبيها وملاحقتهم قضائياً, وكذلك ضعف التعاون الدولي في مواجهة الجريمة الإلكترونية.

وهذا المصدر كانت موضوع بحثنا حول صعوبات الإثبات الجنائي في الجرائم الإلكترونية.

الكلمات المفتاحية: الجريمة الإلكترونية، الدليل الإلكتروني، الحاسوب الآلي.

.

İÇİNDEKİLER

قائمة المحتويات

المقدمة

شهد العالم اليوم تطورا هائلا في مختلف وسائل الاتصال و(تقنية المعلومات) بحيث اصبح يطلق على هذا العصر(بالعصر الثورة المعلوماتي), ذلك من خلال التغيرات السريعة والحاصلة على التقدمَ العلمي والتقني والتي شملت اغلب جوانبُ الحياةَ, وبالتالي لقد ترتبَ على هذه الثورة الكبيرة والطفرة الواسعة التي جلبتها حضارة التقنية في العصر المعلوماتي, وظهورمصطلح (الجريمة الالكتروني) وكثرة استخدامها وزيادة خطورة الجرائم الإلكترونية, ومن حيث المساعدة على إبتكار أساليب وطرق إجرامية جديدة أو من حيث تسهيل الإتصال بين الجماعة الإجرامية وتنسيق عملياتها كـ(أختراق المواقع, والتفخيخ الإلكتروني والقصف الإلكتروني وغير ذلك من الطرق والأساليب المتقدمة والمتطورة, وبالتالي نتيجة لهذا التطور التكنولوجي أخذ الجريمة بعداً حديثاً يختلف عن النمط العادي (التقليدي) المتعارف عليه حيث أصبح المجرمون يوظفون هذه التقنية في إرتكاب جرائمهم بما يوفر لهم ذلك من إمكانيات واسعة, فـ (العالم الإفتراضي) يوصف لدى أغلب الفقهاء بأنه الملاذ الآمن مثل هذه المجاميع الإجرامية, وبذلك يمكنهم من خلاله التواصل فيما بينهم وبسهولة.

وشبكة الإنترنيت في (الوقت الحاضر) بات يسخر بشكل كبير في التدريب على أعمال الإجرامية, وكيفية تنفيذ العملية والتخطيط لها عن بعد من دون حاجة للإتصال كما في الجريمة التقليدية, وفضلاً عما تتيحه هذه البيئة الإلكترونية من فرصة لهذه المجاميع من التخفي بعيداً عن أنظار الأجهزة الأمنية, وبهذه الطريقة يكون الجاني قد دخل في مرحلة متقدمة للغاية بحيث تجسد فيها الجريمة الإلكتروني الذي تعد تسخير الإنترنيت في إرتكاب جرائم التقليدي, وبالتالي أصبحت الشبكة ذاتها وأنظمة المعلومات في الوقت نفسه هدفاً للمجاميع الإجرامية, ومن خلال هذه الوسائل الإلكترونية يتمكن هذه المجاميع الإجرامية من القيام بأعمال التجسس المعلوماتي من أجل الحصول على كافة أنواع المعلومات منها اقتصادية وسياسية وعسكرية, ونتيجة لكثرة الاعتماد على منظومة المعلومات (الإلكترونية) التي اصبحت منهج حياة المجتمعات العصرية في جميع أنحاء العالم, ولها سيطرة كاملة على جميع المجالات, وقد ترتب عليه وتنوع واتساع في مجال الاهداف التي يمكن للمجرمين مهاجمته مع وجود توافر فرصة كبيرة من السلامة للمهاجمينَ ومحققين في الوقت ذاتها خسائر كبيرة من الناحية البشري وكذلك في الممتلكات المادية والمعنوية أيضاً, وبالتالي صاحب هذا الكشف بشكل واضح عن الأهداف المعرضة الى الخطر أكثر من الكشف عن المجرمين أنفسهم, وبالتالي فرض هذا التحول في شكل الجريمة أختلافاً في مدى مسؤولية مزوري خدمة شبكة الإنترنيت, وكذلك الى الأختلاف في درجة المكافحة ومحاولة فهم طرق وأساليب الجريمة الجديد وأهدافه في التحكم في التكنولوجيا, وبحيث جعل

العالم امام ثورة في أعمال الإجرامية في التركيز على التكنولوجيا واسلحة الدمار الشامل, وفي الآونة الأخير شهد الأعمال الإجرامية تغيراً في طبيعته وخصائصه, وهناك من الدول من تمارس أعمال الإجرامية على شعوبها, حيث كان للفاعلين الجدد دوراُ مهماً في التأثير في تغير طبيعة الأعمال الإجرامية بأستخدام التكنولوجيا الجديدة ليعكس ذلك تغيرات في التنظيم القانوني وكذلك المبادئ التقنية المستخدمة والاستراتيجيتها.

اولاً- أهمية الدراسة:-

أن أهمية دراسة مثل هذا الموضوع من كون العالم الذي ترتكب فيه هذه الجرائم "عالم إفتراضي معلوماتي" عالم يجمع الملفات الشخصية وكذلك ملفات ومعلومات عن المؤسسات الحساسة الموجودة في الدولة, فالجرائم الواقع على هذه المعلومات قد تكون أشد وقعاً من الجرائم العادية(التقليدية), مما قد يترتب عليه أضرار بالغة, بالإضافة الى ذلك فالمجرم الإلكتروني من أكثر المجرمين خطورة لأنه يتخفى وراء شاشة جهاز الحاسوب, وكذلك الخدمات التي يقدمها شبكة الإنترنيت كـ(خدمة البريد الإلكتروني), وتظهر أهمية الدراسة من الجانب آخر من حيث تنفيذ العملية يتم بسهولة, وبمجرد ضغطه زر على لوحة المفتاح تتم عملية إجرامية, ويترتب عليها خسائر في الأرواح البشرية تقدر بالعشرات من العمليات الإجرامية التقليدية, كـ(الدخول على المنظومة الحاسوبية لاطلاق الصواريخ والتلاعب والعبث بمحتوياتها), وبالتالي يترتب على ذلك كارثة انسانية على مستوى العالم, وكذلك الى وجود خسائر مالية لا تقدر بثمن كتدمير برامج وأنظمة المعلومات لإحدى المؤسسات, وما يصاحب ذلك من صرف أموال كثيرة لإعادتها الى حالتها الاعتيادية.

ثانياً - مشكلة الدراسة:-

تتركز مشكلة الدراسة فيما ياتي:-

1. من الصعب وضع التعريف محدد شامل جامع للأعمال الإجرامية, في تحديد إطار أي جريمة وحصر عناصرها, وما يندرج تحتها من أعمال تكمن في تعريف هذه الجريمة بصورة واضحة وشاملة ومانعة.
2. إشكالية تطبيق الجانب الإجرائي وفيما يتعلق بإجراءات ضبط الأدلة الإلكترونية حيث أنها أدلة مخفية غير مرئية, وكذلك كيفية تفتيش جهاز الحاسوب الآلي.
3. كيفية تطبيق عناصر الجريمة التقليدي (العادي) على الجريمة الإلكتروني, من ضمن هذه العناصر عنصر(العنف المادي - وكيفية بث الرعب والخوف في نفوس الأشخاص) وإحداث هذا الرعب اثره الغريزي كما في الجريمة العادي, وهل من الممكن اجماع كل هذه العناصر معاً حتى نكون بصدد جريمة أم إن لإحدى هذه العناصر كعنصر الغاية السياسية أهمية على العناصر الأخرى, ويجب توافرها بالأساس حتى نكون بصدد جريمة هي من أهم الإشكاليات التي واجهت هذه البحث.

ثالثاً - أهداف الدراسة:-

هناك جملة من أهداف تسعى اليها البحث يمكن أجمالها بما يلي:-

1. يسعى هذا البحث الى تحقيق هدفه الرئيسي والمتمثل في محاولة تقديم الدراسة تبين لنا ما المقصود بالجريمة الإلكترونية وذلك من خلال خصائص هذا المجرم ودوافعه.
2. نشر وعي أكثر لدى الأشخاص والحكومة والمؤسسات من خطورة هذا الجرائم, ومحاولة تنبيههم في كيفية أخفاء معلوماتهم بالوسائل الفنية المناسبة, والمحافظة على هذا المعلومات من خلال إجراءات الدخول المعقدة كـ (بصمة العين, بصمة الاصابع, نبرة الصوت).
3. تشجيع المجنى عليه من هذه العمليات الإجرامية بإبلاغ الجهات الأمنية عن وقوعها في وقت قصير.
4. وضع تنظيم قانوني يتم بموجبه مواجهة الجريمة الإلكترونية, والتركيز والتدقيق على هذا التنظيم على ملامح شخصية المجرم الإلكتروني لما يمتلك من الذكاء ومن ذوي المؤهلات العالية في بعض الأحيان.

رابعاً - أسباب أختيار الموضوع:-

هناك عدة أسباب دفعتني الى أختيار هذا الموضوع هي:

1. أن الجرائم الإلكترونية هي من أخطر الجرائم في العصر الحديث, فآثارها لا تقتصر على شخص أو مؤسسة أو على الدولة الواحدة بل أنها تتجاوز الحدود الأقليمية لها.
2. أن هذه الجرائم بـدأ يغـزو المجتمعات خاصة مـع كثرة أستخدام هذا الجهاز في جميع أعمال الحياة بسبب الجهاز وكثرة الأنتهاكات الواقعة وقلة الحماية القانونية.
3. يمكن تنفيذ العملية بخفاء وبعيداً عن أنظار السلطات الأمنية, والذي يعطي دافعاً كبيراً لبحث هذا الموضوع من أجل الوقوف على كيفية التنفيذ, وبيان إمكانية أكتشافه من عدمه.
4. نقص الخبرة لدى أجهزة الأمنية أو السلطة المختصة بالتحري عن الجريمة والتحقيق فيها في مجال الجريمة الإلكترونية والأخطار الناتجة عنها, وبالإضافة الى عدم تنبه الأشخاص لأهمية المعلومات, وبالتالي قد يمتلك الكثير من موظفي المؤسسة - الرقم السري- الخاص بالجهاز بالدخول الى معلوماتها من دون محاولة حصر هذا الرقم بأشخاص معينين, وتغيرهم بصورة دائمية.

خامساً- هيكلية الدراسة:-

لقد قسمنا دراستنا لموضوع صعوبات الإثبات الجنائي في الجرائم الإلكترونية على ثلاثة فصول تناولنا في الفصل الأول ماهية الجريمة الإلكترونية والدليل الإلكتروني وقسمناه على مبحثين تناولنا في المبحث الأول مفهوم الجريمة الإلكترونية وقسمناه على ثلاثة مطالب الأول تناول تعريف الجريمة الإلكترونية والثاني تناول

خصائص الجريمة الإلكترونية وذاتيتها, أما الثالث فتتناول الطبيعة القانونية للجريمة الإلكترونية, وتناولنا في المبحث الثاني مفهوم الدليل الإلكتروني وقسمناه على ثلاثة مطالب أيضاً إذ بينا في المطلب الاول تعريف الدليل الالكتروني وفي الثاني أنواع الدليل الإلكتروني وبينا في الثالث مميزات الدليل الالكتروني وذاتيته, وتناولنا في الفصل الثاني المشكلات الأجرائية المتعلقة بكيفية الحصول على الدليل الإلكتروني وقسمناه على مبحثين تناولنا في المبحث الأول المشكلات المتعلقة بسلطات التحري وجمع الأدلة والتحقيق وقسمناه على خمسة مطالب الأول تناول الصعوبات المتعلقة بعدم الإبلاغ عن الجريمة المعلوماتية والثاني تناول نقص الخبرة لدى سلطات التحري وجمع الأدلة والتحقيق, أما الثالث فتتناول الصعوبات المتعلقة بضخامة كم البيانات المعلوماتية, أما الرابع صعوبة تفتيش جهاز الحاسب الآلي, أما الخامس سنتناول صعوبة الحصول على الشاهد في الجريمة المعلوماتية, وتناولنا في المبحث الثاني الصعوبات المتعلقة بأحالة المتهم الى المحكمة المختصة وقسمناه على مطلبين أيضاً إذ بينا في المطلب الأول الاختصاص المكاني وفي المطلب الثاني الاختصاص النوعي, وتناولنا في الفصل الثالث أيضاً المشكلات القانونية المتعلقة بالدليل الإلكتروني وقسمناه على مبحثين أيضاً تناولنا في المبحث الأول القيمة القانونية للأدلة المستخرجة من الكمبيوتر, وقسمناه على أربعة مطالب الأول تناول الأوراق والثاني تناول جهاز الحاسوب الآلي وملحقاته وأما الثالث فتتناول نطاق تطبيق مبدأ الاقتناع القضائي واما الرابع سنتناول مدى أمكانية أيجاد الوسائل لتقييم الدليل الإلكتروني وتناولنا في المبحث الثاني الأسباب القانونية لتعذر الحصول على الدليل الإلكتروني وقسمناه على ثلاثة مطالب أيضاً إذ بينا في الاول عدم ظهور الدليل المادي وفي الثاني عدم رؤية الدليل وبينا في الثالث فقدان الآثار التقليدية

الفصل الأول

ماهية الجريمة الإلكترونية والدليل الإلكتروني

إن الدليل الإلكتروني الجنائي يولد بمولد الجريمة ذاتها, سواء كان ذلك سابقاً على ارتكابه أومعاصراً لها عند اقتراف الأفعال الإجرامية.

فالأدلة بطبيعتها تتواجد بتواجد الجريمة التي تقع, لأن الدليل الإلكتروني يولد في محله, وهي الجريمة الإلكترونية، أي أنها تلك الواقعة الاجرامية المدعى بحدوثها من قبل سلطات الإتهام الذي يترتب على النجاح في إثبات وقوعها وصحة اسنادها لمرتكبها ثبوت ادانته وتقرير مسؤوليته.

لذلك يجب الحديث عن الجريمة الإلكترونية بأعتبارها نطاقاً للعمل به, والتي تعد ظاهرة حديثة مقارنة بالجرائمَ العادية.

فأننا سنتناول في هذا الفصل مبحثين: فيما يتعلق بالمبحث الأول سيكون الحديث عن مفهوم الجريمة الإلكترونية، والمبحث الثاني عن مفهوم الدليل الإلكتروني.

1.1: مفهوم الجريمة الإلكترونية

يوصف العصر الحالي بالعصر السرعة الرقمي أو ما يسمى بالعصر الإلكتروني, فهو يتضمن تطورات تكنولوجيا هائلة وكبيرة تخدم جميع مجالات الحياة, مما يؤدي الى خدمة المجتمع الدولي بأكمله, فهذه التكنولوجيا تخدم جميع المجالات العامة والخاصة داخل الإطار الضيق للدول, لأن هذا العصريتحرك من خلال تكنولوجيا المعلومات والاتصالات, والتي واكبتها حركة إجرامية, فأنتشرت الجرائم الإلكترونية بشكل

كبير في جميع دول العالم, فالكثير يستخدم الحاسوب الآلي, والكثير معرض الى الوقوع تحت تهديد هذه الجرائم[1]

يبدو في الواقع ان تكنلوجيا الإلكترونية هي وقود (الثورة الصناعية), لان المعلومات بحد ذاتها هي المادة الاساسية للانتاج التي يعتمد عليها المجتمع في انتاجها والأستفادة منه[2].

وعليه سنقسم هذا المبحث الى ثلاثة مطالب, سنتناول في الاول تعريف الجريمة الإلكترونية, وفي الثاني سنتناول خصائص الجريمة الإلكترونية وذاتيتها, والمطلب الثالث سنتكلم عن الطبيعة القانونية للجريمة الإلكترونية.

1.1.1: تعريف الجريمةُ الإلكترونية

لابد في بداية ان نشير إلى انه لا يوجد تسمية موحدة للدلالة على هذه الظاهرة الإجرامية, لذا هناك تباين في التسميات التي يطلق عليها, فالبعض يطلق عليها جرائم الحاسوب الآلي, ويطلق عليها أيضاً بالجرائم الإلكترونية, والبعضَ الاخر يطلق عليها جرائم أصحاب الياقات البيضاء وغيرها من التسميات وآخرون يفضلون تسميتها بالجريمة المعلوماتية[3].

ولكن قبل أن نعرف الجريمة المعلوماتية يجب علينا أن نعرف كل من الجريمة أو المعلومات كل على حد سواء.

ويعرف الجريمة بأنها (كل سلوك خارجي ايجابياً كان ام سلبيا حرمها القانون ويعاقب عليها اذا صدر عن شخص مسؤول)[4]. أما المعلومات فتعرف بانها(رسالة يعبر عنه في شكل يجعله قابلة للتنقل أو الابلاغ للغير, أو هي رمز او مجموعة من رموز ينطوي على امكانية الافضاء الى معنى فالمعلومة أداة مهمة وفعالة ومؤثرة في سلوك الافراد والجماعات في عصرنا الحالي)[5].

---

(1) ثنيان ناصر آل ثنيان، إثبات الجريمة الإلكترونية - دراسَة تأصيلية تطبيقية ,رسالة الماجستير, جامعة نايفَ العربية للعلوم الأمنية, كلية الدراسات العليا, السعودية, 2012م، ص19

(2) نهلا عبدالقادر المومني, الجرائم المعلوماتية، دار الثقافة للنشَر, الاردن, 2008, ص46.

(3) نهلا عبدالقادر المومني, مصدرسابق, ص46

(4) د.قصي علي عباس, مدى إمكانية تطبيق نصوص الجنائي على الجرائم المعلوماتية, ص348.

(5) محمد علي سالم وحسون عبيد هجيج, الجريمة المعلوماتية, مجلة جامعة بابل, العلوم الانسانية, المجلد 14, العدد 2, 2007, ص86

كما أن مشروع قانون الجرائم المعلوماتية العراقي عرف المعلومات بأنه(البيانات والنصوص والصور والأصوات والاشكال وقواعد البيانات وبرامج الحاسب وما شابه ذلك التي تنشأ او تعالج أو ترسل بالوسائل الإلكترونية)[6].

وأيضاً تعرف الجريمة الإلكترونية بانها(النشاط الاجرامي الذي يستخدم فيه التقنية الالكترونية بصورة مباشرة أوغير مباشرة من أجل تنفيذ الفعل الإجرامي المستهدف)[7].

الجريمة الالكترونية(هي كل نشاط ضار يأتيه الفرد عبر أستعماله الحاسوب الآلي وشبكة الإنترنيت, وتكون لهذا النشاط اثار ضار على غيره من الافراد, وكذلك هو فعل إجرامي تستخدم من خلال الوسائل التقنية الحاسوبية الحديثة في ارتكابه لتحقيق غرض غير مشروع)[8].

كما عرفها الاستاذ(Rosenblatt) بأنها (نشاط غير مشروع موجه لنسخ أوالتغييرأوالوصول الى المعلومة المخزونة داخل الحاسب الآلي او حذفها او الوصول او التي يحول عن طريقها)[9].

ويعرف الجريمة الإلكترونية أيضاً على أنها (كل فعل غير مشروع يقوم به شخص تكون على المام كافي بتقنية المعلومات بالأعتداء على نفس أو المال أو المعلومات عن طريق الحاسوب الآلي ومحاسبة مرتكبه والتحقيق معه وملاحقته قضائياً)[10].

في ضوء ما سبق فإن الباحث يقترح تعريفاً للجريمة الإلكترونية بأنها(كل فعل أو أمتناع يتم تخطيط له عن طريق استخدام أي نوع من الحاسوب الآلي سواء كان حاسب شخصي أو شبكات الحاسوب الآلي أو الإنترنيت أو مواقع التواصل الاجتماعي لتسهيل عملية ارتكاب جريمة أوعمل مخالف للقانون او التي تقع على الشبكة نفسها عن طريق اختراقها بغرض تخزينها أو تعطيل البيانات).

وهنا نقسم هذا المطلب الى فرعين سنتناول في الفرع الأول تعريف الجريمة لغة, وفي الثاني سنتناول تعريف الجريمة اصطلاحاً.

---

(6) المادة (ا/ثاني عشر) من مشروع قانون الجرائم المعلوماتية العراقي

(7) ثنيان ناصرال ثنيان, مصدرسابق, ص19 وما بعدها

(8) ثنيان ناصرال ثنيان, المصدرنفسه, ص8.

(9) نهلا عبدالقادر المومني, مصدرسابق, ص48

(10) عبدالله دغش العجمي, المشكلات العلمية والقانونية للجرائم الالكترونية, رسالة الماجستير مقدمة الى جامعة الشرق الاوسط, 2014م, ص12

1.1.1.1: تعريف الجريمة لغة

الجريمة لغة: التعدي, والجرم الذنب, الجمع اجرام وجروم وجرائم, وهوالجريمة, هوجرم يجرم جرما واجترام واجرم, وأجرم يعني جني, وهو مجرم وجريم, وجرم اليهم وعليهم جريمة واجرم جني جناية, والجارم : الجاني, والمجرم: المذنبَ[11].

جرم جرماً: أذنب, يقال جرم نفسه وقومه وجرم عليهم واليهم: جني جناية وفلان لاهله كسب, والرجل اكسبه جرما, أجرم: ارتكب جرماً[12]

2.1.1.1: تعريف الجريمة اصطلاحاً

لم ينكر الفقه الصعوبة في تعريف الجريمة بل تباين الفقهاء في ما بينهم حسب مذاهبهم في تناول الوضوع, فذهب البعض الى تعريف الجريمة بأنه((كلِ نشاط خارجي للانسان سواءِ تمثل في فعل او أمتناع يفرض له القانون عقاباً)) وكذلك عرفها البعض الآخر بأنه((الواقعةُ التي ترتكبَ ضرراً في مصلحة حماها المشرع في قانون العقوبات ويرتب عليه اثراً جنائيا متمثلاً بالعقوبة)) وهنا أبسط تعريف للجريمة هو((أنها الخروج عن النظام الذي يضعه القانون))[13].

2.1.1: خصائص الجريمة الإلكترونية وذاتيتها

سنقسم هذا المطلب الى فرعين, سنتكلم في الفرع الاول خصائص الجريمة الإلكترونية, والثاني سنتكلم عن ذاتية الجريمة الإلكترونية.

1.2.1.1: خصائص الجريمة الإلكترونية

يمكن إجمال خصائص الجريمة الإلكترونية بما يأتي:-

---

(11) إبن منظور, لسان العرب, الجزء الثاني, باب الجيم, دار احياء العربي التراث العربي, لبنان, الطبعة الثالثة, 1419ه - 1999م, ص258

(12) أبراهيم مصطفى واخرون, المعجم الوسيط, ط3, مجمع اللغة العربية, القاهرة, سنة1998, ج1, ص283

(13) دلخاز صلاح فرحان, الحماية الجنائية الموضوعية للمعلوماتية في القانون العراقي, دراسة مقارنة, لنيلِ شهادة ماجستير في الحقوق, جامعة الاسكندرية, كليةُ الحقوق, قسم القانون الجنائي،2015، ص24.

أولاً: الجريمة الإلكترونية عابرة للحدود: -

عندما يكون الفعل أو الامتناع الذي ياتيه الانسان من خلال نظام معلومات معين إعتداء على حق او بيانات معلوماتية يحميها القانون او ادى الى ضرر بـ (المكونات المنطقية للحاسب) او بـ (انظمة الشبكات) المتصلة به ماساً في حدود اكثر من دولة, وفي هذه الحالة نكون أمام جريمة الكترونية عابرة للحدود[14].

ويطلق تعبير على الجرائم عابرَة للدول او الجرائم عالمية على تلك الجرائم التي يقع بين اكثر من دولة [15].

لذا فأن الجريمة الإلكترونية لايعترف بالحدود الحغرافية ولا يعيرها أي اهتمام, وهو مجتمع منفتح عبر شبكات وتخترق المكان والزمان من دون ان يخضع الى حرس حدود, وأن مسرح الجريمة الإلكترونية لم يعد محلياً بل أصبح عالمياً, لأن الجاني يتواجد مادياً على مسرح الجريمة وهذا التباعد في المسافات بين الفعل المرتكب عن طريق الحاسب الآلي والفاعل وبين المعلومات التي كانت محل إعتداء, لان الجاني يتمكن من القيام بجريمته من خلال الدخول الى المواقع الإلكترونية الموجودة في بلد, وهذا الفعل قد يسبب إضراراً لشخص ما في دولة غير دولة الجاني [16].

ثانياً: صعوبة اكتشاف الجريمة الإلكترونية وإثباتها: -

أن الجرائم الإلكترونية لا تترك أي أثر خارجي بصورة مرئية بل ترتكب هذه الجرائم في الخفاء ودون أن تترك أي اثر تدل على مرتكب الجريمة, وأن المجني عليه في الجرائم الإلكترونية يمتنع من الإبلاغ عنها وذلك لعدة أسباب منها افتقاره الى الخبرة الفنيةِ التي تمكنها مِن أكتشاف الجريمة, او تجنباً من الضرر في مصالحه وهز الثقة في كفاءته, إذا ما أعلن عند تعرضه لإعتداء, وذلك إذا كان الاعتداء واقعاً على مؤسسات مالية او تجارية كبيرة فيؤدي ذلك الى الاعلان عن الاعتداء الى إلحاق اضراراً بالمركز الحالي واهتزاز ثقة الجمهور لها بحيث تصبح خسائر الاعلان عن الجريمة أكثر من خسائر الجريمة نفسها, وبذلك يكون عدم الإبلاغ والتكتم عنها أفضل من إعلانها [17].

---

(14) د.سامي فقي حسين, التفتيش في الجرائم المعلوماتية (دراسة تحليلية), دارِ الكتب القانونية, مصر, 2011م, ص27.

(15) ثنيان ناصر ال ثنيان, مصدر سابق, ص23.

(16) د.قصي علي عباس, مصدر سابق, ص352.

(17) د.سامي جلال فقي حسين, مصدرسايق, ص29

ثالثاً: نقص الخبرة لدى الأجهزة الأمنية والقضائية:

نقص الخبرة الفنية لدى الأجهزة الأمنية والقضائية يشكل عائقاً أمام إثبات هذا الجرائم وذلك لأن هذا النوع من الجرائم يتطلب الماماً واسعاً بالأمور الفنية والتقنية لدى أجهزة الأمنية والقضائية, وذلك للتوصل الى مرتكبي هذه الجرائم وإثباتها.

ونتيجة لهذا النقص الحاصل في الخبرة, فأن القائمين في مجال التحقيق لا يبذلون جهوداً كبيرة للتواصل الى مرتكبي هذا الجرائم وإثباتها على الجاني, لأن المحقق نفسه أحياناً يكون سبباً في محو الدليل وذلك بسبب سوء تعامله مع الأدلة نفسها بسبب نقص معرفته وخبرته الفنية والتي تمكنه من الكشف عن الدليل بشكل سليم [18], ويجب على المحقق معرفة أساليب استخراج الدليل في الجرائم الإلكترونية, لانها من العوامل المهمة التي يتمكن من خلالها إثبات الجريمة على الجاني ومحاسبته قضائياً [19].

رابعاً: أنها ترتكب من مجرم غير تقليدي وهي جرائم ناعمة: -

يختلف المجرم في الجرائم الإلكترونية عن المجرم في الجرائم التقليدية (العادية), وذلك لأن له سمات مختلفة عن غيرها, كما أن العوامل التي تدفعه لآرتكاب الجريمة مختلفة عنه أيضاً, فسمات هذا المجرم هو أنه أنسان أجتماعي وغالبا ما تكون له مكانة معتبرة فيه ويحظى بالاحترام منه, وكذلك أن هذا المجرم يمتلك المعرفة والمهارة والوسيلة الخاصة في هذا المجال, وله الخبرة والاحتكاك بالأخرين, وأن هذا المجرم هو أنسان ذكي ويستغل ذكائه في تنفيذ جريمته, ولا يستعين بالقوة الجسدية [20]

ولذلك أن الجريمة الإلكترونية هي جرائم ناعمة لا تحتاج الى عنف أو مجهود عضلي عند تنفيذها, وأنما يرتكبها المجرم بكبسة زر, وبالتالي يعتمد فيها بشكل رئيسي على الخبرة في المجال الحاسبات الإلكترونية, ولا تستدعي طبيعة هذه الجريمة الاستعانة بالأسلحة والإنتقال من مكان الى آخر[21].

---

(18) د.محمد حماد مرهج الهيتي, جرائم الحاسب ماهيتها وموضوعها واهم صورها, ط1, عمان, 2006, ص216

(19) د.محمد عبيد الكعبي, جرائمَ الناشئة عن الاستخدام غير المشرَوع لشبكة الإنترنيت, (دراسة مقارنة), القاهرة, 2009، ص42

(20) عزيزة رابحي, الأسرار المعلوماتية وحمايتها الجزائية, اطروحة لنيل شهادة الدكتوراه في القانون الخاص, كلية الحقوق والعلوم السياسية, قسم القانون الخاص, جامعة ابو بكر بلقايد- تلمسان, 2017- 2018, ص94

(21) د.محمد عبيد الكعبي, مصدر سابق, ص39

خامساً: مرتكب الجريمة ذو خبرة فائقة في مجال الحاسوب الآلي:-

غالبيةِ المجرمين في الجرائم متخصصين في تقنيات الحاسب, ولهم قدرات فنية في التعامل مع الحاسب الآلي الى الحد الذي تمكنهم من تنفيذ الجريمة وأختراق الحواجز وملء الثغرات [22]

لذلك نجد ان أغلب من يرتكبون هذه الجرائم هم من الخبراء في مجال الحاسوب الالي, وان الشرطة اول ما يبحث عن الخبراء الكمبيوتر والإنترنيت عند ارتكابهم الجرائم [23]

سادساً: الجريمة الإلكترونية يتم بأشتراك اكثر من شخص:-

تتطلب الجريمة الإلكترونية عادة أشتراك اكثر من شخص في أرتكابها وفي أغلب أحيان ما يشترك في اخراج الجريمة الى حيز الوجود شخص ذواختصاص في تقنيات الحاسب الآلي والإنترنيت, ويقوم بجانب الفني من المشروع الإجرامي, وشخص آخرمن خارج المؤسسة المجني عليه, والسبب في ذلك لكي تغطي عملية التلاعب وتحويل هذه المكاسب اليه.

والاشتراك في إخراج الجريمة الإلكترونية الى حيز الوجود قد يكون اشتراكاً سلبياً, وهو الذي تترجم بالصمت من جانب من يعلم بوقوع الجريمة في محاولة منه لتسهيل عملية اتمام الجريمة, وقد يكون اشتراكاً ايجابياً وهوغالباً, وكذلك يتمثل في مساعدة مادية أو فنية [24]

2.2.1.1: ذاتية الجريمة الإلكترونية

سنبين في هذا الفرع أوجه الشبه والأختلاف بين الجريمة الإلكترونية والجريمة التقليدية (العادية) وكما يلي:-

أولاً- أوجه الشبه بينهما: -

تتشابه الجريمة الإلكترونية مع الجريمة التقليدية (العادية) في العديد من النقاط ويمكن إجمالها بالشكل التالي:-

1. **كلاهما يقومان على اساس تخطيط وتنظيم وعلى نوع من السرية والتخفي** فالجريمة الإلكترونية لا تختلف عن الجريمة التقليدية في هذه النقطة مثال على ذلك إختراق المواقع الإلكترونية لا يتم بشكل عشوائي بل يصاحبه نوع من التخطيط والتنظيم, وقد يستغرق هذا الامر شهوراً.

---

(22) تغريد سامي ابراهيم الطائي, جرائم الإرهاب الإلكتروني, رسالة الماجستير مقدمة مجلس فاكلتي العلوم الإنسانية, سكول القانون السياسة, قسم القانون, جامعة دهوك, 2010, ص30.

(23) منير محمد الجنبيهي وممدوح محمد الجنبيهي, جرائم الإنترنيت والحاسوب الالي ووسائل مكافحتها, دار الفكر الجامعي, الاسكندرية, الطبعة الأولى, 2006, ص15

(24) نهلا عبد القادر المومني, مصدر سابق, ص58

2. كلاهما يبث الفزع والرعب في نفوس الأشخاص سواء كانوا أشخاص طبيعيين أو معنويين, والرعب هو الأثر الذي يترتب على أستخدام الجريمة, والجريمة الإلكتروني في أحيان كثيرة يخلف فزعاً شديداً يفوق الجريمة العادية, والسبب في ذلك لما قد يترتب عليه من جريمة دموي والمثال على ذلك: دخول الى أنظمة الطيران وتعطيلها, ويؤدي ذلك الى سقوط الطائرة وموت جميع من فيها [25]

3. كلاهما يهدفان الى الإخلال بأمن المجتمع وسلامته ويشمل هذه الجرائم كل الأفعال والأعمال التي تهدف الى تكدير الأمن الداخلي للدولة، فقانون العقوبات العراقي[26] والقوانين الجنائية في الدول المقارنة تجعل الجرائم الإلكترونية ضمن باب الجرائم المخلة بأمن الدولة الداخلي [27]. إذا كان هذا الكلام ينطبق على جريمة التقليدية (العادية) بإعتبار إنه قد تم النص عليه, فالجريمة الإلكترونية يخل بأمن المجتمع الداخلي من باب أولى بما يحدث من فوضى وعدم الاستقرار والمساس بأمن الدولة من الداخل.

ثانياً- أوجه الأختلاف بينهما:-

على الرغم من أوجه الشبه بينهما التي بيناها سابقاً فالأختلاف بينهما واضحاً من خلال النقاط التالية:-

1- صعوبة اكتشاف هذه الجرائم وإثباتها:-

أن اكتشاف الجريمة الإلكترونية امر في غاية الصعوبة, لأن من النادر جداً اكتشاف هذه الجريمة, واذا اكتشفت فإن ذلك يكون بالمصادفة وبعد وقت طويل من ارتكابها, وأن عدد الحالات التي تم فيها أكتشاف هذه الجرائم قليلة جداً قياساً بالجرائم غير المكتشفة, وبالتالي يمكن رد الاسباب التي يقف ورائها صعوبة أكتشاف الجريمة الإلكترونية الى عدم ترك هذه الجريمة لأية أثار مادية ملموسة, وعلى عكس الجرائم العادية التي يترك مرتكبها اثراً مادية ملموسة مرئية مثل (الجثة أو الدماء أو البصمات ... الخ).

أن الجريمة الإلكترونية ترتكب في الخفاء من دون أي أثار يشير الى مرتكبها, كما ان المجرم يمكنه أرتكاب هذه الجريمة في دولة وفي أي قارة اخرى, إذا الجريمة الإلكترونية جريمة عابرة الحدود الدولة [28]

إن للجريمة الإلكترونية في أكثر صورها خفية لا يشعر بها أو حتى لا يعلم بوقوعها, والامعان في حجب السلوك المكون لها وإخفائه عن طريق التلاعب غير المرئي في الذبذبات الالكترونية

---

(25) تغريد سامي إبراهيم الطائي, مصدر سابق, ص35

(26) قد تم النص عليها في الباب الثاني.ن قانون العقوبات العراقي, رقم 111, لسنة 1969, تحت عنوان الجرائم الماسة بامن الدولة الداخلي في المواد (190-222)

(27) تغريد سامي إبراهيم الطائي, المصدر نفسه, ص36

(28) أ سميرة معاشي, الجريمة المعلوماتية (دراسة تحليلية لمفهوم الجريمة المعلوماتية), مجلة المفكر, العدد 17, جامعة محمد خيضر, كلية الحقوق والعلوم السياسية, بسكرة, 2018, ص412

التـي يسـجل البيانـات عـن طـريقهـا, وهـذا لا يعـد بـالأمر العسـير علـى مرتكبهـا, وذلـك بسـبب المعرفـة والخبـرة الفنيـة فـي مجـال الحاسـبات لـدى مرتكبيهـا [29] كمـا أن قـدرة الجـاني علـى محـو وتـدمير الدليل في زمن قصير جدا أي أقل من الثانية الواحدة [30]

2- القوة والعنف:-

أن الأختلاف بينهما يكون من خلال العنف المادي والقوة المادية, ويدخل ذلك الأسلحة بأنواعها (الأسلحة النووية - أسلحة الدمار الشامل – الجرثومية – الكيمياوية) سواء كانت هذه العنف أو القوة موجهة الى الأشخاص, بالقتل والأذى أو نحو الممتلكات((بالتخريب – والتدميرللاموال العامة أو الخاصة)) لذا فأن القوة المادية والعنف المادي تميز الجريمة التقليدية, أما الجريمة الإلكترونية فهو لا يحتاج الى هذين العنصرين بمفهوم المادي, وبعبارة أدق يمكن القول أن القوة التقنية هي التي يستعين بها المجرم الإلكتروني, والعنف المعنوي يكون بالضغط والتهديد, لذلك نقطة الأختلاف بينهما تكون في هذين العنصرين [31].

3- جرائم الإلكترونية جرائم ناعمة:-

يتميـز الجـرائم الإلكترونيـة بأنهـا جـرائم ناعمـة لا تحتـاج فـي ارتكابهـا الـى الجهـد العضـلي والحركـة, وأنمـا تنفـذ بـأقـل جهـد ممكـن أن يقـوم بهـا المجـرم, وكـذلك يعتمـد فيهـا علـى الخبـرة التقنيـة فـي المجـال الحاسـوب الآلـي, كنقـل بيانـات مـن حاسـب الـى آخـر, علـى عكـس الحـال فـي الجريمـة التقليديـة (العاديـة) الـذي يحتـاج الـى جهـد عضـلي أذ يسـتعين الجـاني بأعضـاء جسـمه فـي إتمـام العمليـة متمثلـة اليد-القدم - وغيرها الى وصول الى غايته [32].

4- **نقطة الأختلاف الرابعة بينها** تكمن في أن الجريمة الإلكترونية ينفذ جميع عملياته ويتلقي برؤسائه, ويناقش المعلومات معهم من دون الحاجة الى الاجتماع في مكان واحد, في حين في الجريمة التقليدية لابد من عقد الندوات والاجتماعات في مكان مخصص لذلك [33]

5- المجرم الإلكتروني كأنسان ذكي:-

---

(29) الهام بو الطمين, الإثبات الجنائي في مجال الجرائم الإلكترونية, رسالة الماجستير, مقدمة الى جامعة العربي بن مهيدي- أم البوَاقي- كلية الحقوق والعلوم السياسية, قسم الحقوق, سنة 2017 / 2018م, ص12 ومابعدها

(30) نادر عبدالكريم العزاوي, الحماية الجنائية من الجرائم الانترنيت (دراسة مقارنة), ص21.

(31) تغريد سامي إبراهيم الطائي, مصدرسابق, ص36 ومابعدها

(32) د.محمد عبيد الكعبي, مصدرسابق, ص39

(33) تغريد سامي إبراهيم الطائي, المصدرنفسه, ص37

أن مـرتكـب الجريمة الالكترونية (المعلوماتية) شخص يتميز بـ (الذكاء والـدهـاء) في الغالب, وهذا النوع من الجرائم يتطلب مهارات عقلية وذهنية عـاليـة, وكذلك درايـة بأسلوب التي يستخدمها فـي مجال الحاسوب الالي والإنترنيت, وكيفية تشغيله وتخزين المعلومات التي يحصل عليه, فالمجرم الإلكتروني يستخدم مقدرته العقلية ولا يلجأ الى استخدام العنف بل يحاول دائما أن يحقق أهدافه بهدوء,على عكس الجرائم التقليدية (العادية) - وفـي أغلب الاحيان - يكون شخص امـي بسيـط ومتوسط التعليـم [34]

6- ونقطة الأختلاف بينهما تكمن في أن مرتكب الجريمة الإلكترونية (المعلوماتية) قـد يكـون متكيفـا اجتماعيـا وقـادرا ماديـا, الا ان دافعه على ارتكـاب جريمتـه في أغلب الاحيان, هو رغبته فـي قهـر الانظمة, ولكن هذه الـرغبة قـد تضيف عنـده على رغبته من أجل الكسب الربع أو النفع المادي, على عكس في الجريمة التقليدية حيث أن مرتكبها - في الغـالب- يكون غير متكيف اجتماعيا, ورغبته من أجل الحصول على الربع تفوق اي رغبه آخرى [35]

3.1.1: الطبيعة القانونية للجريمة الإلكترونية

لابد من التمييز بين مسألتين في غاية الأهمية عند تحديد الطبيعة القانونية في موضوع الجريمة الإلكترونية هما:-

أولاً:- إذا تم الاعتداء على جهاز الحاسوب بمكوناته المادية من حيث آلة طابعة وشاشة وأجهزة الإدخال والإخراج, والأشرطة الممغنطة في حالة ما إذا كانت هذه خالية من البيانات والمعلومات, في هذه الحالة لا توجد أية مشكلة قانونية لأنها تندرج تحت اطار الاعتداء على الاموال المادية بمعنى التقليدي, في هذه الحالة فأن نصوص قانون العقوبات هي واجب التطبيق.

ثانياً:- اما في حالة إذا تم الأعتداء على المكونات غير المادية, ويقصد به ما موجود داخل الحاسوب الآلي من معلومات وبيانات, وهنا تثارمشكلة بشأن تحديد الطبيعة القانونية على هذه الاموال, وأكتساب هذه المسالة على أهتمام العديد من الفقهاء والقضاة وحول مدى إمكانية تطبيق نصوص قوانين العقوبات التقليدية, أم أن الأمر قد يحتاج الى إستحداث قوانين خاصة لكي تواكب طبيعة هذه الأموال [36]

---

(34) د.عمارة فتيحة, الجريمة المعوماتية, مجلة أبحاث قانونية, السنة رابعة, العدد السابع, يونيو 2019م, ص84

(35) د.ابراهيم رمضان ابراهيم, الجريمة الإلكترونية وسبل مواجهتها في الشريعة الاسلامية والإنظمة الدولية (دراسة تحليلية تطبيقية), 2015, ص373 ومابعدها

(36) تغريد سامي إبراهيم الطائي, مصدر سابق, ص31

لقد انقسم الفقه الى فرعين لتحديد الطبيعة القانونية للجرائم الإلكترونية

1-1-3-1- التقليدي يرى إن المعلومـة لهـا طبيعـة مـن نـوع خـاصَ.

2-1-3-1- الحديث يـرى إن المعلومـة ماهي الا مجموعـة مـن القيـم.

سنبينَ مضمون كل منهما كالاتي:-

1.3.1.1: الاتجاه التقليدي/ المعلومـةَ لها طبيعة مـن نـوع خاص

يرى هذه الفقـه ان للمعلومة طبيعـة من نـوع خاص, وقد استهلموا هذه الفكرة من تطبيقه للمنهج التقليدي, والذي بموجبه يعطي وصف القيمة للاشياء المادية فقط, إذ يروا أن الأشيـاء التـي يوصف بالقيـم هـي تـلك الأشياء التي تكون قابلة للإستحـواذ المادي, ويرون ذلـك أن لها طبيعة معنوية, فإنه من غير قابلة للإستئثار والإستحواذ المادي الإعن طريق حق الملكية الأدبية.

أو الفكرية أو الصناعية, وذلك فإن المعلومات المخزونة في الحاسوب والتـي لا ينتمي الى اي مـن المـواد الادبيــة او الفكرية او الصنـاعيـة ولا تنـدرج ضمن مفهوم القيـم المحميـة قانونا [37]

فأن الفقه والقضاء يعترفان بـوجـود خـطا عند استحواذ علـى معـلومات الغـير, لذاَ حـاول هـذا الاتجاه ان يحـمي هـذه المـعلومات من دعوى المنـافسة غيرالمشروعة, وذلك استنـادا الى حـكم المحكمة النقض الفرنسي الذي يقضـي" ان وسيلة مـن دعـوى المنـافسة غـير المشروعة هـي تـأمين حمـاية قانونية للشخص الـذي لايـمكن ان ينتـفَع لأي حـق أستثنائي".

وهكذا فقد قرر الأستاذ Debois في وقت مبكر بأن الملكية - والتي اطلق عليها الملكية العلمية, لربما سيأتي يـوما وسيعترف به الى صاحب فكـرة الذي لـم يحصل بعدعلى حـق بـراءة أختراع بأعتبار ان الفكـرة السابقـة مستبعـدة مـن مـجال المـلكية الفكرية [38]

2.3.1.1: الاتجاه الحديث/ المعلومات مجموعة مستحدثة من القيم

يرى انصار هذه الاتجاه أن للمعلومة قيمة أقتصادية ويرجع الفضل في ذلك في إخفاء وصف القيمة الى كل من الأستاذين Vivant,Catala [39]

---

(37) محمد عبدالله أبو بكر سلامة, موسوعة جرائم المعلوماتية جرائم الكمبيوتر والإنترنيت, منشأة المعارف, الاسكندرية, 2006, ص88 ومابعدها.

(38) د.محمد علي العريان, الجرائـم المـعلوماتية, دار الجامعة الجـديدة للنشر والتوزيع, الاسكندرية, مصر, 2004, ص49

(39) تغريد سامي إبراهيم الطائي, مصدر سابق, ص32

فتعد المعلومة وفقاً لرأي الأستاذCatala الى قابلية المعلومة للإستحواذ كـ (قيمة مستقلة) عن دعامتها المادية, ويبرر الأستاذ Catala هذه الوصف على أنها أي معلومة يقوم بها وفقاً الى سعر السوق عندما يكون غير محظورة تجاريا, انها ينتفع بغض النظرعن الدعامة المادية, عن عملِ قدمه, ويقول الأستاذ Catala أنها ترتبط بصاحبها عن طريق علاقة قانونية يتمثل بعلاقة المالك في الشيء الذي يملكها, وهي تخص صاحبها وبسبب علاقة التبني التي يجمع بينهما.

لذلك فقد أستند الاستاذ (Catala) الى حجتين رئيستين لاضفاء وصف القيمة على المعلومات: الحجة الأولى – قيمتها الاقتصادية((حيث تقوم المعلومة وفقاً لسعر السوق وحيث أنها تنتج بغض النظر عن دعامته المادية وعن عمل من قدمها)) والحجة الثانية – وجود علاقة التبني الذي يجمع بينها وبين مؤلفها))[40]

أما الأستاذ Vivant يتبنى هذا الاتجاه واسسه على حجتين أيضاً بالنسبة للحجة الأولى/ قد استمدها كل من الأستاذين ((Ripert-Planiol)) تتمثل هذه الحجة الى ان فكرة الشيء او القيمة له صور معنوية, وان نوع محل الحق يمكن ان ينتمي الى حقل القيم المعنوية ذات الطابع أقتصادي, وتكون هذه جديرة في الحماية القانونية.

أما الحجة الثانية/ خاصة بالأستاذ ((Vivant))حيث رآى ((ان كل الاشياء المملوكة ملكية معنوية والذي يعترف به القانون, وتعترف بان للمعلومة قيمة عندما يكون من قبيل البراءات او الرسوم او النماذج الصناعية, والشخص الذي يقوم ويكشف ويطلع الجماعة على شيء ما بغض النظرعن الشكلِ او الفكرة, وبذلك يكون قد قدم لهم معلومة بالمعنى الواسع ولكنه خاصة بها, يجب ان يعامل هذه الاخيرة بوصفها قيمة وتصبح محلا للحق ولا يوجد ملكية معنوية وبدون الاقرار في القيم المعلوماتي)) وبذلك هو يرى ان القيم المعلوماتي بوصفها قيمة تندرج في إحدى مجموعة القانون الوضعي, وأن القيمة المعلوماتية ليست بالشيء المستحدث [41]

يتفق الاستاذ Vivant مع الرأي السابق, حيث رآى إن للمعلومات قيمة قابلة للتمليك, لانه له قيمة أقتصادية, ويمكن أن يكون محلاً لعقد بيع [42]

---

(40) محمد عبدالله أبو بكر سلامة, مصدرسابق, ص91

(41) د.محمد علي العريان, الجرائم المعلوماتية, دار الجامعة الجديدة للنشر والتوزيع, الاسكندرية, مصر, 2011, ص63 وما بعدها

(42) د.سامي جلال فقي حسين, مصدرسابق, ص47

ونرى أن الاتجاه الحديث هوالافضل لأنه يعطي للمعلومات قيمة مالية ويمنحها حماية قانونية شرط وجودها في حيازة مالكها, لأن وجودها في اطار محدد يمكن أن تبلغ بوضوح وبمعزل عن وسطها المادي, لأنه إذا لم تمنع المعلومات التي تكون لها قيمة مالية حماية, ستكون جميع المعلومات معروضة للاعتداء عليها دون رادع.

2.1: مفهوم الدليل الالكتروني

وكان من الضروري معرفة معنى الدليل الالكتروني ومفهومه لكي يسهل توضيح كل الجوانب المتعلقة به.ان الدليل الالكتروني بإعتبارها من الأدلة ألجنائية الخاصة التي ظهرت عند ظهور الجريمة الالكترونية بهدف اثباتها, بإعتباره الوسيلة الوحيدة أوالرئيسة لإثبات هذه الجرائم,

لذا سنقسم هذا المبحث الى ثلاثة مطالب: يتعلق الاول بتعريف الدليل الالكتروني، فيما يتعلق الثاني بأنواع الدليل الالكتروني، والمطلب الثالث سنتناول فيها مميزات الدليل الالكتروني وذاتيته.

1.2.1: تعريف الدليل الإلكتروني

هناك عدة تعريفات التي أنصبت على الإدلة الالكترونية، فقد عرفها البعض الدليل الالكتروني "بانه الدليل المأخوذ من اجهزة الحاسوب الآلي, يكون على شكل مجالات اونبضات مغناطيسية أوكهربائية، وكذلك يمكن تجميعها أو تحليلها بإستخدام برنامج تطبيقات وتكنولوجيا خاصة، ويتم تقديم معلومات على أشكال متنوعة مثل صورأو تسجيلات صوتية أو مرئية من اجل الربط بين الجريمة والجاني والمجنى عليه (بشكل قانوني) يمكن أعتماده امام القضاء" [43]

ويلاحظ على هذا التعريف إنه يقتصر مفهوم الدليل الرقمي على ذلك الدليل الذي تم استخراجها من الحاسوب فقط, لا شك ان ذلك فيها تضييق للدائرة الإدلة الإلكترونية, وهي كما يمكن ان يستمد مِن الحاسوب الالي, ومن الممكن ان تتحصل عليه من اية الة الإلكترونية اخرى, والهاتف والات التصوير وغيرها مِن الاجهزة التي يعتمد التقنية الإلكترونية في تشغيله, ويمكن ان يكون مصدرا للدليل (الإلكتروني).

(43) نعيم سعيداني، اليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري،(رسالة الماجستير), جامعة الحاج خضر- باتنة، كلية الحقوق والعلوم السياسية، الجزائر، 2013 م, ص120

وعُرِفَ أيضاً بأنه(الادلة التي يشمل جمع البيانات الإلكترونية التي يمكن ان يثبت ان هناك جريمة قد أُرتكِبت او يوجد صلة بين الجريمة والمتضررمنه, فالبيانات الإلكترونية هي مجموعة الارقام التي يمثل مختلف المعلومات من ضمنها النصوص المكتوبة، الرسوم، أو الصورة أو الصوت) [44]

وكذلك يمكن تعريف الدليل الإلكتروني بأنه((هو كل بيانات يمكن اعدادها وتخزينها على شكل الإلكتروني، حيث تمكن الحاسب الآلي من انجاز مهمة ما)) وعرف ايضا بأنها ((الدليل إلذي له يجد اساساً في العالم الأفتراضي ويقود الى الجريمة)) [45]

ويعرف أيضاً بأنه ((تلك المعلومات التي يقبلها المنطق والعقل ويعتمدها العلم ويتم الحصول عليها باجراءات قانونية وعلمية في ترجمة المعلومات والبيانات المخزونة في اجهزة الحاسب الآلي وملحقاتها وشبكة الأتصال(الإنترنيت)، بحيث يمكن أستخدامه في اي مرحلة من مراحل التحقيق او المحاكمة لأثبات حقيقية فعل او الشخص له صلة بالجريمة أوالجاني او المجني عليه))[46]

ومن جانبنا نقترح التعريف الآتي (أنه الدليل المتحصل عليه من الحاسوب بمكوناته المادية والمعنوية أو من أي نظام الكتروني آخر, وذلك لاعتماده أمام سلطات التحقيق والمحاكمة).

ونقسم هذا المطلب الى فرعين: فيما يتعلق بالفرع الأول نعرف الدليل الإلكتروني لغة، أما الفرع الثاني سنعرف الدليل الإلكتروني اصطلاحاً.

1.1.2.1: تعريف الدليل لغة

الدليل لغة: مايستدل به، و(الدليل) هوالدال ايضاً، ويقال دله على الطريق يدله بـ (الضم) دلالة بـ (فتح الدال) وكسرها، ودلولة بـ (الضم) والفتح اعلى، أو يقال (ادل) والأسم الدال بـ (تشديد اللام)، وفلان يدل فلاناً أي يثق به [47]

وقال أبوعبيد: (الدال)قريب المعنى مِن المعنى من الهدى وهما السكينة والوقارِ في الهَيئة والمنظر وغيرذلك [48]

---

(44) هدى طالب علي, الإثبات الجنائي في جرائم الإنترنيت والاختصاص القضائي بها, رسالة الماجستير مقدمة الى كلية الحقوق, جامعة النهرين, 2012م, ص118 وما بعدها

(45) د. اشرف عبدالقادر قنديل, الاثبات الجنائي في الجريمة الإلكترونية, دارالجامعة العربية, مصر, 2015, ص123

(46) د.محمد الامين البشري, الأدلة الجنائية الرقمية(مفهومها ودورها في الاثبات), المجلة العربية للدراسات الأمنية والتدريب, الرياض, المجلد17, العدد 33, 2004م, ص109

(47) إبن منظور، لسان العرب، الطبعة الثالثة، باب - دال، دار احياء العربي، المجلد الحادي عشر, بيروت، 1994, ص248

(48) عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن، دار الجامعة الجديدة، مصر، 2010، ص50

والدليل في اللغة هو المرشد، وما يتم به الارشاد, و(ما يستدل به), و(الدليل الدال) و(الجمع أدلة ودلالات) [49]

2.1.2.1: تعريف الدليل اصطلاحا

بعد التطرق الى التعريف اللغوي للدليل الجنائي الإلكتروني في الفرع السابق سنتاول في هذا الفرع التعريف الآصطلاحي له, وذلك من خلال التعريف الآصطلاحي للدليل الجنائي الإلكتروني.

تعريف الدليل اصطلاحا: هو ما يلزم من العلم به علم شي أخر، وغايته أن يتوصل العقل الى التصديق اليقيني بما كان يشك في صحته.

بمعنى أنه الوسيلة التي يستعين القاضي بها للحصول على الحقيقة التي ينشدها، أي التوصل به الى معرفة الحقيقة [50]

وجاء ذكر الدليل في القرأن الكريم في قوله تعالى((الم ترعلى ربك كيف مد الظل ولوشاء لجعله ساكناً ثم جعلنا الشمس عليه دليلا)) [51]

تعريف الإلكتروني: يقصد بكلمة الإلكترونية (Electronigue)الجسيمات السالبة الشحنة, والمتناهية الصغر تنبعت من المهبط بتأثر اصطدام أيونات الغاز الموجبة به [52]

2.2.1: أنواع الدليل الإلكتروني

نقسم الدليل الجنائي الإلكتروني الى قسمين:-

أدلة أعتبر لتكون وسيلة اثبات, وأخرى لم تعد لتكون وسيلة اثبات، وعلى النحو الأتي: -

أولاً: أدلة أعدت لتكون وسيلة إثبات:

فتتمثل هذه الإدلة في:-

---

(49) د. محمد الأمين البشري, المصدر نفسه, ص104

(50) د. منصورعمرالمعايطة, الإدلة الجنائية والتحقيق الجنائي، الطبعة الأولى, دار الثقافة للنشروالتوزيع, عمان, 2007, ص17

(51) سورة الفرقان، الأية, (45).

(52) سلامة محمد المنصوري, تطبيق مبدأ الاقتناع القضائي على الدليل الإلكتروني, أطروحة مقدمة لإستكمال متطلبات الحصول على درجة ماجستير في القانون العام, جامعة الامارات العربية المتحدة, كلية القانون , قسم القانون العام, نوفمبر, 2018, ص16

أ- السجلات التي تم إنشاؤها بواسطة جهازالحاسوب بشكل تلقائي، تعتبرهذه السجلات من مخرجات جهاز الحاسوب وبالتالي ومن ثم لم يلمسها أو لم يساهم الإنسان في إنشائها مباشرة، ومثال على ذلك سجلات الهواتف والفواتير, البطاقات البنكية.

ب- السجلات الذي جزء منه يتم حفظها بـ(الإدخال)وجزء أخر يتم انشاؤه بواسطة الحاسب الآلي(الكمبيوتر)، وأمثلة على ذلك رسائل غرفة المحادثة التي تتبادل عبرالإنترنيت ورسائل البريد الإلكتروني (53)

ثانياً: أدلة لم تعد لتكون وسيلة اثبات:

هذا النوع من الأدلة الإلكترونية نشأة من دون ارادة الشخص، فهو عبارة عن أثار يتركها الجاني على مسرح الجريمة ودون ان يكون راغب في وجودها, ولذا يسمى هذا النوع من الادلة بـ (البصمة الوراثية) أوالإلكترونية ويسمى أيضا بالأثار المعلوماتية والرقمية.

وتتجسد هذه في الأثار التي يتركه المستخدم شبكة الإنترنيت, وبسبب تسجيلها للرسائل المرسلة منها، او التي تستقبلها, وكذلك كافة الأتصالات التي تمت مِن خلال الحاسوب الآلي او المواقع الإنترنيت (54)

وفي الواقع ان هذا النوع منَ الدليل لم يعد اساساً في الحفظ من طرف صدرعنه، ولكن الوسائل الفنية الخاصة يمكن من ضبط هذه الادلة وإن مرت عليه مدة زمنية طويلة، فالأتصال التي يجري عبر الإنترنيت والمراسلات التي صدرت من شخص او التي تلقاها، وكلها يمكن ان يضبط بواسطة التقنية الخاصة بذلك (55)

تبدو اهمية التمييز بين هذين النوعين في ما يأتي:

أ- فالنوع الثاني من الادلة الإلكترونية هي الاكثر من اهمية من الاول لكونها لم يعد اصلا ليكون اثاراً لمن صدر عنه, لذا فهو في الغالبا يتضمن معلومات ذات مصداقية يفيد بالكشف عن الجرائم ومرتكبيها.

ب- يتميزالنوع الاول من الادلة الإلكترونية بسهولة الحصول عليها لكونها قد اعد اصلا لان يكون دليل على الوقائع التي يتضمنها, بينما يمكن أن يحصل على الثاني من الادلة في إتباع تقنيات خاصة لا تخلو من الصعوبة والتعقيد.

---

(53) خالد عياد الحلبي، اجراءات التحري والتحقيق في جرائم الحاسب والإنترنيت، دارالثقافة والنشر والتوزيع, عمان، 2011، ص234

(54) خالد عياد الحلبي, المصدرنفسه، ص234 ومابعدها

(55) نعيم سعيداني، مصدرسابق, ص129

ت- أن الاول من الأدلة قد اعد سلفا كـ(وسيلة لإثبات بعض الوقائع), فإنها عادة ما يعمد الى حفظها للإحتجاج به لاحقا, وهوما يقلل من امكانية فقدانها, بينما الثاني من الأدلة الإلكترونية بحيث لم يعد يحفظ وهو ما يجعلها عرضة الى فقدان بسهولة لاسباب منها فصل التيار الكهربائي [56]

3.2.1: مميزات الدليل الإلكتروني وذاتيته

نقسم هذا المطلب الى فرعين, سنتنكلم في الاول مميزات الدليل الإلكتروني, وسنتكلم في الفرع الثاني عن ذاتية الدليل الإلكتروني.

1.3.2.1: مميزات الدليل الإلكتروني

تتميز الدليل الإلكتروني في عدة مميزات إهمها:-

1. تتميز الدَليل الإلكتروني في صعوبة محو أوتحطيمه، حتى لوكان في حالة محاولة اصدار امر بإزالة الدليل من أجهزة الكمبيوتر، وبالتالي من الممكن اعادة اظهارها من خلال ذاكرة الحاسوب الآلي التي تحتوي على الدليل.
2. في حالة أذا حاولة المجرم أن يمحو الدليل الإلكتروني بذاته يسجل عليه كـ (دليل)، وبالتالي ان قيامه بذلك يتم تسجيل في ذاكرة الحاسوب الآلي, ويمكن استخراجها واستخدامها ضده كـ (دليل).
3. ان الطبيعة الفنية للدليل الإلكتروني تمكنه مِن اخضاعها الى بعض البرامجيات والتطبيقات لكي يتعرف إذا كان قد يتعرض الى العبث وكذلك الى التحريف [57]
4. يتميز الدليل أيضا برصد المعلومات عن المجرم وتحليلها في نفس الوقت، بحيث يمكنه ان تسجل حركات الشخص، وكما انه يسجل عادات وسلوكيات وبعض الامور الشخصية عنه [58]

2.3.2.1: ذاتية الدليل الإلكتروني

ان البيئة إفتراضية التي يعيش فيه الأدلة الإلكترونية هي بيئة متطورة في طبيعتها، بحيث يشمل على انواع متعددة من البيانات الالكترونية، حيث قد تكون منفردة أومجتمعة, ولكي تكون دليل للادانة أوالبراءة، قد انعكست على هذه الأدلة، ومما جعلها تتصف بعدة خصائص وميزتها عن الدليل الجنائي العادي على النحو التالي:-

---

(56) طارق محمد الجملي, الدليل الرقمي في مجال الاثبات الجنائي, محاضر في كلية الحقوق, جامعة بنغازي ليبيا, مجلة الحقوق, المجلد(12), العدد (1), ص46 وما بعدها

(57) الجريمة الإلكترونية وحجية الدليل الرقمي في الأثبات الجنائي، مركزهردو لدعم التعبيرالرقمي، ص24

(58) د.فتحي محمد أنورعزت, الادلة الإلكترونية في المسائل الجنائية والمعاملات المدنية التجارية للمجتمع المعلوماتي، دار الكتب القانونية, ط2، القاهرة، 2010, ص556.

1. الدليل الإلكتروني دليل علمي:-

تتكون الدليل الالكتروني من البيانات والمعلومات ذات هيئة الكترونية غيرملموسة، وكذلك لا تدرك بـ (الحواس العادية), ولكنها تتطلب ادراكها الأستعانة بالحاسبات الآلية وكذلك بالاجهزة الالكترونية، وبأستخدام برنامج الكترونية خاصة بذلك [59]

بمعنى لا يمكن الحصول على الدليل الإلكتروني سوى بأستخدام الأساليب العلمية, وإن هذه الخاصية تفيدعند قيام رجال ضبط القضائي أوسلطات التحقيق في التعامل مع هذا الدليل الكتروني من أجل السعي لإثبات الحقيقة، ويكون البحث هنا على أسس علمية, وإن الدليل العلمي تخضع الى قاعدة اللزوم وتوافق تجارياً مع الحقيقة، وهذا وفقاً الى القاعدة في القضاء المقارن هي القاعدة (ان القانون مسعاه العدالة واما العلم فمسعاه الحقيقية) وعلى الرغم من الأنتقادات التي توجه هذه القاعدة من حيث الألتزام الذي يلقيه القانون المقارن على عاتق اعضائه بضرورة توافر معرفة علمية، لكي يمكن إقامة بنيان التمييز بين ماهو قانوني وما هوعلمي [60]

وكذلك تفيد هذه الخاصة حين نتطرق الى مسألة حفظ الدليل الإلكتروني على أسس علمية وكذلك ضرورة الحث على تحديث أسلوب تحرير المحاضر في هذه الشأن، فتحرير محضريتناول دليلاًعلمياً، يختلف عن تحريرمحضر يتناول إعتراف شخص بجريمة قتل أوإنتهاك حرمة مسكن أو سرقة عادية ...الخ.

وتحرير محضربالدليل العلمي يعني ضرورة توافر مسلك علمي في تحريره, ويتوافق مع ظاهرة الدليل العلمي تحديداً بحيث يجب ألا يتخذ صوره المحضر التقليدي [61]

2. الدليل الإلكتروني دليل تقني:-

التقنية بنت العلم, ولا يمكن إن تتواجد بدون أسس علمية، لأن الدليل الإلكتروني هو دليل علمي، فأن ذلك يثبت إن التقنية هي الخاصية الثانية التي يتمتع بها الدليل الإلكتروني، ويجب أن يتم التعامل مع الدليل الإلكتروني من قبل تقنيين مختصين في الدليل الإلكتروني وفي العالم الإفتراضي، لأن الدليل الإلكتروني ليس مثل الدليل العادي، ولا ينتج التقنية لنا سكينا يتم بها أكتشاف القاتل أواعترافاً مكتوبا او مالا في جرائم الرشوة أو بصمة أصبع, انما ما تتجه إليه التقنية هو نبضات أومجالات مغناطيسية، أوكهربائية، وتشكل قيمتها في امكانية تعاملها مع القطع الصلبة التي تشكل الحاسبات في أي شكل يكون عليها [62]

---

(59) خالد عياد الجلبي، مصدرسابق، ص231

(60) د.فتحي محمد أنورعزت، مصدر سابق، ص648

(61) د.فتحي محمد أنورعزت، المصدرنفسه، الصفحه نفسها

(62) د.فتحي محمد أنورعزت، مصدرسابق, ص649

3. الدليل الإلكتروني يصعب التخلص منه :-

أن هذه الخاصية تعد من أهم الخصائص التي تتمتع بها الـدليل الإلكتروني عـن غيرها مـن الادلة العادية، ويمكـن التخلـص منها وبسهولة مـن الأوارق وكذلك الاشرطة المسجلة التي تحمل إقرار بأرتكاب شخص للجرائم, وذلك بـ (تمزيقها وحرقها)، وكما أنه يمكن أن يتخلـص مـن بصمـات الأصابع بمسحه من موضعه، كما انه قد يلجأ بعض المشتبه فيهم الى قتل الشهود أوتهديدهم بعدم الإدلاء بالشهادة، حيث أنه من الصعب استرجاع الدليل المستخدم فيها، وذلك بسسب قيامهم بتدميرها، وهذا فيما يخص الأدلة التقليدية، أما بالنسبة للأدلة الإلكترونية الذي يمكن استرجاعه بعد محوه وإصلاحه، وبعد إتلافه وإظهاره بعد إخفاءه، مما يؤدي الى صعوبة التخلص منه.

لأن هنالك العديد من البرامج الحاسوبية التي يمكن بواسطتها استرجاع كافة الملفات التي تم إزالتها وإلغاؤها من الحاسوب.

أن نشاط الجاني في محو الدليل يسجل دليلاً أيضاً، فنسخة من هذا الفعل (وفعل الجاني لإخفاء الـدليل)، ويتم تسجيلهـا فـي الكومبيوتر، وكذلك يمكن أستخراجه وأستخدامه لاحقا كـ (دليل ادانة ضده) [63]

4. إن الدليل الإلكتروني متنوع ومتطور:-

إن الدليل الإلكتروني يشمل جميع أنواع بيانات الإلكترونية التي من ممكن تداولها الكترونياً، حيث تكون بينه وبين الجريمة رابط مـن نـوع خاص، ويتصل بـ (الضحية) على النحـو الـذي تحقق هـذه رابطة بينه وبين المجرم، وتعني هذه الخاصية بأنه على الرغم من أن الدليل الإلكتروني في أساسه متحد التكوين بلغة الحوسبة والرقمية، الإ أنه مع ذلك يتخذ أشكالاً مختلفة كأن يكون بيانات غيرمقروءه، كما هو الحال في المراقبة عبر الشبكات، وقد يكون الدليل الإلكتروني مفهوماً للأشخاص كما لوكان وثيقة معدة بنظام المعالجة الالية، كما من الممكن أن يكون صورة ثابتة أو متحركة أومعدة بنظام التسجيل السمعي البصري أومخزونة في البريد الإلكتروني، فهذه الخاصية تستوجب مواكبة التطور الحاصل في عالم تكنولوجيا المعلومات [64]

5. الـدليـل الالكتـروني قـابـل لاستنساخ:-

---

(63) د.أشرف عبد القادر قنديل، مصدرسابق، ص127

(64) د.فتحي محمد أنورعزت، مصدرسابق، ص651 وما بعدها

ويمكن إستخراج نسخه من الدليل الجنائي الإلكترونية مطابقاً للاصل, وكذلك لها نفس القيم العلمية والحجية الثبوتية، وكذلك هذا خاصية لا يتوافر في باقي الادلة الجنائية الاخرى(العادية)، ومما يشكل ضمانة شديدة الفعالية في حفاظ على الدليل ضد (التلف والفقدان والتغيير)عن عمل نسخة طبق الاصل من الدليل, ومثل هذا الامر لاحظه المشرع البلجيكي فقام بتعديل قانون التحقيق الجنائي بمقتضى قانون المؤرخ في((28 نوفمبر2000))حيث تم إضافة المادة -39- والتي سمحت بـ (ضبط الادلة الكترونية)، ومثل نسخ المواد المخزونة في نظام المعالجة الألية في البيانات, الغاية منه عرضه على السلطات القضائية [65]

وكما يتميز الدليل الكتروني في السعة التخزينية، والة الفيديو يمكن أن يخزين فيه مئات من الصور، وكذلك دسك صغير يمكن تخزين مكتبة صغيرة [66]

والدليل الإلكتروني له خاصية رصد المعلومات عن المجرم وتحليلها في ذات الوقت، وحيث يمكن ان تسجل حركات الشخص، وتسجيل سلوكياته, وكذلك بعض الامور الشخصية، لذلك فان الباحث الجنائي قد يجد غايتها وبسهولة ايسر من الدليل التقليدي [67]

وهناك نقول إن هذه الخصائص سبغت على الدليل الإلكتروني طابعاً مميزاً، فإصبح يعتبر الدليل الأفضل للأثبات في الجرائم الإلكترونية، وذلك لأنه ينتمي الى نفس البيئة التي ارتكبت فيه، سواء كانت هذه الجرائم مرتكبة بنظام المعالجة الألية أوكانت تشكل إعتداء أو مساساً على نظام المعالجة الألية [68]

---

(65) عائشة بن قارة مصطفى، مصدر سابق, ص64

(66) د.اشرف عبد القادرقنديل، مصدرسابق، ص127 وما بعدها

(67) خالد عياد الجلبي، مصدرسابق، ص233

(68) شهرزاد حداد, الدليل الإلكتروني في مجال الإثبات الجنائي, مذكرة لنيل شهادة الماجستيرفي الحقوق, تخصص قانون جنائي للأعمال, كلية الحقوق والعلوم السياسية, قسم الحقوق, جامعة العربي بن مهيدي,2017/2016, ص16

الفصل الثاني

المشكلات الإجرائية المتعلقة بكيفية الحصول على الدليل الإلكتروني

سنقسم هذا الفصل أيضاً الى مبحثين، سنتناول في المبحث الاول المشكلات المتعلقة بسلطات التحري وجمع الأدلة والتحقيق. وفيما يتعلق بالمبحث الثاني سنتناول الصعوبات المتعلقة بأحالة المتهم على المحكمة المختصة.

1.2: المشكلات المتعلقة بسلطات التحري وجمع الأدلة والتحقيق

الجريمة الإلكترونية شأنها شأن الجرائم الاخرى، يمر في مرحلة التحري والتحقيق الجنائي, وكذلك ما تترتب عليها من اجراءات قانونية وفنية، وكذلك اجراءات التحقيق الجنائي العام هو الاساس في تحقيق الجرائم الحاسوب، ذلك من خلال سماع الشهود وكذلك معاينة وقبض وأستجواب، ولكن اجراءات التحقيق الاخرى الفنية منها وكذلك النفسية تتوقف أستخدامها على ظرف كل جريمة مع مراعاة الخاصية الذي يتسم به الجريمة الإلكترونية (69)

وكذلك هناك صعوبة كبيرة فيما تتعلق في عمل سلطة التحري وجمع الأدلة وكذلك التحقيق سنبحثها كالأتي:-

المطلب الأول:- الصعوبات المتعلقة بعدم الإبلاغ عن الجريمة المعلوماتية.

المطلب الثاني:- نقص الخبرة لدى سلطات التحري وجمع الأدلة والتحقيق.

المطلب الثالث:- الصعوبات المتعلقة بضخامة كم البيانات المعلوماتية.

---

(69) د.عبدالفتاح بيومي حجازي، الدليل الجنائي في جرائم الكومبيوتر والإنترنيت, دار الكتب القانونية, المجلة الكبرى, مصر, 2005, ص67 ومابعدها.

المطلب الرابع:- صعوبة تفتيش جهاز الحاسوب الآلي.

المطلب الخامس:- صعوبة الحصول على شاهد في الجريمة المعلوماتية.

1.1.2: الصعوبات المتعلقة بعدم الإبلاغ عن الجريمة المعلوماتية

تبقى الجريمة المعلوماتية (الإلكترونية) مستترة مالم يتم الإبلاغ أو الأخبار عنه، وثم تحريك الدعوى الجنائية حسب القانون الساري, وكذلك صعوبة التي يواجه اجهزة الامنية وكذلك المحققين, السبب ان هذه الجرائم لا يصل الى اذهان السلطات المعنية بالصورة العادية، وكما هو بالنسبة للجريمة العادية، بسبب صعوبة اكتشافه مِنَ قبل الأفراد العادين او حتى الشركة والمؤسسة التي وقعت مجنيا عليه في هذه الجرائم، او أن هذ الجهة يحاول إخفاء الاثار السلبية في الاخبار عما يوقع له وحرصه على ثقة العملاء, ولا يبلغ عن الجريمة التي ارتكبت ضده.

تدخل هذا المؤسسة في اعتبارات ان الأخبار عن الجريمة الإلكترونية التي وقعت ضدها لربما سيؤدي ذلك الى احاطة المجرمين معرفة في نقاط الضعف في انظمتها، لاسيما البنوك الكبرى.

وبذلك يكون من الملائم لدى سلطات الأمنية في الجرائم الإلكترونية, وأكتشافها أن يرصد حركة المعاملات التجارية داخل المؤسسة المالية وحوله - وكذلك عن طرق جمع معلومات السرية وعن حركة السوق, وكذلك الاموال المتداول والممتلكات وأيضاً التغيرات الأجتماعية للموظفين وكذلك صغار رجال الاعمال الذين ينتمون الى هذه المؤسسات، وان جرائم الحاسوب هو من ادوات واسلحة هذه الجريمة، وبالتالي يجرى كسب وتعامل مع صغار الموظفين ومن الذين لهم خبرة فنية والذين لهم معرفة من اسرار برنامج الحاسوب في المؤسسات المالية, وكذلك الشركات التجارية, وبالتالي يرتبط ذلك في ضرورة تطور ثقافة الحاسوب في وسط رجال الامن, وكذلك ربط هذه الثقافة بالثقافة الامنية في صورها العادية، وهذا ما يضمن نجاح للاجهزة الامنية في مواكبة ظاهرة جرائم الحاسوب الآلي (70)

كذلك الجريمة في صورته العادية يصل الى أذهان سلطة التحقيق عن طريق الشكوى أو الأخبار, وأيضاً قد تصل علم بالجريمة الى أعضاء السلطة القضائية متى ما يتم ضبط الجريمة متلبس بوقوعه, أذا ان هناك

(70) د.عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر الإنترنيت، دار الكتب القانونية، مصر، 2007, ص109 ومابعدها

أجراءات وجوبية على عضو الضبط وسلطة التحقيق أتخاذها في حاة التلبس ومن معروف أن الجريمة يكون مشهودة تكون في بضع حالات هي:[71]

1. رؤية الجريمة إثناء ارتكابه.
2. أو رؤية الجريمة بعد ارتكابه ببرهة بسيرة.
3. أو متابعة المجرم عند وقوع الجريمة من قبل مجني عليه.
4. أو رؤية المجرم بعد وقوع الجريمة في وقت قصيرحاملاً اشياء او أوراق, أو فيه أثار يدل على أنه هو فاعل او شريك في الجريمة.

أما بالنسبة للجريمة المعلوماتي تصل العلم في وقوعها الى سلطات الضبط بإحدى الطرق الآتية [72]:

1) يتلقى سلطات الضبط أو أجهزة التحقيق المعلومات عن ممارسة أشخاص معروفين أو غير معروفين لانشطة يندرج تحت تعريف الجريمة الإلكترونية, ذلك من خلال مكان معروف, وعلى أجهزة محددة وفق لغات برمجية معلوماتية.
2) أو مسك الفرد وفي حوزته أموال مشبوهه أو بطاقة مزورة.
3) أو أخبار السلطات الضبط منَ قبل المجني عليه تفيد صدور تلاعب أو ممارسة خاطئة في حقه أو بحقوق الأخرين, سواءاً كان ذلك في صورة عجز مالي في حساب مؤسسات المالية او حصل تغيرات في الودائع, ودون بيان ما أن كان هذه الجريمة معلوماتية من عدمها, لأن عملية تكيف السلوك الإجرامي هي مسالة أخرى لا دخل لها بالمبلغ.
4) أو وجود معلومة عن نشر فايروسات تخريبية عبر مواقع (الإنترنيت).

وكذلك أن تطبيق القانون في مكافحة الفايروسات الإلكترونية التي يواجهه تحديات كبيرة [73]هي:-

- المجني عليه ليس له دراية بـ (المخرب) الذي صنع هذه الفايروس الذي هاجمها.
- أو المجني عليه ليس له الرغبة في الإبلاغ أو الأخبار بأن هناك فايروس في نظامه الإلكتروني, وذلك من أجل الحفاظ على الثقة بينها وبين الذين يستعملون مثل هذه النظم.

---

(71) المادة (1/ ب) من قانون اصول المحاكمات الجزائية العراقي

(72) د.عبد الفتاح حجازي، الاثبات الجنائي في جرائم الكومبيوتر والإنترنيت, دار الكتب القانونية، القاهرة, 2007، ص159 وما بعدها

(73) نقلاً عن د.عبادة أحمد عبادة, بحث بعنوان (التدمير المتعمد لأنظمة معلومات الإلكترونية), مركز البحوث والدراسات لدى شرطة دبي, دولة الإمارات العربية المتحدة, العدد 87, مارس, 1999م, ص4

- أو المجني عليه ليس له المعرفة بإصابة نظامها بفايروس الإلكتروني لمدة من الزمن, وكذلك من الصعب معرفة وقت الإصابة.
- أو عدم إمكانية معرفة الخسائر التي يحدثها هذا الفايروس.

وأيضاً مِنَ أجل تفعيل عملية الإبلاغ أو الأخبارعن الجريمة الإلكترونية عن طريق الحاسوب الآلي, من ثم المساهمة بطريق ايجابية من منع وقوع الجريمة او في سرعة أن يحصل على الدليل التي يتعلق به، وما طالب بعض في -الولايات المتحدة الامريكية- بان يتضمن القوانين التي تتعلق في الجرائم الحاسوب الآلي، نصوص يلزم موظفي طرف المجني عليه ايا كانت في ضرورة الأخبار عن ما تصل الى علمها من جرائم يتعلق في هذا المجال.

الإ انه عندما عرضه هذا الإقتراح على- الجنة الخبراء في المجلس أوربا- تم رفضه بسبب قانوني، وهو ان المجنى عليه (هو الشركة التي ارتكبت بحقها جريمة الإعتداء الإلكتروني) وسوف يصبح متهماً بعدما كانت مجنيا عليه, وبالتالي ظهور إقتراحات بديلة, وقد يكون بعضها مقبولة والبعض ملزمة بالإخبار جهة خاصة، او إخبار جهة اشرافية، وأن تشكيل جهاز خاصة بتبادل المعلومات وإصدار الشهادة – امن خاصة– لأن بعده يمنع مراجعة وتدقيق من قبل هيئة خاصة من المراجعين، وبالتالي يتعين على هذه الهيئة إخبار الشرطة بالجرائم التي تكشفها.

لذلك فان من الصعب الأخبارعن هذه الجرائم على نطاق دولي, ولا يوجد شبكات دولية بتبادل المعلومات الامنية, وهو ما موجود في شبكات يورب بول التي يعمل في أطار الشرطة الدولية.

وبذلك فإن الشرطة (الأنتربول) بدأت تتهم بمكافحة جرائم الإنترنيت, وانشأت لديه فرقة خاصة بهذا الغرض, وهي دائماً على اتصال بفرق مكافحة الجريمة الإلكترونية في اوربا والولايات المتحدة الامريكية وأستراليا, وكذلك الى تبادل المعلومة من أجل اكتشاف مثل هذا النوع من الجرائم(الإبلاغ) وكذلك تشديد الاجراءات الامنية في شان المعلومات والبيانات الحاسوب.

وهنا تثير مسألة الإبلاغ أو الأحبارعن الجريمة الإلكترونية عن طريق الحاسوب الآلي, والمسائل يتعلق في مدى ماهو متاح من النصوص في الأنظمة الجزائية التي يوجب الأخبار ويرتب عقوبات على ذلك [74]

(74) د.عبد الفتاح حجازي، مبادئ الاجراءات الجنائية في جرائم الكومبيوتر الإنترنيت، مصدر سابق, ص116 ومابعدها

وفي القانون العراقي عدا الجرائم التي علق عليه القانون بتحريك الدعوى فيه وعلى شكوى أو طلب من المجني عليه, ويحقً لكل فرد التبليغ عن الجريمة, وذلك قد نص –المادة 47- من قانون (أ.م.ج) (رقم 23 لسنة 1971)على أنه لـ (من وقعت عليه جريمة ولكل من يعلم في وقوع الجريمة تحرك الدعوى فيها وبلا شكوى أوعلم في وقوع موت مشتبه به أن يبلغ قاضي التحقيق أوالادعاء العام أو أحد مراكز الشرطة).

وهذا هي القاعدة العامة يحق لكل شخص أو فرد في الأخبار طالما ان الجريمة ليست مما يلزم الى تحريك الدعوى عنها شكوى أو طالب من الجهة التي حدده القانون, وبالتالي من حق كل من يعلم في وقوع الجريمة الكترونية أن يبلغ عنها أذا لم ينص القانون على غير ذلك.

ويوجد هناك حالات من الممكن الأخبار عنها واجبا على كل شخص يعلم في وقوع الجريمة, وتترتب على الأخلال في هذا الواجب جزاء جنائي او تأديبي, لقد اوجب (المادة 219) من (ق.ع.ع) أن كل من يعلم في وقوع جريمة من الجرائم التي نص عليه في الباب الثاني من هذا القانون [75], ان يسرع في الإبلاغ الى السلطة المختصة والإعوقب بالحبس والغرامة أو بإحدى هاتين العقوبتين.

وكذلك نص (المادة247) من القانون المذكوراعلاه على ان (يعاقب بالحبس أو بالغرامة كل من كان ملزمً قانوناً بأخبار أحد العاملين في خدمة عامة عن امر ما أو أخباره عن أمور معلومة له فإمتنع عمداً عن أخبار في الكيفية المطلوبة, وكذلك في الوقت الواجب قانونا. وكذلك كل مكلف في خدمة عامة أعطى له البحث عن الجرائم أو ضبطها اهمل الأخبار عن جريمة أتصلت في علمه, ذلك كل مالم يكن رفع الدعوى معلقا على شكوى).

وأيضأ فان (المادة 48) من قانون (أ.م.ج) [76], فقد أوجبت على المكلف في خدمة عامة ان يخبر عن الجرائم التي يعلم بها اثناء تأدية واجبة أو بسبب تأدية, وبشرط أن لا يكون من الجرائم الحق الشخصي, وكذلك تكون الإبلاغ واجبا على الموظف, والا يتعرض الى المساءلة التاديبية. وايضاً من هذه الناحية ويجب على اي موظف أوالمكلفين في خدمة عامة وذلك حسب النص أن يخبروا عن اي جريمة علموا بها والا يتعرض الى المسائلة.

---

(75) يشمل الجرائم الماسة بأمن الدولة الداخلي

(76) نص المادة 48 (كل مكلف في خدمة عامة علم إثناء تادية عمله أو بسبب تاديته في وقوع جريمة أو أشتبه بوقوع جريمة تحرك الدعوى فيها بلا شكوى ويخبرون فورا احدى ممن ذكرو في المادة(47))

من المفروض الإبلاغ المقرر في نص المادة (48) أصولية لا تمتد الى أولئك العاملين في القطاع الخاص ومؤسساتها وشركاتها, وهي أغلب الجهات التي يستخدمون أجهزة الحاسوب, مثل الشركات والمصانع الكبيرة التي هو ليس ملكاً الى الحكومة, أو أنه لا تشترك فيه في النصيب.

كذلك من ضرورة الإسراع في وضع تشريع ينظم العقوبة على الجرائم الإلكترونية أو ضبط قانون العقوبات والقوانين ذات العلاقة لكي تستوعب العقوبة على مثل هذه الجرائم.

وأيضاً أن المشرع الاماراتي جعل الإبلاغ عن الجريمة ملزماً كـ (قاعدة عامة), وبالتالي من خالف هذه القاعدة سوف يتعرض الى الجزاء الجنائي, ولذا أوجب (المادة37) من قانون الاجراءات الجزائية الأتحادية (رقم 35 لعام1992) على كل من يعلم في وقوع جريمة مما يجوز للادعاء العام رفع الدعوى عنه من غير شكوى او طلب ان يخبر الأدعاء العام او احد أعضاء السلطة القضائية عنه, وكذلك نص (المادة 38) من نفس القانون على (أنها يجب على كل من يعلم من الموظفين او المكلفين في خدمة عامة اثناء تادية واجبه او بسبب تاديته في وقوع جريمة, ومن الجرائم التي يجوز للادعاء العام رفع الدعوى من غير شكوى او طلب ان يخبر فورا الادعاء العام او اقرب أعضاء السلطة القضائية), وكذلك رتب المشرع على الاخلال لهذا الواجب عقاب جنائي, اذ نص (المادة2/272) من قانون العقوبات الاتحادي على انه (يعاقب بالغرامة كل موظف غير مكلف في البحث عن الجرائم أوضبطها أهمل او ارجا اخبار السلطة المختصة في جريمة يعلم به إثناء او بسبب تاديته وظيفته, ولا عقوبة أذا كان رفع الدعوى معلق على شكوى).

ويؤدي ذلك الى معاقبة الموظف جنائياً بسبب عدم الإبلاغه أوالإهماله فيه, حتى وان لم يكون مكلف بالبحث عن الجريمة [77]

وان في هذا الحالة هناك أختلاف في القانون العراقي والإماراتي عن القانون المصري في ان القانون العراقي والإماراتي جعل هذا الفعل بـ (مثابة جريمة جنائية) معاقباً عليه بغرامة, بينما الأمر في القانون المصري يختلف اذ يكتفي بالعقاب التأديبي.

كذلك أختلف القانون الاماراتي عن العراقي والمصري على أنها جعل الإخبار جريمة عامة, حتى على المواطن العادي, وكذلك بالنسبة الى كل الجرائم وليست لجريمة خاصة, وكما هو بالنسبة للجرائم امن الدولة, وحسب (المادة 84) من (ق.ع.المصري) وكذلك نصت (المادة 274)من (ق.ع. الإماراتي على انه"يعاقب

(77) راضية سلام عدنان، مشروعية الدليل الإلكتروني، بحث مقدم الى مجلس كلية الحقوق وهو جزء من متطلبات نيل البكالوريوس في الحقوق، جامعة النهرين،2015، ص32

بالغرامة لا تجاوز الف درهم كل من يعلم في وقوع الجريمة وإم الإمارات تنع عن أخبار ذلك السلطات المختصة".

وبالتالي عدم أخبار تعد جريمة بالنسبة للشخص أو المواطن العادي, أذ لم تتوافر فـي حقه سبب للاعفاء كـ(علاقة القرابة والمصاهرة).

وصفة هذا النص أنه فضلا عن الزام الشخص العادي بأخبار حتى لو كان في الجرائم الإلكترونية التي يصل الى علمه, لانها بلزم أيضاً موظفي شركة القطاع الخاص, والتي يستخدمون الحاسوب, ومتى ما علموا بالجريمة لها صلة بالحاسوب الآلي, ويصنف من ضمن الجرائم الإلكترونية, ويترتب على هذا الإبلاغ جزاء جنائي من قبل المتخاذل وبالتالي ان كل هذا كان في مصلحة الدعوى الجنائية وإمكانية جمع الادلة بشأن الجرائم الإلكترونية [78]

2.1.2: نقص الخبرة لدى سلطات التحري وجمع الأدلة التحقيق

من الصعوبات التي يواجه عمليات استخراج الأدلة في الجرائم التي ترتكب عبرالإنترنيت هو نقص الخبرة أو المعرفة لدى أعضاء الضبط القضائي او اجهزة الامن بـ (صفة عامة)، وأيضاً لدى اجهزة العدالة الجنائية المتمثلة بسلطات الإتهام والتحقيـق الجنـائي، وكذلك فيما تتعلق بالثقافة الحاسوب والالمام بالعناصر الجرائم التي ترتكب عبر الإنترنيت عن طريق الحاسوب الآلي وتعامله معه في دول العربية، والسبب في ذلك هو التجارب الأعتماد على الحاسوب وتقنياتها وأنتشارها في هذه الدول جاءت متاخرة عـن أوربا والولايات المتحدة، وان اجهزة العدالة التي تكافح الجرائم التي ترتبط في هذه التقنية تبدأ بالتكوين والتشكيل بعد ما ظهر هذه الجرائم، وهو امر تستغرق وقتا أبطأً من وقت أنتشار الجريمة لان هـذه الجـريمة تتطور وبسرعة فائقة يساوي سرعة تطور التقني نفسها، وحتى الان فان الثقافة الامنية او القانونية في خصوص هذه الجرائم لا تسير بنفس المعدل، وهذا الفارق في التقدم الذي ينعكس سلبا على فنية اجراء التحري والتحقيق في الدعوى الجنائية عن الجريمة المرتكبة عبرالإنترنيت، وهنا تأتي الدعوى الى وجوب تاهيل سلطات الامن وجهات التحقيق والإدعاء والحكم بشأن هذه الجرائم [79]

وهذا ما تتطرق إليه الفقه الجنائي ان البحث والتحقيق في جرائم الحاسوب هي مسالة في غاية الأهمية، ولأسيما بالنظر لاعتبارات التكوين العلمي والتدريبي والخبرة التي اكتسبها اعضاء السلطة القضائية ,وكذلك

---

(78) د.عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكومبيوتر والإنترنيت، مصدر سابق, ص80

(79) د.عبد الفتاح حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنيت، مصدر سابق, ص81

سلطات التحقيق الجنائي، وذلك ان تجديد هذه الجرائم وتقنياتها العالية يتطلب من العاملين على البحث والتحقيق إلماماً كافياً به، وهذا لا يكفي ان تكون عندهم الخلفية القانونية, وبالتالي لابد من الالمام بخبرة الفنية في الجريمة المرتكبة عبرالإنترنيت [80]

إن المشكلة هي ليست في منح الموظفين الذين لهم صلة بجرائم الإنترنيت صفة عضو الضبط القضائي، وذلك أن عضو الضبط العاملين بالفعل وسلطات التحقيق الجنائي تنقصهم الخبرة والثقافة في الجريمة التي ترتكب عبر الإنترنيت، وأن نقص الخبرة عند رجال الأمن والتحقيق العاملين في مجال مكافحة الجرائم المرتكبة عبر الإنترنيت هو خير دليل لمرتكبي جرائم الإنترنيت.

أن الواقعة اثبتت أن هناك جرائم تتعلق بالإنترنيت ارتكبت على مرأى ومسمع من قبل رجال الشرطة، وكذلك قيام بعض رجال الشرطة في تقديم يد العون لمرتكبي جرائم الإنترنيت من دون عمد وعدم الأدراك، وإذا كان هذا هو حال الاشخاص التي اعطى لهم إنفاذ القوانين وكذلك حماية المجتمع من الأشرار، فإننا حسب أن الكثير من عامة الناس قد يقع في حقهم او بتسهيل منهم جرائم الإنترنيت [81]

وأن التحديات التي تواجه أجهزة التحقيق الجنائي في جرائم الإنترنيت ان الجناة في هذه الجرائم لهم المصطلحات الخاصة بهم، الى درجة أنهم يسمون أنفسهم أسم – النخبة - وبدعوى انهم الاكثر دراية بأسرار الحاسوب ولغاته المتميزة، ويطلق على رجل الامن والقضاء صفة الضعفاء او القاصرين.

وبدأت بعض الدول محاولة في استقطاب رجال الأمن والقضاء من ضمن المختصين في علوم وتطبيقات الحاسوب, فضلاً عن قبولهم خبراء هذا المجال ضمن رجال الضبط والقضاء، وبالتالي هذه المحاولات لن يأتي بثمارها في القريب العاجل للأتي[82]:-

(1) الميزانيات المالية الموجودة في الأجهزة الحكومية تكون ضعيفة بالنسبة الى الخبرات المختصين في الحاسوب الآلي, وأن ذلك المبالغ لا تصل الى المبالغ التي يسددها مؤسسات وشركات القطاع الخاص.

(2) جرائم المرتكبة عبر الإنترنيت نوع من الجرائم التي تستحوذ على أهتمام الشرطة وكذلك القضاء ضمن منظومة اخرى من الجرائم التي نصت عليها قانون العقوبات، وبذلك فأن الجرائم

---

(80) د.عبدالفتاح حجازي، مبادئ الاجراءات الجنائية في جرائم الكومبيوتر الإنترنيت، مصدر سابق, ص122 ومابعدها

(81) صغير يوسف, الجريمة المرتكبة عبر الإنترنيت, مذكرة لنيل شهادة ماجستير, جامعة مولود معمري, كلية الحقوق والعلوم السياسية, الجزائر, 2013, ص122

(82) د.محمد الأمين البشري، التحقيق في جرائم الحاسوب الآلي, بحث مقدم الى مؤتمر القانون والكومبيوتر والإنترنيت, المنعقد في الفترة من 1- 5/3/ 2000, كلية الشريعة والقانون, في دولة الإمارات العربية المتحدة, ص366

المرتكبة عبر الإنترنيت ليس هو كل أهتمام الشرطة او القضاء، ولكن هنالك جرائم اخرى، وصحيح, وأن الجريمة المرتكبة الإنترنيت قد يكون صاحب الشهرة الاوسع والإهتمام الاكثر من قبل اجهزة التحقيق، ولكن ان الجريمة العادية كـ(جريمة التزوير) قد يرتكب عن طريق الحاسوب، وأيضاً بالنسبة لجريمة تزييف العملة، ومع ذلك يبقى الجرائم المرتكبة عبر الإنترنيت كـ(نوع من الجرائم) من ضمن أهتمام اجهزة التحقيق الذي يشير الى بقية أنواع الجرائم وهذا ما يطلق عليها الجرائم العادية.

(3) أن الخبرة العلمية لدى سلطة التحقيق الجنائي تأتي من خلال ممارسة اعمال الضبط والتحقيق والتدريب عليها، وذلك يقتضي وقوع هذه الجرائم موضوع الضبط والتحقيق، وبالتالي فأن الجريمة المرتكبة عبر الإنترنيت لم يقع الى هذه لحظه بالعدد والشكل الذي يحاذي جريمة العادية كـ(السرق او القتل)، وبالتالي فالخبرة الإجرائية في الضبط والتحقيق لدى اجهزة العدالة في شأن الجريمة الإنترنيت مازالت جديدة، ومع أنتشار الحاسوب وظهوره في الحياة العامة والخاصة، وما يستتبعها من افعال مخالفة (وليس مجرم) وذلكً بسبب عدم وضوح الرؤية بشأن نصوص التجريم، لان ذلك سوف يزيد عمل سلطة الضبط والتحقيق في مستقبل.

(4) أن أنتشار الحاسوب الآلي على مجال واسع وتنوع أنظمتها وبرامجها وتتطورها وبشكل سريع, ويجعل متابعتها من حيث إعدادها وتدريب رجال الضبط والتحقيق الجنائي عليها ويعتبر في غاية الصعوبة، مع ذلك يجب أن لا يكون ذلك مبررا, والسبب في ذلك لان التدريب على جهاز الحاسوب لهو فائدة في كل الاحوال، علما ان هذه اجهزة عند تدريب عليها ستكون قابلة لتحديث، وبالتالي فإن القواعد العامة في فنون الحاسوب الآلي والجريمة المرتكبة عبر الإنترنيت موجود لديهم اساساً، وبدلاً من عدم تدريبهم أصلاً.

بالأضافة الى ذلك أن هنالك مشاكل وتحديات خاصة تتعلق في مواجهة الجريمة المرتكبة عن طريق الإنترنيت وهذه الجرائم يعود اساساً الى طبيعة تداول المعلومة على هذه المواقع, وبالتالي يؤدي الى إرهاق سلطات الضبط والقضاء، وهذه الصعوبات وتحديات يتمثل في الاتي [83]:

1- شهد قطاع التكنولوجيا المعلوماتية طفرة واسعة وسريعة في الانتاج الكمي والنوعي، أضافة إنه يمكن الاشتراك بالشبكة في كافة المجالات الأجتماعية والأقتصادية.

2- لا يوجد قانون دولي أو نص دستوري تجرم مثل هذا الافعال الاجرامية حتى الان, على حد أطلاعي كونها لا يزال يعتبرمن الجرائم ذات الطابع الحديث في الشكل والمضمون.

---

(83) د.عبد الفتاح حجازي، مبادى الإجراءات الجنائية في جرائم الكومبيوتر الإنترنيت, مصدر سابق, ص127 وما بعدها

3- لا يوجد قضاء مختص في الجرائم الإلكترونية.

4- لا يوجد شبكة دولية لكي يتبادل المعلومات الامنية.

5- من الصعب السيطرة على المشتركين, وكذلك لا يوجد ضوابط محلية أو دولية يحدد أهداف المستخدم.

6- صعوبة معرفة المسؤول عن هذه الجرائم, لان هناك بعض المواقع على الإنترنيت يسهل إرسال الرسائل من دون أن يحدد أسم المرسل.

3.1.2: الصعوبات المتعلقة بضخامة كم البيانات المعلوماتية

أن رجال الضبط والتحقيق الجنائي في الجرائم المرتكبة عبر الإنترنيت يواجهون تحديات كبيرة في كمية المعلومات والبيانات الضخمة, والتي هي بحاجة الى فحص ودراسة لكي يستخرج منها الأدلة هذه الجرائم، فضلاً عن ضرورة أن يتوافر لدى رجال الضبط أوالمحقق الخبرة الفنية في مجال الحاسوب الآلي والمعلوماتي، ويتعين أيضاً أن يتوافر لديهم القدرة على فحص ودراسة هذا الكم الهائل من المعلومات والبيانات المخزونة على جهاز الحاسوب الالي أوعلى ديسكات أو اسطوانات منفصلة.

لهذا السبب يمكن أن نقول أن ضخامة هذه البيانات والمعلومات يكون عائقا في تحقيق جرائم المرتكبة عبر الإنترنيت، وبالتالي أن استنساخ كل ما هو موجود على جهاز الحاسوب، ويتطلب العديد من الصفحات, والتي لا تقدم شيئاً مفيداً الى التحقيق.

وهذا عكس ضخامة أو كثرة المعلومة في الجرائم العادية كـ(القتل أوالسرقة)، وذلك أن كثرة المعلومة في مثل هذه الجرائم هو أمر يساعد رجال الضبط أو المحقق في استخراج الأدلة الجنائية في هذه الجريمة[84].

وكذلك في ظل المستوى الفني لرجل الضبط والمحقق الجنائي التي تتعلق بفن الحاسوب وأستخداماته، فأنه يكون من الممكن الاستعانة بالخبراء فنيين في مثل هذه الجرائم, حتى يتمكن من فرز المعلومات التي يحتاجونها في التحقيق عن تلك التي لاحاجة لها، والا رجل الضبط والمحقق يواجه صعوبات وتحديات في الحصول على هذه المعلومات، ويتطلب ان يكون ندب هؤلاء الخبراء وجوبياً, وبعد ذلك تعديل التشريعات الجنائية القائمة التي يجعل- ندب خبير- في الدعوى أمراً جوازياً الى المحقق إن شاء أمر به أو رفضه، وذلك بسبب طبيعة الجريمة التي يتطلب التعامل معها وبطريقة فنية تفوق قدرات رجل المحقق إلا اذا كان مؤهلً لهذا الغرض،

---

(84) د.عبد الفتاح بيومي حجازي, الدليل الجنائي والتزوير في جرائم الكومبيوتر والإنترنيت, مصدر سابق, ص168 ومابعدها

فيمكنه الاعتماد على قدراته الشخصية في ضبط هذه الجرائم بشرط أن لا يخرج عمله عن الأصول الفنية المتعارف عليه.

لذلك يحاول الخبراء في مجال الجريمة المرتكبة عبر الإنترنيت طرح حلول قانونية وعلمية لمكافحة هذه الجريمة في ظل شيوع الدليل الإجرامي فيها، ويكون هدف هذه الحلول هو إما مساعدة الجهات المجني عليها في استرداد أموالها التي فقدت جراء هذه الجريمة أو تقرير عقوبة جنائية على تلك الجهات التي تتعرض الى الجريمة دون أن يكون لديها وسائل حماية فنية تؤمنها أو عن طريق فتح المحاكم سلطات تؤمن بعدم الإستيلاء على أموال الجهات المجني عليها أو مصادرة هذه الاموال متى ما عجز المجرم الإلكتروني عن إثبات مصدرها كما هو الحال في انجلترا وفرنسا [85].

4.1.2: صعوبة تفتيش جهاز الحاسب الآلي

قد يواجه الشخص المعلوماتي أثناء قيامه بتفتيش الحاسوب بعض الصعوبات وتكمن هذه الصعوبات فيما يلي:-

أولاً- إذا كان الحاسوب محمياً بكلمة سر:

إذا كان الحاسوب محمياً بكلمة سر قد يعمد المتهم الى حماية حاسوبه الذي ارتكب بواسطته الجريمة الإلكترونية بكلمة سر(Pass Word) بحيث لا يمكن لأحد غيره الدخول الى الحاسوب الآلي، وفي هذه الحالة يكون أمام الشخص القائم بالتفتيش خياران هما، - الخيار الأول - أن يطلب من مشغل الحاسوب الكشف عن كلمة السر, وإذا لم يتم كشف كلمة السر من قبل مشغل الحاسوب أو المتهم يلجأ الشخص القائم بالتفتيش الى - الخيار الثاني - وهو استخدام التكلنوجيا في فك رمز الدخول الى الحاسوب (الكمبيوتر).

وأن وضع كلمة سر الى الحاسوب من الأمور السهلة الذي يمكن لأي شخص له المام ودراية بسيطة بالحاسوب أن يضعها على الكمبيوتر، لكن من صعب فك رمز الدخول الى الكمبيوتر، بل يحتاج في أغلب الأحيان الى مدة زمنية طويلة من أجل فك رمز الدخول الى الحاسوب، وهناك برنامج خاصة بكشف كلمات السر (Pass Word) ومن هذه البرامج، برنامج - Access Date – وبرنامج (Soft Ware Crar)وفي أغلب الأحيان تكون كلمات السر سهلة، قد يضع المتهم أسمه أو تاريخ ميلاده أو السنة الميلادية وغيرها من الرموز التي يسهل على الشخص تذكيرها، لذلك على القائم بالتفتيش طلب بعض المعلومات الخاصة من المتهم، كـ

(85) د.عبد الفتاح حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر الإنترنيت, مصدر سابق, ص149

(ألإسم والمواليد وأسم الأب والزوجة, ورقم الهاتف) لمحاولة فتح كلمة السر, فأن تعذر عليه ذلك يجب أن يلجأ الى البرامج الخاصة بفتح الرموز [86]

ثانياً - أذا كانت البيانات مشفرة (تشفير البيانات والمعلومات):

قد يلجأ المتهم الى تشفير البيانات المخزونة في جهاز الحاسوب للحيلولة دون الوصول الى الأدلة التي تدينه والجاري البحث عنها من قبل القائم بالتفتيش، (وتشفير البيانات) يعني تحويل الرسالة الى صيغ سرية بأستعمال أحرف تعويضية محل أحرف الاصلية او عن طريق تبديل موضع أحرف للرسائل الاصلية, وعملية التشفير تتم وفق معادلات رياضية معقدة تسمى الخوارزميات [87]

ويعرف التشفيربأنه (يقصد بتشفير البيانات وكتابتها برموز سرية بحيث لا يمكن فهمها الا من خلال الحائز على مفتاح هذه الشفرة) [88]

وبالتالي يكون أمام القائم بالتفتيش خياران لمعالجة مشكلة التشفير هما، "الخيار الأول" هو طلب مفتاح الشفرة من المتهم, وأذا لم يتمكن من الحصول على المفتاح يلجأ الى استخدام التكنولوجيا الحديثة في فك الشفرة, وتسمى هذه العملية بعلم (تحليل الشفرات)، والذي يعرف بأنه علم إسترجاع النص بدون معرفة المفتاح, وتتم هذه العملية من قبل شخص يسمى - محلل الشفرة - والذي يكون ذو قابلية كبيرةً في الرياضيات التطبيقية وفروعها المختلفة مثل نظرية الأحتمالية ونظرية الأعداد والأحصاء والجبر [89]

وأن نجاح أو فشل عملية تحليل الشفرة يعتمد بالدرجة الأولى على الخبرة والإمكانيات التي يتمتع بها محلل الشفرة, وبالتالي كلما كان محلل الشفرة بإمكانيات علمية عالية كان فك الشفرة أسهل ولا يستغرق وقت طويل والعكس صحيح.

ثالثآ: وجود فايروسات داخل الحاسوب:

الفايروس VIRUSES: هو برنامج صغير غير مرغوب فيه, ويتم ادخاله على جهازالحاسوب الآلي من غير أن يعلم المستخدم, والغرض منه تخريب بعض او جميع البرامج والاجهزة المكونة للحاسوب الالي [90]

---

(86) د.سامي فقي حسين, مصدر سابق, ص223

(87) د.سامي جلال فقي حسين, المصدر نفسه, ص224

(88) د.عمار عباس الحسيني, جرائم الحاسوب والإنترنيت(الجرائم المعلوماتية), الطبعة الاولى, بيروت, لبنان, 2017, ص325

(89) د.علاء حسين حمامي, د. محمد علاء الحمامي, إخفاء المعلومات – (الكتاب المخفية والعلامة المائية), اثراء للنشر, عمان, الأردن, 2008, ص48

(90) د.سامي جلال فقي حسين, مصدر سابق, ص225

وكان أول ظهور للفايروس في عام(1981), أذ صنع العلماء فايروس الكمبيوترهدفه التجربة, ثم بدء الحاسوب بالإنتشار حتى وصل الى الفايروسات المعروفة في الوقت الحاضر, وفي عام (1987) شهد أول ظهور لفايروسات تستهدف الملفات التشغيلية وسمي بأسم فايروس [91]

وينتقل الفايروس من حاسوب الى حاسوب آخر بعدة طرق, فقد ينتقل عن طريق نسخ البرامج, أذ ينتقل الفايروس أوالمعلومات داخل الكمبيوترعن طريق أدخال برنامج منسوخ الى جهاز الحاسوب, وتنتقل العدوى الى الحاسوب أو يكون البريد الاكتروني وسيلة سهلة لنقل الفايروس, ومن هذه الفايروسات فايروس عيد الميلاد أو يدخل من قبل أشخاص الى الجهاز لغرض تدمير وإتلاف الحاسوب [92]

تقسم فايروسات الحاسوب الآلي الى عدة أقسام:

1. **فايروس عام العدوى:** هو ينتقل الى اي برنامج او ملف, ويعمل على تدمير أنظمة تشغيل الحاسوب بكامله.
2. **فايروس محدود العدوى:** ويستهدف هذة النوع أنواعآ معينة في أنظمة الحاسوب فيهاجمه, ويتميز ببطء الانتشار ويكون صعبآ من حيث إمكانية اكتشافه.
3. **فايروس عام الهدف:** وهو ما يندرج تحت أغلبية العظمى من الفايروسات التي يتم أكتشافها, وتتميز في سهولة اعداده, وأتساع مدى تخريبه.
4. **فايروس محدود الهدف:** هذا الفايروس يقوم بتغير الهدف من عمل البرامج دون تعطيله, وهذه النوع من الفايروسات يحتاج الى مهارات عالية في تطبيق المستهدف, كأن يعمل تلاعبآ ماليآ او تعديلاً معينا لتطبيق عسكري مثل فايروس حصان طروادة الذي ينتشر عبر الإنترنيت [93].

وتستخدم الفايروسات لغرضين هما (**حمائي**) ويكون لحماية جهاز الحاسوب بما تحتوي من بيانات وبرامج من خطر النسخ غير المشروع, اذ ينتشر الفايروس بمجرد النسخ ويخرب جهاز أنظمة الحاسبات الآلي الذي يعمل عليها.

والغرض(**تخريبي**) ويكون هذه الفايروس واضح وهو تخريب نظام جهاز الحاسوب أو من أجل الحصول على المنافع الشخصية.

---

(91) منير محمد الجنبيهي وممدوح محمد الجنبيهي, امن المعلومات الالكترونية, دار الفكر الجامعي, الإسكندرية, 2006, ص48

(92) د.محمد أمين الرومي, جرائم الكومبيوتر والإنترنيت, دار المطبوعات الجامعية, الإسكندرية, 2004, ص60

(93) محمد أمين أحمد الشوابكة, جرائم الحاسوب والإنترنيت, دار الثقافة, عمان, 2004, ص239

وهناك أنواع عديدة من الفايروسات نذكر بعض منها:

1ـ **حصان طروادة:** وهو الأخطر لأنها تأخذ صلاحيات مدير نظام وتعمل بسرية تامة ومن دون علم المستخدم, وهوعبارة عن برنامج يتمتع بقدرة عالية على الاختفاء داخل البرنامج الأصلي الموجود داخل جهاز الحاسوب لكي يعمل أثناء التشغيل بحيث يؤدي الى تعطيل البرامج أو تغييره أو محو البيانات, وهدف من هذا البرنامج هو إدخال بيانات غير صحيحة الى البرامج مثبت داخل جهاز الحاسوب, الغاية منها تخريب قاعدة البيانات التي يعتمد عليها جهاز الحاسوب في تشغيله ويصعب اكتشاف هذا البرنامج الا من خلال مكافح الفايروسات, وذلك لأن برنامج حصان طروادة يحتوي على معلومات معينة من الصعب ملاحظتها.

2- **برنامج الدودة:** هو عبارة عن برنامج تشغل أية فجوه في أنظمة التشغيل لكي ينتقل من جهاز الحاسوب الى حاسوب آخر, ومن شبكة الى اخرى وعبر الوصلات التي يربط بينهما, وكذلك يتكاثر في اثناء أنتقاله (كالبكتريا)وتجتاج الى النسخ منها.

ومن امثلة على هذا البرنامج ما يعرف بـ (Inter warm) هو برنامج الذي أعده الطالب الامريكي روبرت مورس الذي كان طالباً للدراسات العليا في جامعة كورنيل في (نيويورك) وأدخل هذا الفايروس الى شبكة المعلومات وتسبب في تدمير وتعطيل الاف الأجهزة [94].

3ـ **القنابل المنطقية أو القنابل الزمنية:** القنبلة المنظقية هوعبارة عن برنامج صغير تنفذ في لحظة محدودة او في كل فترة زمنية منتظمة, وكذلك يتم وضعها في شبكة المعلومات, الهدف منها هوتحديد ظروف لغرض تسهيل العمل الغير مشروع, أما **القنبلة الزمنية:** هو عكس الحالة السابقة وهي ينطلق أو ينفجر في لحظة زمنية محدودة حسب توقيتها [95]

وأن أصابة الحاسوب محل التفتيش تؤثرعلى عمل الشخص القائم بالتفتيش في تفتيش البيانات المخزونة داخل جهاز الحاسوب, وذلك لأن الفايروسات يسبب أضراراً كبيرة للحاسوب المصاب بها, ومن هذه الاضرار التي يعيق عمل القائم بالتفتيش في فقد البيانات من ذاكرة جهاز الحاسوب, وتتكاثر الفايروسات داخل ذاكرة الحاسوب, أنه يخلق حياة ذاتية لنفسه, وعندئذ يقوم الفايروس بمسح أجزاء من الملف المخزنة, ويجعل هذا الملف غير قابل للإسترجاعها, والمستخدم لا يستطيع أن يصل الى الملفات المفقودة, وبعض الفايروسات تقوم أحياناً بالهجوم على الفهرس الرئيس لنظام الحاسوب بعدة وسائل منها تغير حرف واحد في هذا الفهرس,

---

(94) د.سامي جلال فقي حسين, مصدر سابق, ص226 وما بعدها

(95) د.محمد سامي الشوا, ثورة المعلومات وانعكاساتهاعلى قانون العقوبات, دار النهضة العربية, مصر, 1994, ص169 وما بعدها

وكذلك لا يستطيع الوصول الى أي ملف على القرص رغم وجود الملفات فعلياً, وبالتالي قد تؤدي أصابة الحاسوب بالفايروس الى تغيير ملفات أو برامج داخل جهاز الحاسوب, والذي يؤدي أيضاً الى عدم التمكن من الوصول الى الملفات المخزونه وغيرها من الاضرار [96]

رابعاً- حذف المعلومات أو إخفائها:

قد يتعمد المتهم الى إخفاء المعلومات محل الجريمة أو حذفها من ذاكرة جهاز الحاسوب محل التفتيش, وبالتالي يواجه القائم بالتفتيش مشكلة في اكتشاف مكان هذا المعلومات أو استرجاعها, وعرفت إخفاء المعلومات (Steganog raphy) بأنها هو تقنية إخفاء البيانات السرية داخل البيانات اخرى, الهدف منها إخفاء البيانات لتجنب الكشف, ويمكن إستخدام إخفاء المعلومات لإخفاء أي نوع من المحتوى الرقمي, ويمكن ان تكون عبارة عن ملفات الصور أو الصوت أو النصوص أو الفيديو, وقد تكون البيانات تنفيذية للبرامج [97]

وبإمكان قيام المتهم بإخفاء المعلومات في مساحة معينة من القرص, وتكون هذا المساحة غير مستعملة أو مستخدمة, وتكون ملفات أنظمة التشغيل مكاناً مناسباً لإخفاء المعلومات, وذلك لأن هذه الملفات تنتج مساحات غير مستخدمة, وتظهر أنها مخصصة لخزن الملفات, وهذا المساحة المخصصة تعرف بأسم مساحة الهادئة (slack) [98]

وبذلك يصعب اكتشاف المعلومات المخفية اذا كانت مخفية بصورة جيدة, وكذلك لم تترك أي اثار, وبالتالي لا يمكن القائم بالتفتيش من إكتشافها وتسمى هذه التقنية التي تتم بواسطتها اكتشاف المعلومات بـ(تحليل البيانات المختفية) (steganalysis) وهي تتم من قبل محلل الكتابة المخفية (steganalys) أو تحليل المعلومات المخفية, وتتم أيضاً بطرق رياضية معقدة لا يفهمها الا المحلل نفسه.

لكن إخفاء المعلومات من قبل المتهم قد يعيق بشكل كبير من مهمة الشخص القائم بالتفتيش في اكتشاف المعلومات, لذا يجب ان يكون الشخص القائم بالتفتيش على علم ومعرفة كبيرة بتقنية إخفاء المعلومات.

وكذلك قد يقوم المتهم بحذف البيانات من ذاكرة الحاسوب بعد إرتكابه الجريمة الإلكترونية, وكذلك يتوجب على الشخص القائم بالتفتيش إستخدام التقنيات الخاصة باستعادة البيانات المفقودة, وتعرف باستعادة البيانات المفقودة بأنها (data recovery) هي عملية استعادة هذه البيانات المحذوفة من الاقراص الصلبة وغيرها

---

(96) محمد العريان, الجرائم المعلوماتية, دار الجامعة الجديدة, الاسكندرية, 2004, مصدر سابق, ص93

(97) د.سامي جلال فقي حسين, مصدر سابق, ص228

(98) د.علاء حسين حمامي, د.محمد علاء الحمامي, مصدر سابق, ص208 ومابعدها

من وسائط الخزن والتي حذفت بالفعل حوادث معنية فنية كـ(إرتفاع الطاقة الكهربائية في جهاز الحاسوب أو في تعمد حذفها) (99)

خامساً- عدم معرفة مكان ووجود الملفات داخل جهاز الحاسوب الآلي:

من الممكن أن تكون هذه المعلومات محل التفتيش غير معروفة الموقع داخل جهاز ذاكرة الحاسوب الآلي المراد تفتيشه, وفي هذه الحاله يمكن للشخص القائم بالتفتيش العثور على البيانات والمعلومات المخزونة داخل جهاز الحاسوب اذا تمكن من معرفة إسم الملف المخزونة الذي فيه معلومات, يتم ايجادها عن طريق البحث العام عن الملفات, حيث يتم ذلك عن طريق ادخال إسم الملف ونوعه ويتم البحث عنها تلقائيا من قبل الحاسوب الآلي, ولكن هذه الطريقة تكون صعبة ومستحيلة, لان الشخص القائم بالتفتيش لا يعرف اسم الملف ونوعه, وهنا يثار التساؤل هل يجوز للشخص القائم بالتفتيش القيام بتفتيش جميع الملفات المخزونة داخل جهاز الحاسوب, الغاية منها ايجاد الملفات المطلوبة والمخزونة الذي فيها البيانات والمعلومات التي يجري البحث عنه, وهذا ما يسمى بالتفتيش العام عن الملفات, والعودة الى القواعد العامة للتفتيش, فأن من شروط التفتيش تحديد محل التفتيش نافياً للضلالة, وذلك لان التفتيش من الإجراءات الماسة بالحرية الشخصية للأفراد وحرمة المساكن, وبالتالي يرى البعض من الفقه أن هذه القاعدة لا ينطبق على الحاسوب وأذا كان مكان المعلومات غير معروفة.

ويذهب هؤلاء الى أنه من حق المكلف أو القائم بالتفتيش هو البحث عن البيانات والمعلومات في جميع الملفات المخزونة داخل جهاز الحاسوب, ويقيسون عملية البحث على الملفات المطلوبة داخل جهاز الحاسوب على التجوال في داخل غرفة المنزل للعثور على الدليل الذي يجري البحث عنه (100)

وبالتالي نؤيد ما ذهب اليه الفقه على الرغم من أن اعطاء الحق في التفتيش العام يؤدي الى إنتهاك حق الخصوصية المتهم أو الحائز جهاز الحاسوب, والبحث عن الصور داعرة مثلا مخزونة داخل جهاز الحاسوب, ويتطلب الاطلاع على جميع الصور الموجودة التي تعود للمتهم, وحائز جهاز الحاسوب اذا لم يعرف مكانها بسبب عدم معرفة موقعها أو أسم الملف المخزون داخل ذاكرة جهاز الحاسوب الآلي, واذا منع من التفتيش ملفات الحاسوب للسبب المذكور اعلاه, وأن ذلك يعني تعذر إثبات الجريمة الالكترونية, وبالتالي يفلت المجرم أو الجاني من العقاب, لذا نقترح نصاً قانونياً ينص على السماح للشخص المكلف بالتفتيش تفتيش جميع الملفات

---

(99) د.سامي فقي حسين, مصدر سابق, ص229

(100) اسامة احمد المناعسة وجلال محمد الزغبي وصايل فاضل الهواشة, جرائم الحاسوب الآلي ولإنترنيت, الاردن, 2001, ص279

والبيانات جهاز الحاسوب في حالة عدم معرفته أسم الملف, وفي حال اذا كان الشخص القائم بالتفتيش يعرف مكان الملف أو أسم الملف فلا يجوز له بعد ايجاد الملف المطلوب اجراء

التفتيش العام على الملفات والبيانات, ويكون هذا التفتيش باطلا اذا قام به لأنه يعتبر انتهاك لحق الخصوصية.

سادساً- خزن المعلومات في حاسوب خارج موقع التفتيش

من الممكن أن يكشف القائم بالتفتيش أن المعلومات التي يجري البحث عنها للحصول عليها مخزونة في ذاكرة حاسوب آخر خارج مكان وجود الحاسوب الأول محل لتفتيش, ومرتبط به عن طريق الشبكة, وفي هذه الحالة يواجه القائم بالتفتيش عدداً من المشاكل والصعوبات, منها قانونية وفنية, ومن الناحية القانونية يجب أن نميزبين هذين الحالتين:-

الحالة الأولى:- اذا كان الحاسوب المخزونة فيه المعلومات والبيانات يقع في مكان اخر داخل الدولة: في هذه الحالة يثار تساؤل حول كيفية امكانية إمتداد اذن التفتيش للحاسوب الآخر عن طريق الشبكة, إذا تبين أن البيانات المطلوب ضبطها مخزونة في ذلك جهاز الحاسوب.

ويرى الفقه في المانيا إمكانية أمتداد التفتيش في البيانات المخزونة في ذاكرة الحاسوب آخر خارج موقع التفتيش بالاستناد الى نص المادة (103) من قانون الإجرائات الجنائية الألماني [101]

وكذلك يرى جانب آخر من الفقه إن وسيلة من التفتيش آصلاً هي جمع الأدلة الأجرامية اينما وجدت, ولكن يجب مراعاة شرطين أساسيين هما:

الشرط الاول:- يجب أن تكون البيانات المخزونة على الحاسوب الآخر مفيدة من أجل الكشف الحقيقة.

الشرط الثاني:- يجب مراعاة ضوابط شروط التفتيش المقررة للأماكن الذي يوجد فيه جهاز الحاسوب الآخر, كأن يكون المكان يتمتع بالحصانة مثلاً أو عبارة عن دار سكنية [102]. وبالتالي قد تبنى قانون تحقيق الجنايات البلجيكي هذا الاتجاه, إذ نص على جواز تجاوز الإختصاص المحلي للبحث عن أدلة الجريمة, وجاء في نص المادة (88) على أنه (إذا أمر قاضي التحقيق في التفتيش في نظام معلوماتي (إلكتروني), او جزء منه فإن البحث يمكن ان يمتد الى نظام معلوماتي آخر ويوجد في مكان غير مكان البحث الاصلي ويتم هذا الامتداد وفقآ لضابطين هما:

- إذا كان الكشف الحقيقية ضرورياً في شأن محل البحث.

---

(101) د.هلالي عبد اللاه أحمد, تفتيش نظم الحاسوب الآلي وضمانات المتهم المعلوماتي, دار النهضة العربية, مصر, الطبعة الثانية, 2008, ص77

(102) أسامة أحمد المناعسة وآخرون, مصدر سابق, ص281

- أو إذا وجدت مخاطر تتعلق في ضياع جزء من الادلة، نظراً لسهولة عملية محو أو اتلاف البيانات) (103)

أن تفتيش جهاز الحاسوب آخر موجود داخل حدود الدولة, والمخزونة فيها المعلومات التي يجري التفتيش عنه, ويمكن برأينا التفتيش عنها ولكن بشرط الحصول على إذن آخر لتفتيش من قاضي التحقيق, سواء كان قاضي تحقيق منطقة الذي يوجود فيه جهاز الحاسوب الأول أو قاضي تحقيق منطقة الذي يوجود فيه الحاسوب آخر, وذلك استناداً الى القواعد العامة والذي لا يجوز إجراء تفتيش في مكان معين من دون أمر من القاضي, وبالتالي يجب أن يتم تحديد المكان الذي يراد تفتيشه تحديداً نافياً للضلالة, وعندما يتم الحصول على هذا الإذن يجوز إجراء التفتيش, ولكن يجب الحضور في المكان المراد تفتيشه, وليس عبر العالم الافتراضي, أي بالإتصال بين الحاسوبين عبر الشبكة, وبالتالي فإن هذا النوع من التفتيش يخلق عدداً من المشاكل القانونية, ومن هذه المشاكل هو إجراء التفتيش ويتطلب حضور عدد من الأفراد أثناء عملية التفتيش وهم المكلف بالتفتيش والمختار وشاهدان وصاحب الدار والمتهم أذا كان موجوداً, وهذا كله لا يمكن تحقيقة اذا تم عملية اجراء تفتيش للحاسوب الأخر عبر الشبكة المعلوماتية(الإنترنيت) وهذا التفتيش يكون باطلاً, والسبب في ذلك للأنه يتعارض مع قواعد الحضور الشكلية, لذا نقترح على المشرع العراقي نصاً قانونياً يتيح تفتيش جهاز الحاسوب أخر الذي يقع خارج مكان وجود جهاز الحاسوب الأول عبرالشبكة المعلوماتية, اذا ثبت انه مخزونة فيه معلومات الذي تفيد في كشف الحقيقة بشرط أن يكون ذلك الحاسوب يقع من ضمن نطاق حدود الدولة الجاري تفتيش عنها.

الحالة الثانية:- إذا كان الحاسوب المخزونة فيه المعلومات يقع في مكان آخر خارج نطاق حدود الدولة:

يجمع الفقه عدم إمكانية تجاوز نطاق التفتيش لحدود الدولة إذا كانت العلومات مخزونة في جهاز الحاسوب أخر الذي يقع خارج نطاق حدود الدولة, والسبب في ذلك لأن إجراء التفتيش مثل هذا النوع يشكل انتهاكاً لسيادة الدولة التي يقع جهاز الحاسوب على أراضيها ومخالفة لقواعد الاختصاص المكاني, وبذلك يذهب رأي الى عكس ما أجمع عليه الفقه حيث يرى إمكانية تفتيش جهاز الحاسوب حتى اذا كان خارج نطاق حدود الدولة, والسبب في ذلك إذا كان الهدف من هذا التفتيش اظهار الحقيقة, ويستشهد هؤلاء بمشروع قانون أساءة استخدام الحاسوب (الهولندي) حيث يجيز هذا النوع من التفتيش (104)

---

(103) د.سامي جلال فقي حسين, مصدر سابق, ص232

(104) نبيلة هبة هروال, الجوانب الإجرائية لجرائم الإنترنيت في مرحلة جمع الاستدلالات (دراسة مقارنة), الاسكندرية , 2007, ص240

لقد أيد القضاء ما أجمع عليه الفقه, وفي إحدى قضايا (الغش الإلكتروني), رفضت محكمة التحقيق الالمانية تفتيش المعلومات المخزونة في جهاز الحاسوب موجود في سويسرا, وذلك الا عن طريق طلب المساعدة القضائية من قبل السلطات القضائية في سويسرا [105] وبالتالي نؤيد ماذهب اليه الفقه والقضاء حول عدم جواز تفتيش جهاز الحاسوب اذا كان خارج نطاق حدود الدولة والسبب في ذلك لان التفتيش يتعارض مع مبدأ سيادة الدول, والحل الآمثل هو الحصول على المعلومات المخزونة داخل جهاز الحاسوب الموجود خارج نطاق حدود الدولة هو طلب المساعدة القضائية من سلطات القضائية للدولة التي يوجد على جهاز الحاسوب اقليمها.

وكذلك تفتيش جهاز الحاسوب المخزونة فيه البيانات المطلوبة الذي يقع خارج مكان وجود جهاز الحاسوب الاول يعتمد بشكل اساس على مسالتين مهمتين هما:

1. **أن يكون جهاز الحاسوب يعمل:** يجب أن يكون الحاسوب في حالة عمل, أي موصولا بمغذي الطاقة, فإذا كان جهاز الحاسوب مطفئاً يكون من الصعب الدخول اليه والتفتيش عن المعلومات المخزونة فيه.
2. **أو أن يكون جهاز الحاسوب المخزونة فيه المعلومات متصلاً بالشبكة,** إذا كان جهاز الحاسوب مفصولاً عن الشبكة تكون من الصعب الاتصال به والدخول اليه, والسبب في ذلك عدم قدرة القائم بالتفتيش الحصول على المعلومات المطلوبة.

أن هذا المسألتين متلازمتان, يجب أن يعمل جهاز الحاسوب, وأن يكون متصلاً بالشبكة في نفس وقت, واذا فقدنا أي واحد من هذين المسألتين يكون من الصعب الحصول على المعلومات المخزونة في داخل جهاز الحاسوب, وقد تواجه القائم بالتفتيش صعوبات وتحديات آخرى أثناء محاولته الدخول الى جهاز الحاسوب, وقد يكون جهز الحاسوب محمياً بكلمة سر(pass ward) تمنع من الدخول اليه, وبذلك يتطلب من القائم بالتفتيش محاولة فتح كلمة السر ليتمكن من الدخول الى جهاز الحاسوب وتفتيشه.

وإذا تعذر من الدخول الى جهاز الحاسوب الآخر المخزونة الذي فيه البيانات يضع المكلف بالتفتيش أمام خيار وحيد, وهو الإنتقال الى مكان وجود جهاز الحاسوب الآخر بشكل مباشر وفعلي لإجراء التفتيش على هذا جهاز, وهذا قد يكون من الصعب من الناحية الواقعية, وقد يكون هذا جهاز الحاسوب الأول يقع في محافظة أربيل مثلاً, وجهاز الحاسوب المخزونة فيه المعلومات يقع في محافظة بغداد مثلاً, وفي هذه الحالة من الصعب الوصول الى جهاز الحاسوب بسرعة, وبذلك قد يلجأ قاضي التحقيق الى انتداب محكمة تحقيق

---

(105) د.هلالي عبداللاه أحمد, مصدر سابق, ص79

بغداد لإجراء التفتيش بالسرعة, وضبط المعلومات المخزونة في جهاز الحاسوب وأرسالها الى محكمة تحقيق أربيل [106]

5.1.2: صعوبة الحصول على الشاهد في الجريمة المعلوماتية

يعرف الشاهد في الجريمة الإلكترونية:- هو الفني صاحب الخبرة والمتخصص في تقنيات الحاسوب الآلي وشبكة الأتصال(الإنترنيت) الذي تكون لديه معلومات تولج نظم المعالجة الألية للمعطيات اذا كان هدف التحقيق هو التقصي عن أدلة الجريمة داخله.

وتعد الشهادة وسيلة من الوسائل إثبات الجريمة الإلكترونية التي يمكن للمحقق أن يستعين بها عن طريق البحث عن الأدلة وتقديمها الى القضاء وهو وسيلة من وسائل إظهار الحقيقة.

وتتقسم الشهادة في الجريمة الإلكترونية التي هي شأنها في ذلك شأن الشهادة في الجريمة التقليدية (العادية) الى ثلاثة أنواع: -

الشهادة المباشرة والشهادة السماعية (الشهادة غير المباشرة) والشهادة التسامح [107]

- الشهادة المباشرة:- هي المعلومات التي يدلي بها الشخص أمام المحكمة, والتي وصلت الى حواسه عن طريق مباشر ومن دون وساطة شخص أخر, كأن يكون هذا الشاهد قد رأى أو سمع أو شم ...الخ, أن يقوم الشاهد بالإدلاء بما شاهده من قيام مرتكب الجريمة بعملية الأختراق لأي ملفات الإلكترونية أو القيام بأي نوع من أنواع التزوير الإلكتروني.
- الشهادة السماعية أو غير المباشرة:- الشهادة السماعية هي بخلاف الشهادة المباشرة, والشاهد هنا لم يرى الجريمة ترتكب أولم يسمع الجاني يتهدد ولكنه سمع عن طريق شخص آخر, وه يفترض رواية الشاهد عن غيره, وبالتالي فهو لم يعاين الواقعة بنفسه, وأنما سمع غيره يذكر المعلومات بشأن ارتكاب جريمة الإلكترونية.
- الشهادة بالتسامع:- تختلف الشهادة بالتسامع عن السماعية, وهي لا تسند الواقع لشخص معين بذاته شاهد الجريمة بنفسه, ومثال على ذلك أن يقول الشاهد سمعت كذا او الاشخاص قد قالوا كذا م ودون ان يستطيع إسناد الجريمة الإلكترونية (المعلوماتية) لأشخاص معينين.

---

(106) د.سامي جلال فقي حسين, مصدر سابق, ص234 وما بعدها

(107) د.رضا هميسي, أحكام الشاهد في الجريمة المعلوماتية, ورقة بحثية مقدمة لأعمال الملتقى الوطني للجريمة المعلوماتية بين الوقاية والمكافحة, يومي 16-17 نوفمبر 2015, كلية القانون, جامعة بسكرة, الجزائر, ص2

والشهادة في الجريمة الإلكترونية قد لا يتطلب الرؤية والسماع, ولكن يتطلب أن يتمتع الشاهد بالخبرة العالية في المجال الإلكتروني, ولم يتم ذلك الا الأخذ بها من خلال الأستعانة بالخبراء الفنيين المتخصصين في مجال الحاسوب الألي [108]

ولذلك يمكن القول أن الشاهد المعلوماتي (الإلكتروني) ينحصر في عدة طوائف وسنعرض لهذه الفئات فيما يأتي:-

1. مشغلوا الحاسوب الآلي:- هو المسؤول في تشغيل جهاز الحاسوب وكذلك المعدات المتصلة بها, وبالتالي لابد أن تكون لديه المهارة ودراية الواسعة في كيفية تشغيل جهاز الحاسوب الآلي, وكذلك استخدام لوحة المفاتيح في إدخال البيانات, وبأضافة الى ذلك يجب أن تكون لديه معلومة عن اسلوب كتابة البرنامج, والذي يقوم في نقل البيانات من الوثائق الى وسائط التخزين التي يجري معالجتها من خلال الحاسوب, ويجب أيضاً ان تكون لديه الخبرة الكبيرة في الكتابة السريعة عن طريق لوحة المفاتيح الحاسوب الآلي.
2. المبرمجون:- هم الاشخاص المتخصصين في كتابة أوامر البرامجية, وكذتك يمكن تقسيمهم الى فئتين: الأول مخططو برامج التطبيقية والثاني مخططو برامج الانظمة.
3. المحللون:- (والمحلل) هو الشخص الذي يحلل الخطوات ويقوم بجمع البيانات وفق نظام معين ودراستها, وثم تحليل النظام الى وحدات منفصلة, واستنتاج العلاقة الوظيفية بين هذه الوحدات, وذلك من خلال قيام بتتبع البيانات داخل النظام عن طريق ما يسمى بمخطط تدقق البيانات.
4. مهندسوا الصيانة والاتصالات:- وهم المسؤولون عن اعمال الصيانة الخاصة بتقنية الحاسوب وبمكوناته وشبكة, الإتصال المتعلقة به.
5. مديرو النظم:- وهم الاشخاص الذين توكل اليهم اعمال الادارة في النظم الإلكترونية [109]

2.2: الصعوبات المتعلقة بإحالة المتهم على المحكمة المختصة

سنتكلم عن االصعوبات والمشاكل المتعلقة بإحالة المتهم على المحكمة المختصة من حيث اختصاص المكاني والنوعي, وذلك من خلال تقسيم المبحث الى مطلبين, سنتناول في المطلب الاول: الاختصاص المكاني, والمطلب الثاني: الاختصاص النوعي.

---

(108) ثنيان ناصر ال ثنيان, مصدر سابق, ص90 وما بعدها

(109) بشرى عواطة, حجية الدليل الإلكتروني في الإثبات الجنائي, مذكرة لنيل شهادة ماجستير في القانون الأعمال, جامعة 8 ماي 1945, كلية الحقوق والعلوم السياسية, 2018/2017, ص55.

1.2.2: الاختصاص المكاني

عندما كانت الجريمة المعلوماتية ذات طبيعة خاصة, ويتميز بخصوصية متعددة منها انها تعتبرجريمة عابرة الحدود الجغرافية، فهو ليس لها حدود عكس الجرائم العادية الامر الذي يجعله في أغلب الأحيان تخضع لقوالب التي تحكم مسالة (الاختصاص المكاني)، وبالتالي ان الطبيعة الخاصة لمثل هذا النوع من الجرائم المتطورة يتطلب التخطي لتلك المعايير القديمة أو التقليدية، والشيء الذي جعل البعض يرى بان تطبيق القواعد التقليدية على الجرائم الإلكترونية لا يتلاءم مع تحديد محل وقوع الجريمة في العالم الإلكتروني، والسبب يعود الى ن هذه الجرائم لا يؤمن بالحدود الجغرافية، وبالتالي الحدود الجغرافية فقدت كل أثرلها في الفضاء، وبالتالي أصبحنا مام جريمة عابرة الحدود الجغرافية التي تم في فضاء الكتروني المعقد وعبارة عن شبكات اتصالات غير ملموسة ومتاحة لاي شخص في العالم, وهوغير تابعة لاي سلطة الدولة تتجاوز فيه السلوك مرتكب المكان، وله وجود حقيقي ولكنها غير محدد المكان.

ونظرا لما يتميز بها (الجرائم الإلكترونية) من كونه جرائم عابرة الحدود الجغرافية, وإنها من هذا المنطلق وجود بعض الإشكاليات القانونية ومن هذه الإشكاليات هوان يحدد الاختصاص والقانون الواجب تطبيقها من ضمن مجموعة قوانين الدول التي ترتكب الجرائم على اراضيها.

وأن هذه الطبيعة عابرة الحدود التي يتسم به هذا النوع من الجريمة سوف تنعكس على امكانية ضبط والتصدي لها, ومما يجعله صعوبة تحديد الحكومة صاحبة الاختصاص في النظر في هذا الجريمة على أعتبار ان هذا الجريمة لم تعترف في معيار (الاختصاص التقليدي) التي اقرتها القوانين في الدول.

وأن موضوع الاختصاص في الجرائم الالكترونية, وفي غياب إطار التشريعي يحكمها وينظمها وكذلك يتم التعامل معها وفقاً لقواعد (الاختصاص المكاني) وهذا ما يطرح جملة من التحديات، خصوصا ان مكان أرتكاب الجريمة الإلكترونية, ودائما يكون في البيئة الالكترونية غير مرئية يكون مختلفاً عن مكان أرتكاب باقي الجرائم التقليدية الاخرى في العالم المادي الملموس.

وذلك فان تطبيق القواعد التقليدية التي يتم تحديد معيار الاختصاص لا يتلاءم مع طبيعة الجريمة, بحيث من الصعب أن يحدد مكان وقوع النشاط الإجرامي في هذه الجرائم، وبالتالي من التحديات التي يطرحها (الجرائم الالكترونية) هي الحالات التي تتوزع فيه السلوك المادي للجرائم في اكثر من دولة كأن يقع السلوك الاجرامي في دولة بينما يتحقق نتيجته الاجرامية في دولة اخرى، و يكون بالتالي قانون كل دولة يتحقق فيها احد عناصر الركن المادي للجريمة قابل للتطبيقها، وبالتالي سيؤدي إلى تنازع أيجابي في الاختصاص بين اكثر من تشريع

وطني وبين اكثر من دولة لكي تلاحقة نفس النشاط الاجرامي، وكما هو الحالة في ارتكاب فعل تهديد عبر - الرسائل الالكترونية - حيث قد يرتكب النشاط المادي في بلد ويتلقاه الضحية في بلد اخر بعد ان مر في أغلب الأحيان بأكثر من دولة قبل أن يصل إلى دولة التي استقبلها.

وعليه من الممكن القول بأن قواعد الاختصاص القضائي التي نصت عليه في القوانين الاجرائية رسخت لكي تقررالاختصاص التي يتعلق في جرائم التي يتم تحديد المكان, وبالتالي لا يمكن اعمالها في شأن (الجرائم الالكترونية) والتي ترتكب في فضاء وتنعدم فيها الحدود الجغرافية, ويكون من الصعب تحديد مكان ارتكاب الجريمة, ويتطلب ايجاد قواعد اجرائية تحكم مسألة الاختصاص في هذه النوع من الجرائم التي يتناسب مع طبيعته الخاصة.

ولهذا السبب أصبح اللجوء إلى معيار الاختصاص المكاني التقليدي متجاوزا امام الطبيعة عابرة الحدود الجغرافية, والتي يمتاز به الجرائم الالكترونية، وفي ظل ظهور معيار اخرى ترتبط ببعض الفئة التي تم استهدافهم من الجرائم الالكترونية وكما هو بالنسبة لجرائم الصحافة وكذلك في الجرائم التي تتعلق بالأحداث والمرتكبة عبر الفضاء الإلكتروني.

ولقد أوجدت معايير حديثة لإنعقاد الاختصاص يتجاوز المعيار التقليدي ويتم اللجوء اليها من أجل تحديد ضوابط الاختصاص في مختلف الجرائم التقليدية الاخرى, وذلك انطلاقا من مجموعة من الاجتهادات القضائية الفرنسية في هذا المجال، وأيضاً هذه معيار ترتبط في خصوصية بعض الجرائم وكما ذكرناها سابقاً, وكما هو بالنسبة في جريمة الصحافة التي ترتكب في البيئة الإلكترونية، بحيث انه من بين المعايير التي تم ظهورها إلى الوجود والتي ارتبطة أساسا مثل هذا النوع من الجرائم، هو المعيار الذي يعطي الاختصاص الى محل تـ (مركز الموقع) والذي نشرت فيها المعلومات بواسطتها، وكما أظهرت أيضاً معايير أخرى حديثة مرتبطة في الجرائم الماسة للحقوق الملكية الفكرية، وكما هو بالنسبة للجرائم التقليد عبر الإنترنيت, وبالتالي يكون الاختصاص أما للمحكمة المكان الذي أرتكب فيها التقليد وأما لمكان نشرها، او لمعيار أمكانية الوصول الى الموقع, كأساس لاختصاص المحكمة عند حالة الأعتداء على حق من حقوق المؤلف من خلال شبكة الإنترنيت (110)

أن ما يميز الجريمة الإلكترونية عن الجريمة العادية(التقليدية) هو تشعب وتنوع الوسائل المستعملة في ارتكابها, وهذا ما يتطلب المشرع العراقي أن يصدر من التشريعات الإجراءات والموضوعية الإزمة والمواكبة

---

(110) اشكالية إثبات الجرائم الإلكترونية www.ahewar.org . تم زيارة الموقع بتاريخ 2020/10/15

لهذا التطور السريع في المجالات الإلكترونية, ورغم فائدتها وبـ (الذات الإنترنيت) الكبيرة للمجتمع الا أن لها من الآثار السلبية الكثير والكثير, مما يشكل تقاطعاً وخروقات للقوانين والأعراف.

أن الخطورة خلف الجرائم الإلكترونية وأثباتها مما تمتاز به هذه الجرائم حيث أن ارتكابها لم يعد يحتاج الى السلاح ووسائل وكسر الأبواب وصولاً الى الهدف المتمثل بالاستحواذ على الإموال من دون وجه حق, بل ممكن الدخول الى الهدف من خلال الدخول غير المشروع على شبكة المعلومات الخاصة بالمصرف المستهدف.

وأن أهم ما يواجه المحقق في إثبات الجريمة الإلكترونية وأحالتها الى المحكمة المختصة, هو مدى إمكانية النصوص الإجرائية في (ق.أ.م.ج) المرقم 23 لسنة 1971 المعدل من معالجة الإحالة والاختصاص بشطريه (المكاني والنوعي), وفيما يتعلق بالجريمة الإلكترونية, لذا نجد وبكل تواضع أن تعدل النصوص الإجرائية بما يتلائم مع خصوصية الجرائم الإلكترونية, أو العمل جدياً بأضافة نصوص إجرامية جديدة لتحل اشكالات الجريمة الإلكترونية في الإحالة والإختصاص وما اليها, أو اعتماد على النصوص الموجودة في قانون أصول المحاكمات الجزائية الحالي مع ما يتطلب من أجراءات الجريمة الإلكترونية.

وبدورنا نرى ضرورة قيام المشرع العراقي بأستصدار تشريع خاص ومحدد بالجرائم الإلكترونية في الجانبين الموضوعي والإجرائي.

ومن هذا المنطلق نجد ومن الآونة الرجوع الى النصوص القانونية الإجرائية النافذة وبالذات في موضوع الاختصاص (النوعي والمكاني) وامتداد الاختصاص, أي الرجوع الى قواعد العامة التي رسمها المشروع في قانون (أ.م.ج) رقم 23 لسنة 1971 المعدل وملائمتها ما امكن مع إثبات وإحالة الجريمة الإلكترونية والاختصاص في نظرها – أي بأختصار الرجوع الى القواعد العامة الإجرائية النافذة المواد {53, 54, 55, 56}.

وأن المحكمة الجزائية لا تكون مخصصة بالفعل في الدعوى الا اذا توافر لها هذا الاختصاص بالنسبة لنوع الجريمة المستمدة اليه المتهم من جهة, وبالنسبة لشخص المتهم من جهة آخرى, وبالنسبة للمكان من جهة أخيرة.

(فالاختصاص هو السلطة التي يخولها القانون للمحكمة من المحاكم للفصل في قضايا معينة) [111]

---

(111) د.محمود محمود مصطفى, شرح قانون الاجراءات الجنائية, ط1, 1976, ص347

واذا تقدم اختصاص المحكمة بنظر الدعوى من احدى الجوانب الثلاث التي سبق أن ذكرناها فلا يكون لها سلطة الفصل فيها, الا أن هناك حالات يمتد فيها اختصاص المحكمة الجزائية, ويسمح لها بنظر في دعوى, ولا تكون ضمن اختصاصها في الأصل, وذلك لاعتبارات يرأى المشرع أنها تسوغ للخروج على القواعد العامة في الإختصاص [112]

فالأختصاص المكاني يراد به جواز التحقيق في القضية من قبل قاضي التحقيق لوقوع الجريمة في منطقة اختصاصه من الناحية الأدارية.

المادة (53) من قانون (أ.م.ج) تركز في الأختصاص على:-

1. المكان الذي وقعت فيه الجريمة.
2. أو المكان الذي وجد فيه المجنى عليه.
3. أو المكان الذي وجد فيه المال الذي ارتكبت بشأنه الجريمة بعد نقله اليه بواسطة مرتكبها.

كما عالجت الفقرة (ب) من المادة (53) التحقيق في الجرائم المرتكبة خارج العراق.

كما جاء في المادة (141) في أصول المحاكمات الجزائية تطبق احكام المواد (53, 54, 55) في تحديد الاختصاص المكاني في المحاكمة وفي تنازع الاختصاص المكاني بين المحاكم الجزائية أي:-

- مكان ارتكاب الجريمة, أي المحل الذي تم فيه الفعل التنفيذي كله أو جزء منه.
- أو تتحققت فيه اية نتيجة ترتبت على الجريمة.

والأختصاص المكاني يقصد به جواز نظرالمحكمة في الجرائم التي وقعت في المكان الذي حدد فيها اختصاص المحكمة, وكذلك يمكن تحديد الاختصاص المكاني للمحكمة تبعاً للتقسيمات الادارية, والتي تكون المحكمة الجزائية مختصة بالنظر في الجريمة المرفوع عنها الدعوى الجزائية, اذا تم دائرة اختصاصها الجريمة كلها أو جزء منها أو اية نتيجة تترتب عليه او فعل يكون جزءا من جريمة مستمرة أو متتابعة أو من جرائم العادة, وكذلك يحدد الاختصاص بمكان الذي وجد فيه المجني عليه أو الذي وجد فيه المال الذي ارتكب من أجله الجريمة بعد نقله اليه بواسطة مرتكبها أو شخص يعلم بها.

أما ما أخذت به بعض القوانين كـ (القانون المصري) من الاختصاص محكمة محل أقامة المتهم ومحل القبض عليه وعلاوة على اختصاص محاكم ارتكاب الجريمة, وبالتالي فأن المشرع العراقي لم يأخذ به والسبب في

---

(112) د.سعيد حسب الله عبدالله, شرح قانون أصول المحاكمات الجزائية, دار ابن الاثير للطباعة والنشر, الموصل,2005, ص266

ذلك في رأي بعض (شراح القانون العراقي) يرجع ذلك الى تأثر القانون العراقي بـ (الأصول الانكليزية) التي لم تأخذ بهذا النوع من الاختصاص.

فأن الاختصاص من حيث المكان يتحدد في القانون العراقي أولاً بمكان ارتكاب الجريمة وهذا المكان في الجرائم المؤقتة يتحدد في المحل الذي تم فيه الفعل الإجرامي (التنفيذي) كله او جزء منه أو تحققت فيه أية نتيجة ترتبت على الجريمة, فان أطلاق عيار ناري على شخص يقيم في منطقة محكمة غير المحكمة التي اطلق العيار الناري في منطقتها وتوفي الشخص أو أصيب بجروح فأن كلتا المحكمتين في المنطقتين المذكورتين أعلاه تختصان بنظر في الدعوى المرفوعة عن الجريمة [113]

1.2.2: الاختصاص النوعي

أما الأختصاص النوعي فيراد به أن تكون المحكمة مختصة بمحاكمة المتهم والجريمة المرفوعة عنها الدعوى تقع ضمن اختصاصها.

لا يكفي لانعقاد الاختصاص للمحكمة الجزائية أن تكون مختصة بمحاكمة المتهم, بل أن يقع ضمن أختصاصها الجريمة المرفوع عنها الدعوى, وهو ما يسمى بـ (الاختصاص النوعي), وبالتالي يتم تحديد هذا الاختصاص بنوع الجريمة المرتكبة, وقد قسم قانون العقوبات الجرائم حسب جسامتها الى (مخالفات وجنح وجنايات), أما المحاكم المختصة بالنظر الدعاوى المرفوعة عن هذه الجرائم فقد حددتها المادة (138) من قانون الأصول المحاكمات الجزائية فـ(محاكم الجنح تختص بالفصل في دعاوى الجنح والمخالفات), ويجوز لها أن تخصص محاكم للفصل في دعاوى الجنح وحدها أو في المخالفات وحدها, في حين تختص محاكم الجنايات بالفصل في دعاوى الجنايات ودعاوى الجرائم الأخرى التي ينص عليها القانون.

بينما تختص محكمة التمييز بالنظر في الاحكام والقرارات الصادرة في الجنايات والجنح والقضايا الاخرى التي ينص عليها القانون.

وكذلك بالنسبة لمحاكم الأحداث التي تختص بالفصل في الدعاوى الناشئة عن الجرائم التي يرتكبها الاحداث, وأن تعيين نوع الجريمة المرتكبة المرفوعة عنها الدعوى هو من اختصاص المحكمة المرفوعة لها الدعوى وهي غير مقيدة بالوصف القانوني الذي احليت به هذه الدعوى اليها, واذا ما وجدت محكمة الجنح أن الفصل في الدعوى المحالة اليها يخرج عن اختصاصها ويدخل في اختصاص محكمة الجنايات فأن عليها أن تقرر

---

(113) د.سعيد حسب الله, مصدر سابق, ص269 وما بعدها

احالة المتهم عليها, وهكذأ بالنسبة اذا وجدت محكمة الجنايات أن الفصل في الدعاوى المحالة عليها من قاضي التحقيق داخل في اختصاص محكمة الجنح فأن لها أن تفصل فيها أو أن تحيل المتهم على محكمة الجنح على أن الفصل في اختصاص المحكمة في الدعوى المرفوع اليها قبل البدء في موضوع الدعوى, وبالتالي فان تبين لها أن الدعوى تخرج عن اختصاصها فأن عليها احالتها الى المحكمة المختصة الا في حالة اذا تبين للمحكمة اقتران ارتكاب الجريمة بظرف من شانه أن يغير من وصف الجريمة, وأن البت في موضوع الاختصاص يتوقف على البت أولا في نظر موضوع الدعوى وفي هذه الحالة يشترط أن يتم النظر في موضوع الاختصاص قبل قيام المحكمة بمباشرة قرار التجريم والحكم [114]

وختاماً ما يمكن القول أن احكام الاختصاص الشخصي والنوعي والمكاني الواردة في قانون أصول المحاكمات الجزائية تطبق بصفتها قواعد إجرائية عامة في الجرائم الإلكترونية من حيث الأحالة والاختصاص.

(114) د.سعيد حسب الله, مصدر سابق, ص268 وما بعدها

الفصل الثالث

المشكلات القانونية المتعلقة بالدليل الإلكتروني

أن البحث عن الجرائم يكون عن طريقة التحري عنها, وكذلك أيضاً عن طريق جمع الإدلة والمعلومات عن هذه الجرائم ومتى ما وصل أمرها الى علم عضو الضبط القضائي, كأن يكون ذلك عن طريق تلقيه بلاغ عنها أو شكوى بشأنها أونتيجة لمشاهدته بنفسه (115)

وقد نصت المادة (41) من قانون (أ.م.ج.ع) الى واجبات أعضاء الضبط القضائي في التحري والتي يتلخص في كالآتي:

أ- التحري عن الجرائم.

ب- قبول الاخبارات والشكوى التي ترد اليهم.

ت- تقديم العون الى القضاة التحقيق والمحققين وكذلك تزويدهم بالمعلومات.

ث- قبض على مرتكبي الجرائم وتسليمهم الى السلطة المختصة.

ج- تحرير محضر بالإجراءات التي يتخذونها.

لذلك فأن الدليل الجنائي "هو معنى الذي يدرك من مضمون واقعة تؤدي الى ثبوت الإدانة أوثبوت البراءة, ويتم ذلك عن طريق أستخدام الأسلوب العقلي وإعمال المنطقي في وزن وتقدير تلك الواقعة ليكون المعنى التي يستمد منها أكثر دقة في الدلالة على الإدانة أوالبراءة " (116)

---

(115) د. عبدالفتاح حجازي, مبادىء الإجراءات الجنائية في الجرائم الكومبيوتر الإنترنيت, مصدر سابق, ص58

(116) راضية سلام عدنان, مصدر سابق, ص21

ولأن الدليل الجنائي قد يكون دليلاً مادياً ويتكون من أشياء مادية وتدرك بـ (الحواس) دون أضاف اليها أي دليل آخر لإثبات الواقعة التي يثار الخلاف حول تحديد وإدراك معناها, ومن أمثلة على ذلك الأسلحة النارية, وقد يكون الدليل المادي مستنداً موضوعه الكتابة.

وأن إجراءات التحقيـق هدفه هو جمع الادلة الكثيرة, ومن هـذه الأدلة (الإنتقال والمعاينة واستماع الى الشهود والاستعانة بالخبراء والتفتيش والأستجواب), ويلاحظ إن إجراءات جمع الأدلة لم ترد في القانون على سبيل الحصر, وبالتالي يجوز للمحقق أن يباشر أي إجراء آخر يرى أنه مناسب للاثبات طالما أنه لا يترتب على اتخاذه تقييد لحريات الأشخاص أو المساس لحرمة مساكنهم

1.3: القيمة القانونية للأدلة المستخرجة من الكومبيوتر.

أن جريمة الحاسوب الآلي يمكن إثباتها بالأدلة التي اشرنا اليها, وهناك بعض الأدلة المادية التي لها قيمتها الخاصة في إثبات الجريمة الإلكترونية ونسبتها الى متهم معين, وسنقسم هذا المبحث الى أربعة مطالب, سنتكلم في الاول عن الأوراق, ونتناول في المطلب الثاني جهاز الحاسوب الآلي وملحقاته, وفي الثالث تطبيق الاقتناع القاضي على الأدلة, وفي الرابع سنتناول فيه مدى إمكانية إيجاد الوسائل لتقييم الدليل الإلكتروني:-

1.1.3: الأوراق

أن الجريمة التي تقع على المال أوالإنسان تترك خلفها قدراً كبيراً من الأوراق والمستندات الرسمية منها والخاصة، ولكن في الجريمة الإلكترونية, فإن الحاسوب الآلي وشبكة الإنترنيت تحفظ كماً هائلاً من المعلومات والأوراق والملفات، ومع ذلك نجد أن الجاني قد يقوم في طباعة المعلومات لغرض المراجعة أو من أجل أن يتأكد من تنسيق المستند أو شكله العام، عندما يكون المستند موضوع الجريمة، وكذلك أجهزة الحاسوب والطابعات المتطورة ذات السرعة الهائلة تخلف في وقت قصير كثيراً من الأوراق، وهي من الأدلة التي يجب الأهتمام والإعتناء بها في البحث وتفتيش مسرح الجريمة عن أدلة يتعلق بالجريمة, ويمكن تقسيم هذه الأوراق ألى أربعة أنواع:-

1. أوراق تحضيرية يتم إعدادها بخط اليد كصورة تصوير العمليات التي يتم برمجتها.
2. أو أوراق متالفة تم طباعتها من أجل التأكد من إكمال الجريمة، وبعد ذلك يرمى في سلة الاوساخ.
3. أو أوراق أصلية تتم طباعتها ويتم الإحتفاظ بها، كمصدر أو لغرض الجريمة.

4. أو أوراق أساسية وقانونية محفوظة في الملفات العادية أو في دفاتر الحسابات، وتكون لها صلة بالجريمة الإلكترونية، خاصة عند تلقيد أو تزويرهذه الأوراق بواسطة الحاسوب الآلي نفسه [117]

2.1.3: جهاز الحاسوب الآلي وملحقاته

يمكن القول بأن الجريمة الإلكترونية، يعني وجود جهاز حاسوب الآلي له صلة بالمكان الذي وقوع فيه الجريمة أو الشخص الحائز على الجهاز الحاسوب, لذا يمكن لخبراء الحاسوب الآلي تمييز نوع الحاسوب وسرعته وكذلك تحديد أسلوب التعامل معه في حالة الضبط والتحريز، وذلك لأن الأجهزة الحاسوب الآلي مختلفة من حيث السرعة في معالجة البيانات والدقة العالية في الحصول على النتائج، وكذلك القدرة على خزن البيانات واسترجاعها عند الطلب، وكذلك له القدرة على حل المسائل والعمليات المعقدة، وأنه كلما كانت هذه الأجهزة أكثر قدرة من حيث التقنية، فإن دورها في مساعدة المجرم الإلكتروني يتعاظم في شأن إعانته على تنفيذ مشروعه الأجرامي الإلكتروني.

وجهاز الحاسوب الآلي يتكون من المكونات المادية التي تعتبر وسيلة لإدخال الأوامر، وله القدرة على أستقبال النتائج من هذا الحاسوب، وهذه المكونات هي:-

أولاً: وحدات الإدخال (In put Units):-

وهي الوسيلة التي يتم من خلالها إدخال البيانات أوالمعلومات الى الحاسوب، وبمعنى أخر أن المجرم الإلكتروني لا يمكن إرتكاب جريمته عن طريق الحاسوب الإ بأستعمال هذه الأدوات والتي يمكنه بمقتضاها تغذية الحاسوب بالبيان أو المعلومة الذي يريد تخزينها أو تزويدها أو يعدل في تلك المعلومات والبيانات المحفوظة لدى الجهاز الحاسوب أو المسجلة في شبكة المعلومات الدولية، وتكون وسائل الإدخال على أنواع:

- وسائل تسمح بالاتصال المباشر بين الإنسان وبين وحدة المعالجة المركزية وتمثل لوحة المفاتيح إحدى هذه الوسائل, حيث يتم إدخال البيانات أو المعلومات من خلال المفاتيح مباشرة الى وحدة المعالجة المركزية.
- وسائل تسمح بأدخال البيانات أوبالمعلومات بصورة غير مباشرة, ويتم بهذه الوسائل تهيئة البيانات أو المعلومات المراد إدخالها على وسائط معينة بمعزل عن الحاسوب أول الأمر, ثم تتم عملية الإدخال عن طريق عملية وحدة إدخال ملائمة الى وحدة المعالجة المركزية [118]

---

(117) د.عبد الفتاح حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر الإنترنيت، مصدر سابق، ص60

(118) نهلاعبدالقادر المومني, مصدر سابق, ص25

وتشمل وحدات الإدخال أيضا:

1. **الفأرة (Mouse):-** جهازمتصل بالحاسوب بواسطة اتصال سلكي أو لاسلكي, ويستخدم من خلالها تحرك السهم الذي يظهر على شاشة الحاسوب ومن ثم يضغط على الأمر المراد تنفيذه ويتولى الجهاز الحاسوب تنفيذ ذلك الأمر.
2. **مشغل الأقراص الممغنطة (Magnetic Disk Drive).**
3. **الماسح الضوئي (Scanner):-** عبارة عن جهاز يربط بالحاسوب, ويتم من خلاله إدخال أو نقل صورة أو مستند أو صورة لخريطة أو صورة لإنسان أو صورة لحيوان أو أي ورقة الى داخل جهاز الحاسوب الآلي بعد تصويرها, وثم بعد ذلك يقوم المجرم الإلكتروني بالتعديل عليها بعد خزنها في جهاز الحاسوب, ثم إعادة طبعها مرة أخرى بالمواصفات التي يحددها المجرم الإلكتروني, ويستخدم هذا الجهاز في بعض أحيان في تزييف النقود الورقية.
4. **مشغل الأسطوانات (CD- Rom):-** وظيفته تشغيل الأسطوانة المدمجة أو قرص الليزر الذي يحتوي بداخلها مجموعة من البيانات والمعلومات التي يريدها المجرم الإلكتروني ويرغب في اختراقها لغرض إجرامي.

ثانياً: وحدات المعالجة المركزية (Central Processing unit):-

دور هذه الوحدات تتلقى الأوامرعن طريق أجزاء الإدخال، وتشتهر بين مستخدمي جهاز الحاسوب بأسمها المختصر (CPU). وكذلك تعتبر هذه الوحدات العقل المفكر والمسيطر على جميع العمليات التي يقوم بها الحاسوب الآلي سواء الحسابية أو المنطقية، لذا يتم من خلالها معالجة البيانات أو المعلومات وتخزينها وأخراجها بالكيفية التي يرغبها مشغل الجهاز، حتى لوكان مجرماً الكترونياً [119]

ثالثاً: وحدات الإخراج (OutPut Units):-

هي الوحدات التي يمكن من خلالها للمجرم الإلكتروني أو لأي شخص أخر إخراج النتائج وأظهارها بأشكال مختلفة منها مرئية ومسموعة، ومطبوعة وهي الوسيلة المستخدمة لإظهار نتائج التشغيل ومعالجة البيانات، ومن أمثلة هذه الوحدات هي (الشاشات (Monitors) – الطابعات (Printers)- مشغل الأقراص(disk

(119) د.عبد الفتاح حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر الإنترنيت, مصدر سابق، ص61 وما بعدها

driver)- الراسمات (Plotters)- وحدات تركيب الأصوات والسماعات (Voice Synthesizers) (120)

رابعاً: وحدات التخزين (Storage divices):-

وهي من أهم أجزاء الحاسوب الآلي، لأنها يحتوي على البيانات والبرامج التي يستخدمها المستخدم في عمله، وكذلك يمكن من خلال أجزائها يمكن لمستخدم الجهاز خزن الملفات التي يقوم بعملها، وهذا الجزء ومهم جداً لكي يرتكب الجريمة الإلكترونية، لأنه عند الدخول الى الملفات المخزونة يمكن أن يحصل على ما يريد من معلومات أوتخزيب هذه المعلومات أوتدميرها أوتزيفها أو تزويرها.

والأجزاء التي تستخدم لتخزين المعلومات هي:-

أ- **الأقراص الصلبة (Hard disk):** يمتاز هذه الأقراص بسعة تخزينها العالي وسرعتها وكفائتها العالية، وتكون مركبة داخل حافظة الجهاز – Case – لكبر حجمها.

ب- **الأقراص المرنة:** تستخدم في تحزين الملفات التي لا تحتاج الى حجم تخزين عالي، لأن حجم التخزين فيها قليل، وأسمها المتعارف عليه هو(Flopy disks) وتحفظ عليها في مكان بعيد وأمن، وكذلك إن بعضهم لخوفه عليها والمعلومات التي يتضمنها يقوم بحفظها في مراكز التوثيق الحكومية أو في خزائن البنوك التجارية الأمنة.

ت- **أقراص الليزر (CD rom): تمتاز أيضاً بسعة التخزين العالية، ولكنها لم تصل الى سعة التخزين** للقرص الصلب أو سرعته، وتبدو أهميتها في الجريمة الإلكترونية في أنه يوجد مع جهاز الحاسوب الآلي الشخصي (P.C) قد تجد كمية كبيرةً من أقراص الليزر، ويدون على غلافه بيانات توضح محتويات كل قرص، وهذه الأقراص لدى الشركات والبنوك قد تجد فيها الالاف من الأقراص، ولكن في التحقيقات الجنائية لن يعتد في الطبع بما دون على غلاف القرص من بيانات بل سيتم إفراغ الأقراص وبمعرفة خبير يقدم الدليل أمام جهات التحقيق أو المحكمة، وفي الجريمة الإلكترونية لا يشترط أن تجد أقراص الليزر مع جهاز حاسوب آلي، ولكنها قد تضبط في مكان أخر، وبالتالي يعتبر ذلك جزءاً من الجريمة الحاسوب الآلي متى ما كانت محتوياتها عنصراً من عناصرالجريمة.

---

(120) د.ميسون خلف الحمداني، مشروعية الأدلة الإلكترونية في الإثبات الجنائي, كلية الحقوق، جامعة النهرين، 2016, ص213

ث- **الذاكرة المضيئة (Flasher Memory F.M):** هي قطعة صماء تشبه تماماً القرص الصلب لجهاز الحاسوب الآلي وسعته التخزينية عالية جداً [121]

خامساً: المودم (Modem):-

هو الغاية التي تمكن الأجهزة الحاسوب الآلي من الإتصال ببعضها البعض عبر شبكة الإنترنيت بإستخدام شبكات الهاتف، فهو يقوم بإرسال الفاكس واستقباله، والاجابة على المكالمات الهاتفية وكذلك تبديل البيانات وتعديلها.

سادساً: كروت أو البطاقات (PCMCLA Cards):-

وهي تستعمل في أجهزة الحاسوب الصغيرة ومن أنواعها الـ (نوت بوك – Note book - وكذلك – اللاب توب - (Laptop) وهي تشبه البطاقات الأئتمانية.

سابعاً: البطاقات الممغنطة:-

وكذلك بطاقات الائتمان القديمة وأيضاً المواد البلاستيكية المستعملة في إعداد تلك البطاقات، تعتبركلها قرائن لإثبات الجرائم الإلكترونية.

كانت الإشارة عاجلة للأثارالتي تخلفها الجريمة الإلكترونية التي من المفروض البحث عنها وضبطها وفحصها حتى يستفاد منها في التحقيق من أجل إثبات دليل الإدانة أو النفي فيها، والتعامل مع هذه الإثار يحتاج الى خبرة فنية عالية [122]

3.1.3: نطاق تطبيق مبدأ الاقتناع القضائي

يقتضي بحث نطاق تطبيق مبدأ الإقتناع القضائي الذي تناول مسألتين ثار الخلاف بشأنهما, الأولى تتعلق بنوع المحكمة التي تتولى أعمال هذا المبدأ, والثانية تتعلق بتطبيقه في مراحل الدعوى الجنائية وهذا سنتناوله في فرعين.

---

(121) د.عبد الفتاح حجازي، الإثبات الجنائي في جرائم الكمبيوتر والإنترنيت، مصدر سابق، ص 102 ومابعدها

(122) د.جاسم خريبط خلف, التفتيش في الجرائم المعلوماتية، بحث منشور في مجلة الخليج العربي، جامعة البصرة, كلية القانون, المجلد (41)، العدد (3-4)، لسنة (2013)، ص258 وما بعدها

1.3.1.3: نوع المحكمة التي تتولى أعمال مبدأ الاقتناع القضائي:

يمتد تطبيق مبدأ الأقتناع القضائي الى كافة أنواع المحاكم الجنائية, سواء كانت(محاكم الجنايات أم الجنح أم المخالفات), وأن كان المشرع المصري [123] والعراقي [124] والبحريني [125] لم يحدد وذلك بصراحة في المواد المقررة لهذا المبدأ, بخلاف المشرع الفرنسي, فقد قام بتعميم تطبيق مبدأ الاقتناع حيث نصت عليه المادة(353) من قانون الإجراءات الجنائية المتعلقة بمحكمة الجنايات, وكما نصت المادة(427) من ذات القانون على تطبيق هذا المبدأ بالنسبة لمحاكم الجنح, أما المادة(536) من نفس القانون فهي مخصصة بالنسبة لمحاكم المخالفات, وهو لم يقم به المشرع البلجيكي مثلا [126]

2.3.1.3: مدى تطبيق مبدأ الاقتناع القضائي في جميع مراحل الدعوى الجزائية:

إذا كان مبدأ الإقتناع القضائي شرع أصلاً لكي يطبق أمام قضاء الحكم, وهذا لا يعني أبداً أن نطاق تطبيقها مقصوراً لهذه المرحلة, بل يمتد أيضاً لكي يشمل مرحلة التحقيق الإبتدائي, وبالتالي أخذ صراحة المشرع العراقي بموجب الفقرة(أ) من المادة (213) من قانون أصول المحاكمات الجزائية التي تنص على أنه:

(تحكم المحكمة في الدعوى بناء على اقتناعها الذي تكون لديها من الأدلة المقدمة في أي دور التحقيق أو المحاكمة ...).

أن هذا المبدأ يطبق أيضاً أمام قضاة التحقيق الإحالة, فهم يقدرون مدى كفاية الأدلة أوعدم كفايتها للأتهام, من دون أن تخضع لقواعد معينة, ولا لرقابة محكمة التمييز النقض, ولكنهم يخضعون في ذلك لضمائرهم واقتناعهم الذاتي.

أما قضاة الحكم فهم يقدرون الأدلة, وذلك من حيث كفايتها أو عدم كفايتها للحكم بالإدانة, وبالتالي يمكن القول بأن وظيفة قاضي التحقيق هو السعي الى ترجيح الظن, بينما وظيفة قاضي الحكم هو السعي الى توكيد اليقين.

وأيضاً يترتب على ذلك نتائج مهمة, وهي أن الشك في مرحلة الاتهام يفسر ضد مصلحة المتهم مما يستوجب إحالة الدعوى الى المحكمة المختصة, بينما يكون في صالحه في مرحلة الحكم.

---

(123) المادة 302 من قانون الإجراءات الجنائية المصري

(124) المادة 213/ أ من قانون أصول المحاكمات الجزائية العراقي

(125) المادة 253 من قانون الإجراءات الجنائية البحريني

(126) عائشة بن قارة مصطفى, مصدر سابق, ص244

وبالرغم من أن "المشرع المصري" لم ينص بصراحة على أن نطاق هذا المبدأ يشمل قضاء التحقيق والإحالة بل الا أن قضاء النقض في مصر, اكد هذا المبدأ وقد جاء في أحكامه: (أن المقصود من كفاية الأدلة في قضاء الإحالة أنها تسمح بتقديم المتهم للمحاكمة مع رجحان الحكم بإدانته, وهو المعنى الذي يتفق وكذلك وظيفة ذلك القضاء كمرحلة من مراحل الدعوى الجنائية) [127]

4.1.3: مدى إمكانية ايجاد الوسائل لتقييم الدليل الإلكتروني

سوف نتناول في هذا المطلب وسائل تقييم الدليل الإلكتروني من حيث سلامته من العبث, ثم وسائل التقييم الدليل من حيث سلامة الإجراءات المتبعة في الحصول عليه من الناحية الفنية, وذلك على النحو الآتي:

أولاً: تقييم الدليل الإلكتروني من حيث سلامته من العبث:

بعدة طرق نذكر منها [128]:

1. علم الحاسوب يلعب دوراً مهما وفعالاً في تقديم المعلومات الفنية التي تساهم في فهم مضمون وشكل الدليل الإلكتروني, وهذه العلوم يستعان بها في كشف مدى التلاعب بمضمون هذا الدليل, وتبدو فكرة التحليل التناظري الإلكتروني من الوسائل المهمة للكشف عن مصداقية الدليل الإلكتروني, ومن خلالها تتم مقارنة الدليل الإلكتروني المقدم للقضاء ومن خلال ذلك يتم التأكد من مدى حصول عبث في النسخة التي تم استخراجها أم لا.
2. إستخدام عمليات حسابية تسمى بالخوارزميات ويلحق الى هذه التقنية حتى في حالة عدم الحصول على النسخة الاصلية للدليل الإلكتروني أو في حالة ان التلاعب قد وقع على النسخة الأصلية, بالإمكان التأكيد من سلامة الدليل الإلكتروني من التبديل أو العبث من خلال العمليات الحسابية.
3. يوجد نوع آخرمن الأدلة الإلكترونية يسمى بالدليل المحايد المخزون في البيئة الأفتراضية, وهو دليل لا علاقة له بموضوع الجريمة, ولكنه يساهم في التأكد من مدى سلامة الدليل الإلكتروني المقصود من حيث عدم حصول تعديل أو تغيير في أنظمة الحاسوب(الكمبيوتر) [129]

وأيضاً من خلال هذه الطرق يمكن التأكيد من سلامة الدليل الإلكتروني ومطابقتها للواقع.

ثانياً: تقييم الدليل الإلكتروني من حيث السلامة الفنية للإجراءات المتبعة في الحصول الدليل الإلكتروني:

---

(127) د.نضال ياسين الحاج حمو, دور الدليل الإلكتروني في الإثبات الجنائي, مجلة جامعة تكريت للعلوم القانونية والسياسية, المجلد1, العدد19, 2005, ص211 وما بعدها

(128) نعيم سعيداني, مصدر سابق, ص217

(129) خالد عياد الجلبي, مصدر سابق, ص249

من المعتاد أن تتبع جملة من الإجراءات الفنية للحصول على الدليل الإلكتروني وقد بينا بأن هذه الإجراءات من الممكن أن يعتريها خطأ قد يشكك في صحة نتائجها, ولذلك يمكن في هذا الشأن إعتماد ما يعرف باختبارات "داو بورت" كوسيلة للتأكد من سلامة الإجراءات المتبعة في الحصول على الدليل الإلكتروني, من حيث إنتاجها للدليل يتوافر فيه المصداقية لقبوله كـ (دليل إثبات) ولذلك فإننا سنعرض بإختصار الخطوات التي تتبع للتأكيد من سلامة هذه الاجراءات من الناحية الفنية:

1. **اخضاع الأداة المستخدمة لعدة تجارب للتأكيد من دقتها في اعطاء النتائج:**

وذلك بإتباع إختبارين اساسيين هما [130]:

أ- **إختبار السلبيات الزائفة:** ومفاد هذا الإختبار ان تخضع الأداة المستخدمة في الحصول على الدليل لإختبار يبين مدى قدرتها على عرض كافة البيانات المتعلقة بالدليل الإلكتروني و إنه لا يتم إغفال بيانات مهمة عنه.

ب- **إختبار الإيجابيات الزائفة:** و مفاد ذلك أن تخضع الأداة المستخدمة في الحصول على الدليل الإلكتروني لإختبار فني يمكن التأكيد على أن هذه الاداة لا تعرض بيانات إضافية أخرى [131]

وذلك يتم من خلال هذين الإختبارين التأكد من أن الأداة المستخدمة عرضت كل البيانات المتعلقة بالدليل الإلكتروني, وفي ذات الوقت لم تضف إليها أي بيان جديد, وبالتالي هذا يعطي للنتائج المقدمة عن طريق جهاز الحاسوب الآلي مصداقية في التدليل على الواقع.

2. **الإعتماد على الأدوات التي أثبتت الدراسات العلمية كفاءتها في تقديم نتائج أفضل:** تبين الدراسات العلمية في مجال تقنية المعلومات على الطرق السليمة التي يجب مراعاتها في الحصول على الدليل

الإلكتروني, وفي المقابل أوضحت الدراسات الأدوات المشكوك في سلامتها وهذا يساهم في تحديد مصداقية المستخرجات المستمدة من تلك الأدوات [132].

ومن خلال ما تقدم يمكن الوقوف على سلامة الدليل الإلكتروني فإذا توافرت في الدليل الإلكتروني الشروط العامة لما يمكن أن يمثل أساساً لتأكيد الثقة فيه, وإنه قد يبدو من غير المعقول أن يعيد القاضي تقييم هذا الدليل وطرحه من جديد على بساط البحث فالدليل الإلكتروني بوصفه دليلاً علمياً, فإن دلالته قاطعة في شأن

---

(130) نعيم سعيداني, مصدر سابق, ص218

(131) خالد عياد الجلبي, مصدر سابق, ص251

(132) نعيم سعيداني, مصدر سابق, ص218

الواقعة المستشهد به عنها، وإذا سلمنا سابقا في إمكانية التشكيك في صحة الدليل الإلكتروني بسبب قابليته للعبث وكذلك نسبة الخطأ في اجراءات الحصول عليه, وتلك هي مسألة فنية لا يمكن للقاضي أن يقضي في شأنها برأي حاسم وان لم تقطع بها أهل الاختصاص ولذلك فإذا توافرت في الدليل الإلكتروني الشروط المذكورة سابقاً بخصوص سلامته من العبث والخطأ فإن هذا الدليل لا يمكن رده إستناداً لسلطة القاضي التقديرية ولاشك أن الخبرة تحتل في هذا الحالة دوراً مهماً في التأكد من صلاحية هذا الدليل كأساس لتكوين عقيدة القاضي في بحث مصداقية هذا الدليل هي من أولويات عمل الخبير وليس القاضي .

وهنا نبين إلى عدم الخلط بين الشك الذي يشوب الدليل الإلكتروني بسبب إمكانية العبث به أو لوجود خطأ في الحصول عليه وكذلك بين القيمة الإقناعية في هذا الدليل فـ (الحالة الاولى) لا يملك القاضي الفصل فيها لأنها مسألة فنية فالقول فيها هو قول أهل الخبرة فإن سلم الدليل الإلكتروني من العبث والخطأ فإنه لا يكون للقاضي سوى القبول لهذا الدليل وأيضاً لا يمكن الشك في قيمتها التدليلية بكونه وبحكم طبيعتها الفنية يمثل إبلاغاً مؤكداً عن الواقع أذا لم يثبت عدم علاقة الدليل بالجريمة المراد إثباتها [133]

2.3: الأسباب القانونية لتعذر الحصول على الدليل الإلكتروني

في الحقيقة فإن الجريمة المرتكبة عبرالإنترنيت هي حرب ما بين المجني عليه وهو الشركة أو المؤسسة التي كانت هدفاً للاعتداء على نظامها الإلكتروني والحاق الضرر بها مالياً وأقتصادياً، وما بين المجرم الإلكتروني أو الجناة، لأن الهيئات والجهات التي تتبنى في نشاطها نظاماً معلوماتياً لكي تسير حركاتها سواء كانت أمنية أو خدمية أو مؤسسات أقتصادية تحاول الحفاظ دائماً على معلوماتها وكذلك بياناتها عن طريق خزن هذه البيانات وكذلك المعلومات بعيداً عن أيادي ماهرين جرائم المرتكبة عبرالإنترنيت، وذلك يظهر واضحاً في مجال التجارة الألكترونية.

وهناك جهات معينة بالتجارة الإلكترونية تحاول المحافظة على عمليات الدفع الألكتروني، فضلاً عن تواصل المعلومات والبيانات فيما بينها وبين الأطراف الأخرى، وحماية عملية التحويلات المالية، هناك طريقتين هما أستخدام أسلوب التشفير والتحقق من شخصية المتعاقدين.

بالنسبة فيما يتعلق بالشفرة فهي متفق عليه بين الطرفين، ويعرف كلاهما بمفتاح هذه الشفرة هي لضمان عدم قراءة الرسالة أوالأطلاع عليها، وذلك إلا لمن هو مرخص له بذلك.

---

(133) طارق محمد الجملي, مصدر سابق, ص70

أما فيما يتعلق بالتحقق من شخصية المتعاقدين يتم ذلك عن طريق أستخدام - شفرة المفتاح العام- حيث يمكن للطرفين المتعاقدين أن يوقعون على المستندات بطريقة رقمية، ويتأكد كل طرف من توقيع الطرف الأخر في أستخدام المفتاح العام للشفرة (134)

من المسائل التي أثيرت كذلك بمناسبة تعذر الحصول على الدليل في الجريمة المرتكبة عبر الإنترنيت بطريقة تقليدية نظراً لخصوصية هذا النوع من الجرائم، ومدى سريان الحماية المعمول بها بمنع الإطلاع غير المرخص به على الأوراق المختومة والمغلقة، لكي تمتد الى نظم المعالجة الآلية في البيانات، والمحمي فنياً ضد الأختراق شرط عدم المساس بمبدأ المشروعية (135)

وسبب في خطر الإطلاع على الاوراق المغلقة والمختومة هو رغبة صاحبها في عدم الإطلاع الغيرعليها، وذلك بدليل أنه اتخذ جميع طرق الحماية الممكنة ضد محاولة الإطلاع غيرالمرخص بها، وبدليل أغلاق هذه الاوراق وتغليفها بأية طريقة، وذات المشكلة يتوافر في المعطيات المعالجة آلياً، حيث لا يمكن بدون الحصول على مفتاح الشفرة أو كلمة المرور أو الكود من الدخول الى نظام هذه البيانات، وهنا يكون صاحب هذه النظام قد رفض مقدماً عملية الإطلاع غير مرخص به، أذا لم يكن الراغب في الإطلاع مرخصاً له عن طريق اعطائه رمز الشفرة أو كلمة المرورالى هذه المعطيات وهذا لا يتوافر في حالة عضو الضبط القضائي المكلف بالتفتيش موضوع الحديث، لأن هذا التوجه يهدف أولاً وأخيراً الى ايجاد حماية قانونية الى نظام المعطيات المعالجة آلياً، والتي لا يصرح بها للغيرالأطلاع عليها (136)

وهنا سنقسم هذا المبحث الى ثلاثة مطالب, سنتاول في الاول عدم ظهور الدليل المادي, وفي الثاني سنتناول عدم رؤية الدليل, وفي الثالث سنتكلم عن فقدان الآثار التقليدية.

1.2.3: عدم ظهور الدليل المادي

من أبرز خصائص الجريمة الإلكترونية هو وقوعها في بيئة أو اطار، لا صلة لها بالاوراق وكذلك بالمستندات, وإنما عن طريق الحاسوب أو شبكة المعلومات (الإنترنيت) يمكن للجاني عن طريق نبضات الإلكترونية لاترى، حيث يمكنه التلاعب في بيانات الحاسوب، وذلك في زمن قصير جداً َ قد يكون جزء من

(134) د.عبد الفتاح حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر الإنترنيت، مصدر سابق, ص89 ومابعدها

(135) د.عبد الفتاح حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر الإنترنيت، مصدر سابق, ص95

(136) د.عبد الفتاح حجازي، الإثبات الجنائي في جرائم الكمبيوتر والإنترنيت، مصدر سابق, ص137

الثانية، وهذه البيانات والمعلومات التي يتم التلاعب بها يمكن إزالتها وكذلك في وقت قصير جداً أيضاً قبل أن تصل يد السلطة اليه.

وأن عملية الضبط لا تتم الا بمعرفة خبير فني أو متخصص، لان رجل السلطة سواء تمثل في سلطات الأمن أو أجهزة التحقيق ليس لهم دراية بالإمورالفنية في الجريمة الألكترونية حتى يمكنه من متابعة المجرم في جرمه والقبض عليه، على عكس الجرائم التقليدية، فرجل الشرطة الذي يقوم بجمع التحريات في واقعة سرقة حتى يصل الى المتهم، ويستصدر أمراً بالقبض عليه، وتتولى سلطات الأمن أو جهات التحقيق واستجوابه واحالته الى محكمة (القضاء الحكم)، وكل هذه وقائع خاضعة لسيطرة أجهزة العدالة, ويكون الدليل فيها مرئي ومقروء، الجريمة الألكترونية التي تتم دون رؤية الدليل الإدانة, حتى في حالة وجود الدليل يمكن للجاني طمس أومحو الدليل، وفي حضور أجهزة العدالة غير مختصة، لذلك فالغالبية الجرائم الإلكترونية تتم أكتشافها عن طريق مصادفة وليس عن طريق الإبلاغ عنها.

في انكلترا لجنة التدقيق أجريت دراسة مسحية في شأن الاحتيال المعلوماتي وإساءة استعمال الحاسوب ضمت (ستة الالاف) المؤسسات التجارية وشركات القطاع الخاص, والتي تعتمدون على الحاسوب في إنجاز أعمالها, وتبين أن معظم حالات الاحتيال التي تمت ضد هذه الشركات والمؤسسات تم اكتشفها بمحضر الصدفة وكبدتها خسائر تقدر بحوالي مليونين جنيه إسترليني [137]

ولأنها لا تخلف في الغالب أي أثر مادي مثل تلك التي تخلفها الجرائم التقليدية، حيث أنها لا تخلف لاسلاحاً ولاسكيناً ولابقعاً دموية ولا ظروفاً فارغة لطلقات نارية أوغير ذلك من الأثار المادية .

وأن أغلب الأثار المتخلفة من هذه الجرائم هي أثار الكترونية، وهذه الأثار هي عبارة عن نبضات الكترونية غير مرئية بالعين المجردة [138]

وهي تصل في شكلها وحجمها ومكان تواجدها الى درجة شبه معدومة، بحيث لا يمكن رؤيتها الا من خلال الأستعانة بأجهزة ووسائل تقنية لكي تظهر للعيان.

---

(137) د.عبد الفتاح حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنيت، دار الكتب القانونية, المجلة الكبرى, مصر, 2005 ,ص24

(138) د.جاسم خربيط خلف، صعوبات الدليل الجنائي في الجرائم المعلوماتية، كلية شط العرب جامعة ذي قار, قسم القانون, مجلة القانون للدراسات والبحوث القانونية, العدد 12, لسنة 2016 ص8 ومابعدها

وأن البيئة الإلكترونية غالباً ما تكون مؤلفة من شبكة منتشرة في كافة انحاء العالم، ومرتبطة بعضها ببعض عن طريق شبكة الإنترنيت بحيث تتيع الفرصة أمام مجرمي الإلكتروني للولوج عن بعد الى البيانات الإلكترونية المخزنة في أية بقعة من بقاع العالم (139)

وعلى العكس فأن سلطات التحقيقية وسلطات الضبط القضائي لا يمكن الولوج الى تلك البيانات كونها تقع اغلبها خارج حدود أختصاص دولته، بحيث تصطدم بسيادة الدول الأخرى (140)

ولصعوبة استخلاص الدليل في مثل هذه الجرائم يرى المختصين في جرائم الحاسوب الآلي، أن هذا الجهاز وما يقع عليه من جرائم الإلكترونية يعد تحدياً هائلاً لرجل الأمن، وذلك لأن رجل الأمن غير متخصص وينحصر معلوماته في جرائم قانون العقوبات بصورته التقليدية من سرقة وقتل وضرب ولن يكون قادراًعلى التعامل مع الجريمة الإلكترونية التي تقع بطريقة تقنية عالية.

إذا كانت المصادفة من الأمور التي يعول عليه في كشف الجريمة الإلكترونية, فأن وجود جهاز الرقابة أو التدقيق داخل جهة الادارة سواءاً كانت هذه أجهزة حكومية أو خاصة او شركة من شركات، فسيؤدي الى كشف وقوع الجريمة، ثم إظهار الدليل المخفي الذي يتسم به مثل هذه الجرائم، وشريطة ان يكون الجهاز الذي يتولى هذه الرقابة ذا اختصاص وخبرة عالية في التعامل مع الجهاز الحاسوب الآلي وبرامجها، وعالماً بأحداثها وطريقة التعامل معها، وأن المجرم في هذه الجريمة لديه الخبرة الفنية والمعرفة الكافية التي تمكنه من تنفيذ جريمته (141)

والامثلة على ذلك كثيرة, ومن هذه الامثلة هي:-

1) لاحظ الموظف المسؤول عن إدخال معطيات العمل الاضافي للموظفين في محل تجاري ويبلغ عددهم (300) موظف, أن جميع ساعات العمل الإضافي للموظفين تدخل ضمن برنامج حفظ الوقت, ودفتر الدفعات وبإسم الموظفين وأرقامهم, وكان الحاسوب معداً لاستخدام رقم الموظف فقط, وذلك للتعرف على إسم الموظف وعنوانه وطباعة شيكات الدفعات, وكما لاحظ أيضا أن إسم المراجعة الخارجية جميعها مبنية على إسم الموظف فقط, ولا يقوم أحد بمراجعة حقوق الأشخاص بأرقامهم, وبذلك انتهز هذه الفرصة وسيطر على الملفات واستخدم أسماء الموظفين الذين يعملون عملاً إضافياً, وأدخل رقمه الخاص دون أن يكتشف أحد رغم

---

(139) د.جاسم خربيط خلف، صعوبات الدليل الجنائي في الجرائم المعلوماتية, مصدر سابق، ص9

(140) د.جاسم خربيط خلف، المصدر نفسه، الصفحة نفسها

(141) د.عبد الفتاح حجازي، مبادئ الإجراءات الجنائي في جرائم الكومبيوترالإنترنيت, مصدر سابق, ص68

ارتفاع دخله بألاف الدولارات حتى جاءت المراجعة من قبل الضرائب لتكتشف إرتفاع دخل هذا الشخص, وعند مواجهته إعترف بالجريمة التي لم تكن معقدة, وكان يمكن إستمرارها لسنوات دون أن يكتشفها أحد.

ويدل هذا -المثال على ما سبق- تقديمه من خفاء الدليل في الجريمة الإلكترونية والتي تلعب المصادفة دوراً كبيراً في اكتشافها.

2) في حالة أخرى قام موظف بالتلاعب في بيانات الحاسبات(الكمبيوتر) في مكتبه, حيث كان يتولى التدقيق والمراجعة لشركة شحن فاكهة وخضراوات, ولقد لاحظ بحكم كونه محاسباً في الأصل, أن التدقيق والمراجعة في الشركة غير دقيقة, فأختلف عدد((15)) شركة وهمية, مما جعل لها في حسابات شركة الشحن مستحقات مالية التي يراجع لها عن خدمات تؤديها لها, وبالتالي يقوم هو بالاستيلاء على هذه المستحقات, وكذلك حرصه على أن لا يتجاوز اختلاسه على هذه المستحقات النسب المعقولة, والتي يمكن أن يثار الشكوك حوله, ويعد ذلك برنامج خاص يتولى وفق معايير محاسبية, وتراعى مختلف الظروف الواقعية دون أن يتم كشف أمره في عملية التدقيق والمراجعة, وبهذه الطريقة تمكنه في أول سنة من أختلاس ما يقارب ربع مليون دولار دون الإخلال بالنتائج حسابات الشركة التي يتعامل معها, على مدى خمس سنوات, ولم يكتشف احد تلاعبه سوى أحد البنوك الذي شك في الحسابات الخاصة في إحدى الشركات الوهمية التي اسسها, وذلك بسبب ضخامة الشيكات التي تسدد عن عمال هذه الشركات الوهمية لهذه المنظمات العمل.

وهذا المثال الثاني- يدل على أن الجريمة الإلكترونية يرتكبها المتخصصين في علوم الحاسبات الإلكتروني, فالجاني كان له مكتباً للحاسبات, كان يتولى المراجعة والتدقيق في إحدى شركات الشحن التي تم الجريمة بإسمها على مدار خمس سنوات, وبذلك نجح في إخفاء دليل جريمته خلال هذه الفترة, ولم يتم الكشف الجريمة الا عن طريق الصدفة عن طريق أحد البنوك التي يتعامل الجاني معها [142]

وبالتالي نجد ان المتخصصين وجانبا من الفقه الجنائي وبسبب أخفاء الدليل في الجريمة الإلكترونية, ويطلق على الجناة اسم القراصنة, وهم نوعين:-

هواة قراصنة هم من الشباب المتطفلين الذين يعملون للتسلية ولا يشكلون خطورة على أنظمة المعلومات [143]

ولكن الخطورة تكون في فئة المخادعين, وهؤلاء يحدثون أضراراً ويؤلفون أندية لكي تتبادل المعلومات في ما بينهم, وبحسب خفاء الدليل في جرائمهم, وتقسم جرائمهم الى جرائم:

---

(142) د.عبدالفتاح حجازي, مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنيت، مصدرسابق، ص70 وما بعدها

(143) د.عبد الفتاح حجازي, الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنيت, مصدر سابق, ص33

1- المخادعين fraudeurs

لهم قدرات فنية عالية بأعتبارهم أخصائيين في الحاسوب الآلي ومن أصحاب الكفاءات ولديهم قدرة فائقة على إخفاء دليل الجريمة الإلكترونية, وتنصب جرائمهم على شبكات لتحويل الاموال والتلاعب في حسابات المالية.

2- الجواسيس espions

وهؤلاء يعملون على جمع المعلومات لمصلحة دولهم أو لمصلحة بعض الأفراد أو المؤسسات المتنافسة بينها, ولا شك أن هؤلاء قادرون على إخفاء جريمتهم نظراً لكونهم مجرمين متخصصين ولديهم قدرة عالية على طمس الأدلة المتعلقة بجرائمهم.

ولعل عدم ظهور وإخفاء الدليل في الجريمة الإلكترونية يجد سنده في ان هذه الجريمة قائمة على معلومات التي يتم سرقتهم عن طريقها أو تزويرها, وبمعنى آخر أن هذه المعلومات هي الغاية لارتكاب الجريمة, والتي تختلف أثاراً مادية في ما بعد, مثل الوصل الى رقم بطاقة ائتمان خاصة بأحد الأفراد ومعرفة رمز البطاقة, والرقم السري لها(pass ward) وبعد ذلك الدخول الى حسابه عن طريق الصراف الآلي وسرقة مال المودع في حسابه في المصرف, وأن هذه الجريمة يعتمد على معلومة, يجد الفقه الجنائي مشكلة في التسليم كونها موضوعاً للسرقة واعتبارها من الأموال الذي من الممكن سرقته, وذلك أن المعلومات ليست من الاشياء المنقولات (144)

2.2.3: عدم رؤية الدليل

أن دليل الإثبات في الجريمة التقليدية (العادية) يكون الدليل فيها مرئياً، مثال على ذلك السلاح الناري أو الإدوات الحادة االتي يستخدمها في القتل والضرب، وكذلك المادة السامة التي استعمله في القتل أو المحرر نفسه الذي تم تزويره، وكل هذه الأمثلة حيث يستطيع رجل الضبط القضائي أو سلطة التحقيق رؤية الدليل المادي وملامسته بإحدى حواسه (145)

بينما في الجريمة الإلكترونية- كما ذكرنا سابقاً- تكون البيانات والمعلومات في الحاسوب الآلي (الإنترنيت)عبارة عن نبضات إلكترونية غير مرئية تنساب عبر الأنظمة المعلوماتية، كما تنساب الكهرباء عبرالأسلاك، وهي غير مرئية، وكذلك تكون في الغالب مرمزة أو مشفرة بحيث لا يمكن للشخص قراءتها, لذلك يمكن للمجرم أن يطمس الدليل وأزالته كلياً من قبل الفاعل أمراً في غاية السهولة (146)

---

(144) راضية سلام عدنان، مصدر سابق، ص25

(145) د.عبدالفتاح حجازي، الإثبات الجنائي في جرائم الكمبيوتر والإنترنيت، مصدرسابق، ص118

(146) نهلا عبدالقادر المومني, مصدر سابق, ص56

قد يكون مصدر هذه الصعوبة هي أن أجهزة الحاسوب الآلي لو طبعت ورقة تحتوي على بيانات مخزونة في جهاز الحاسوب الآلي، فلاً يمكن معرفة من قام بطباعتها وغرض منها، حتى لو وجدت هذه الخاصية فإنه يتعين على الشخص الذي يقوم بالتحليل ان يكون مختصاً وعلى مهارة عالي من التدريب والتقنية في مجال الحاسبات ، وهذا لم يتوافر لدى رجل الأمن العادي والمحقق العادي (147)

وبذلك يرى جانب من الفقه الجنائي أن متطلبات السلطة الجنائية تفرض على الأجهزة الدولة أن تتحمل مسؤوليتها كاملة نحو كشف الجرائم وضبط المجرمين ومحاكمتهم، وذلك يقتضي بتوفير الإمكانيات التقنية اللأزمة في تحقيق الجرائم الإلكترونية.

وبعبارة أخر يتعين أستقطاب وجذب الكفاءات المهنية المختصة في هذا المجال، للأستعانة بها في التحقيق الجرائم، ويتعين ايضاً عدم التذرع بالميزانية المالية كسبب يحول دون قيام الحكومة بواجباتها نحو تحقيقق العدالة الجنائية، حتى يتم ذلك يرى هذا الجانب ضرورة الأستعانة بالنخبة المختصة في الحاسوب الآلي حال تحقيق الجرائم الإلكترونية، وذلك لضبط وكشف الجرائم, وتقديم ادلة الإدانة فيها وشرح هذه الادلة وابعادها امام المحكمة (148)

ويجب أن يتم ذلك في أطار القانون الجنائي وخاصة قواعد الخبرة أمام المحكمة الجنائية والتي ينظمها قانون الإجراءات الجنائية (149)

3.2.3: فقدان الآثار التقليدية للجريمة

تبقى الجريمة التي ترتكب عبر الإنترنيت مجهولة أذالم يتم الابلاغ عنها الى الجهات المعنية بالجمع الأدلة، والمشكلة التي تواجه أجهزة السلطة الجنائية, أن هذه الجرائم لا يصل الى علم السلطات المعنية بالطرق الأعتيادية كبقية جرائم قانون العقوبات، وهي جرائم غير عادية، ولا تخلف أثاراً مادياً مثل تلك التي تخلفها الجريمة التفليدية, مثل جثة المجني عليه في القتل، وأختلاس المال من المجني عليه في السرقة...الخ.

ويرجع ذلك الى صعوبة اكتشاف الجرائم المرتكبة عبر الإنترنيت، وذلك لأن الجهات التي تتعامل مع الحاسوب الآلي في معاملات اليومية مثل الشركات التجارية والمؤسسات لا تراجع حساباتها دائماً، بل وحتى تلك التي تقوم بالمراجعة (اليومية أوالاسبوعية أوالشهرية) قد لا يتم الكتشف عن الجريمة، وتبدو وكأنها خسائر

---

(147) د.عبدالفتاح حجازي, مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنيت، مصدرسابق، ص78

(148) د.محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي, ص367

(149) د.عبدالفتاح حجازي، الدليل الجنائي والتزوير في جرائم جرائم الكمبيوتر والإنترنيت، مصدرسابق, ص37.

عادية على أثرممارسة نشاطه، حتى وأن تم أكتشافها فإن بعض الجهات المجني عليها لا تقوم على الإبلاغ خوفاً من الأثار السلبية الذي ينعكس عليه من جراء هذا البلاغ (150)

والسبب في ذلك يرجع الى فقدان الأثار التقليدية التي ترتكب عبر الإنترنيت ما لاخطه جانب من الفقه، أن هنالك بعض العمليات التي يجري عليها ادخال المعلومات مباشرة في جهاز الحاسوب الآلي دون أن يتوقف ذلك على أنها يوجد وثائق ومستندات يتم النقل منها، وكما لو كان البرنامج مخزوناً على جهاز الحاسوب، وكذلك يتوافرأمام المتعامل عدة خيارات وليس له سوى أن يضغط على الخيار الذي يريدها في هذا الحالة تكتمل حلقة المطلوب تنفيذه, وكما في المعاملات المالية في المصارف أو برامج المخازن في المؤسسات التجارية الكبرى، حيث يتم ترصيد الأشياء المخزونة أو حسابات العملاء أو نقلها من مكان الى أخر, بطريقة آلية حسب الأوامر المعطاة الى جهاز الحاسوب الآلي.

ويمكن في الفروض السابقة إرتكاب بعض أنواع الجرائم مثل الإختلاس أو التزوير، وذلك بإدخال بيانات غير معتمدة في نظام الحاسوب أوتعديل البرامج المخزونة في جهاز الحاسوب (الكمبيوتر)، وتكون النتيجة مخرجات على هوى مستعمل الجهاز الذي أدخل فيها البيانات أوعدل برامج دون أستخدام وثائق ومستندات ورقية، وبالتالي أنها تفقد الجريمة أثارها التقليدية (151)

كذلك هنالك بعض الافعال الغير المشروعة التي يرتكبها الجاني في الوسائل الاتصالات، ويكون أمرها هو اللجوء عليهم كـ (التجسس على المعطيات) وملفات المخزونة، والوقوف على ما فيها من أسرار، وكذلك أنهم قد يطبعون هذه الملفات ويحصلون على نسخة منها, والغاية هو استعمالها في تحقيق مصالحهم الخاصة، وكذلك قد يعملون أيضاً بأختراق قواعد البيانات والتغير في مضمونها من أجل تحقيق مأرب خاصة، وقد يدمرون النظم بحيث يمكن تمويها, و كما لو كان مصدره خطأً في البرامج أو في نظام التشغيل، وقد يدخلون في بيانات غير معتمدة في أنظمة الحاسوب ويعدلون برامجه أو يحرفون المعلومات المخزونة في داخله دون أن يترك وراء ذلك ما يشير الى حدوث هذا الإدخال مما يزداد خطورة وإمكانية وسهولة إخفاء الادلة التي تم الحصول عليها من الوسائل الإتصال، ويمكن أزلة الدليل في أقل من ثانية, فالمجرم نفسه يمكن أن يزيل الادلة التي تكون قائمة ضده أو تدميرها في وقت قصير جداً, وبحيث لا يتمكن السلطات من أن يكشف هذه جرائم

---

(150) د.عبدالفتاح حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوترالإنترنيت, مصدرسابق، ص83

(151) د.عبد الفتاح الحجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنيت، مصدر سابق، ص42 ومابعدها

إذا ماعلمت بها، في حالة اذا علم بها فأنه يستهدف بالتدمير والمحوالسريع عدم أستطاعة هذه السلطات أقامة الدليل ضده (152)

لذلك نجد أن أعضاء الضبط القضائي أحياناً أنهم غير قادرين على التعامل بإجراءات التقليدية مع هذه النوعية من الجرائم، وفضلاً عن صعوبة أجراءات التحريات السرية ومتابعة مسار العملية الإلكترونية العابرة للحدود (153)

(152) د.جاسم خربيط خلف، صعوبات الدليل الجنائي في الجرائم المعلوماتية, مصدر سابق, ص16

(153) د.خالد ممدوح إبراهيم, التقاضي الإلكتروني, دار الفكر الجامعي, الإسكندرية, ط1, 2007, ص324

الخاتمة

فبعد أن انتهينا من هذه الدراسة توصلنا من خلالها الى العديد من الاستنتاجات والتوصيات, يمكن إجمالها كما يلي:-

أولاً- الاستنتاجات:-

1. من خلال الدراسة لاحظنا أن شبكة الإنترنيت كانت أداة لارتكاب الجرائم, إما أن تكون أداة إيجابية أو أداة سلبية (للمجرم الإلكتروني) أي أن تكون وسيلة لارتكاب الجريمة, وهي في الحالة الأولى تسهل للمجرم الإلكتروني أرتكاب جرائم أخرى يعاقب عليها, وهي تشكل أغلب جرائم الأعتداء على الأفراد كجرائم الأعتداء على حق الأنسان في حرمة حياته الخاصة, وجريمة الأعتداء على شرفه وسمعته, وتتحقق في الحالة الثانية كأداة سلبية فيها لو كانت هي هدف الجاني وغايته في الحصول على البيانات والمعلومات المنقولة عن طريقها, والأستفادة منها بصورة غير شرعية أو الأعتداء على هذه البيانات والمعلومات بإتلافها أو تزويرها.
2. أختلف الفقه حول تسمية الجرائم المعلوماتية فالبعض يسميها بالجرائم الإلكترونية والبعض الآخر يسميها بالجرائم الحاسوب الآلي.
3. أن الأفعال الإجرامية التي تجسد السلوك الإجرامي للمجرم الإلكتروني تتطور وأخذت أساليب جديدة وحديثة في تطور نمط السلوك الإجرامي, والذي يعتمد بدوره على التطور التكنولوجي.
4. ان هنالك صعوبات تحيط بالدليل الجنائي بـ (النسبة للجريمة المعلوماتية), سواءاً من حيث طريقة الحصول عليها او من حيث طبيعتها, وبالتالي الحصول عليها قد تحتاج الى عملية فنية - علمية وكما ان طبيعتها قد تكون غير مرئي, كـ (الذبذبات - النبضات), وبالتالي ومن السهل أستخدام التقنية العلمية في أخفائه او اتلافه, وهذا تتم عن طريقة تشفير وكلمة (pass word) وأستخدام الفايروسات المدمرة.
5. للجريمة الإلكترونية خصائص فريدة من نوعها كصعوبة أكتشافها, وأنها تعد من الجرائم الناعمة, ويكون المجرم فيها شخص ذو خبرة عالية في مجال المعلومات الإلكترونية.
6. أن البرامج والفايروسات المستخدمة في مجال الجريمة الإلكترونية من قبل المجرم الإلكتروني أشد فتكاً وخطورة في بعض أحيان من الأسلحة التقليدية التي يستخدمها المجرم العادي, من حيث الأضرار التي يسببها للأنظمة الإلكترونية, وذلك ما يمكن أن يشهده العالم من خسائر مالية فادحة جراء أنتشار من هذا النوع من البرامج بفعل النشاط الإجرامي الإلكتروني منفرد ومقارنة عما قد يتسببه جريمة التقليدية(العادية) مادية واحدة.

7. أن ما يتميز به الدليل الإلكتروني هو صعوبة أزالتها او تحطيمها, وبالتالي يمكن كشف محاولة المجرم لأزالة لهذا الدليل ليكون دليلاً ضد الجاني.

8. ويمكن أيضاً أن نقسم الدليل الإلكتروني الى نوعين, الأولى هي أدلة أعدت لتكون وسيلة الإثبات والثانية أدلة لم تعد لتكون وسيلة أثبات, ويميز النوعَ الاول بسهولة الحصول عليها, وكذلك ضمان عدم فقدانها, بينما تتميز الثاني بأحتوائه على قدر اكبر من معلومات حول الجريمة.

9. أن مرتكب الجريمة الإلكترونية يتميز عن المجرم التقليدي(العادي) بمجموعة الصفات منها أنه أجتماعي وذكي ويتمتع ايضاً بالخبرة التقنية الحديثة بأضافة أنه غير عنيف, وبالتالي فهذا النوع من الجرائم لا يتطلب القوة والعنف.

10. أن الجريمة الإلكترونية هي الأفعال المخالفة للقانون التي ترتكب بواسطة جهاز الحاسوب (الكمبيوتر) من خلال شبكة الإنترنيت.

11. تختلف دوافع أرتكاب الجريمة الإلكترونية من شخص الى آخر, منها قد تكون دوافع شخصية هدفها تحقيق مصلحة خاصة, وقد تكون أيضاً خارجية هدفها الأنتقام منها مثلاً.

12. أن الجريمة الإلكترونية كغيرها من الجرائم التقليدية (العادية) تتميز بالخطورتها ولكونها تمس الأشخاص والمؤسسات وتتعدى حتى تكون خطر على أمن الدولة وأستقرارها, وبالتالي فهي من الجرائم العابرة الحدود(القارات)لارتباطها بشبكة الإنترنيت, وكذلك تتميز الجريمة الإلكترونية بكونها تعتمد على التقنيات الحديثة وصعوبة أكتشافها وإثباتها.

13. ان من أهم الوسائل المستخدمه في الجرائم الإلكترونية إستخدام (البريد الإلكتروني) والسبب في ذلك هو تواصل بين (الجماعات الإجرامية), وكذلك تبادل المعلومات فيما بينها بشأن العمليات الإجرامية, وقد أكتشفت جهات التحقيق في وقت قريب أن الكثير من العمليات الإجرامية التي تحدث في الاونة الاخيرة كان سببها البريد الإلكتروني, والسبب هو يعتبر وسيلة تبادل المعلومات وتناقل بين القائمين بـ (العمليات) والذين يخططون له.

14. إن إختراق البريد الالكتروني يعد خرق في خصوصية الأشخاص ويعتبرهتك لحرمة بياناتهم ومعلوماتهم, فهو إنتهاك لخصوصية الأشخاص.

15. أن جهاز الحاسوب الآلي(الإنترنيت) له أهمية كبرى على صعيد الأعمال المؤسساتية في كافة القطاعات (الاقتصادية , الصحية , المصرفية , الحكومية), لأن العديد من الأعمال التابعة لهذه القطاعات لا يمكن إجرائها بدون برامج, وخاصة برنامج (اكسل) وقيمة البرامج وأهمية من الناحية العلمية باتت كأي شيء آخر لايمكن الإستغناء عنه.

ثانياً - التوصيات:-

في ضوء الاستنتاجات السابقة التي أظهرتها الدراسة خلصت الى بعض التوصيات وتتمثل في:

1. خلق ثقافة أجتماعية جديدة تصور جرائم الإنترنيت على أنها أعمال غير شرعية مثلها مثل أنماط الجرائم الأخرى, والتأكيد على أن المجرم الإلكتروني يستهدف الى الأضرار بالأخرين, ويستحق العقوبة على فعله بدل نظرات وعبارات الاعجاب.
2. أن من الضروري تدريب وتأهيل أفراد الضبطية القضائية من العـامليـنَ في الادعـاءِ العامَ والقضاة على كيفيـةَ التعـامَـلِ مثل هـذا النـوَع مـنَ الجرائم وتحقيق التعـاونَ مع أصحاب الخبرة, وذلك من خلال عقد دورات تدريبية بشكل دوري ودائم للأستفادة من خبراتهم وإرشاداتهم, إبتداء من مرحلة البحث والتحري وأنتهاء بقرارات المحاكم.
3. تدرس مَـواد الانظمة الإلكترونية والجرائـم التي قـد تنشا مَنهـا فـي كلية القانون والمعهد القضائي.
4. من ضروري أن يفعل دور الاسرة في متـابعـة ابنائهم لوقايته من الاثـار السلبية وكذلك المخـاطـر التي تترتب على الأستخدام غير الصحيح لشبكة الإنترنيت.
5. دعوة المشرع العراقي بضرورة الإسراع في سن التشريعات التي تجرم إساءة أستخدام أجهزة الاتصالات الحديثة ومكافحة الجرائم الإلكترونية.
6. ضرورة الحضور خبـراء الانظمة المعلـومـاتيـة على أختلاف تخصصـاتهـا امام المحـاكـم لمناقشتها ومناقشة تقاريرها التي خـلصـوا اليها لإظهار الحقيقة.
7. كذلك العمـل على أستحداث ضبطيـة قضائيـة, كذلك أدعاء العام متخصص في مجال الجرائم الإلكترونية اسـوة بـ (الدول) التي سبقتنا في هذا المجال.
8. من الضروري أعادة النظَـر فـي مَقررات كلية الحقوق والمعاهد وكلية الشرطة, وحيث تفرد مقـررٍ مَستقـل الجرائم الإلكترونية.
9. من الضروري تجريم وتشديد العقوبات على الجرائم التي ترتكب بواسطة الشبكة الإلكترونية ومنها جرائم الأعتداء على الأعراض, وجرائم الأرهاب, وأضافة الى الألفاظ التي تدل على ارتكابها بواسطة النظم الإلكترونية وشبكة الإنترنيت وكذلك الأفعال الذي يتم ارتكابها عن طريق الإنترنيت مثل أنشاء المواقع الإلكترونية الغاية منها ارتكاب تلك الجرائم أو الترويج لها.

10. من الضروري أنشاء هيئة وطنية لتتولى مراقبة مواقع الإلكترونية عبر مواقع الإنترنيت, وذلك من خلال حجب مواقع المشبوهه التي يهدد امن وأستقرار المجتمع وخاصتاً الجرائم غير الأخلاقية التي يتعارض مع القيم ومبادى المجتمع العراقي.

11. السعي الى وضع قانون لمكافحة الجرائم الالكترونية, بحيث يشمل في أحد جوانبه على هذه الجرائم بشقها الموضوعي, إذ يجرم الأعمال غير المشروعة التي تمارس بواسطة النظام الإلكتروني والأفعال التي تتخذ من هذا النظام لها ويعاقب مرتكبيها, والجانب الإجرائي بحيث يوضع إجراءات تفتيش الحاسوب الآلي وضبط المعلومات التي يحويها.

12. الدعوة الى عقد المزيد من المؤتمرات العلمية حول جرائم الإلكترونية, بحيث تتاح من خلالها الفرصة لتلاقي الأفكار والإتجاهات لكل من يعنيهم أمر في مكافحة الإجرام المعلوماتي (الإلكتروني), بما في ذلك رجال الأمن القضاء والقانون والإعلام وخبراء تقنيات الملوماتية.

13. السماح بمراقبة المواقع المشبوهة على شبكة الانترنيت على أن يكون ذلك عن طريق تصريح من القضاء درءا لأي تعسف وبما لا يشكل إنتهاكاً للحريات الفردية وللحق في الخصوصية.

14. تطوير تقنيات المراقبة والتنصت على المجرمين, وذلك عن طريق البريد الإلكتروني وغرف الحوار والدردشة على أن يكون ذلك تحت إشراف فريقين أحداهما من المتخصصين في مجال الحاسبات, والثاني من المحترفين في القانون وثغراته.

قائمة المصادر والمراجع

أولاً:- القران الكريم

(1) سورة الفرقان، الأية,(45).

ثانياً:- معاجم اللغة العربية

(1) ابراهيم مصطفى واخرون, المعجم الوسيط, ط3, مجمع اللغة العربية, القاهرة, ج 1, سنة1998.

(2) إبن منظور, لسان العرب, الجزء الثاني, باب الجيم, دار احياء العربي التراث العربي, لبنان, الطبعة الثالثة, 1419ه - 1999م.

(1) إبن منظور، لسان العرب، الطبعة الثالثة، باب - دال، دار احياء العربي، المجلد الحادي عشر, بيروت، لبنان، 1994.

ثالثاً:- الكتب

(1) د.ابراهيم رمضان ابراهيم عطايا, الجريمة الإلكترونية وسبل مواجهتها في الشريعة الأسلامية والإنظمة الدولية (دراسة تحليلية تطبيقية), 2015.

(2) اسامة احمد المناعسة وجلال محمد الزغبي - صايل فاضل الهواشة, جرائم الحاسوب الالي والإنترنيت, الاردن, 2001.

(1) د.أشرف عبدالقادرقنديل, الإثبات الجنائي في الجريمة الإلكترونية, دارالجامعة العربية, مصر, 2015.

(2) خالد عياد الحلبي، اجراءات التحري والتحقيق في جرائم الحاسب والإنترنيت، ط1، دارالثقافة والنشر والتوزيع، عمان، 2011.

(3) د.خالد ممدوح ابراهيم, التقاضي الإلكتروني, دار الفكر الجامعي, الاسكندرية, ط1, 2007.

(4) د.سامي جلال فقي حسين, التفتيش في الجرائم المعلوماتية (دراسة تحليلية), دار الكتب القانونية, مصر,, 2011م.

(5) د.سعيد حسب الله عبدالله, شرح قانون أصول المحاكمات الجزائية, دار أبن الأثير للطباعة والنشر, الموَصل, 2005.

(6) عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الاثبات الجنائي في القانون الجزائري والقانون المقارن، دار الجامعة الجديدة، القاهرة، 2010.

(7) د.علاء حسين حمامي, د.محمد علاء الحمامي, إخفاء المعلومات – (الكتاب المخفية والعلامة المائية), اثراء للنشر, عمان, الأردن, 2008.

(8) د.عبدالفتاح حجازي، الدليل الجنائي في جرائم الكومبيوتر والإنترنيت, دار الكتب القانونية, المجلة الكبرى, مصر, 2005.

(9) د.عبدالفتاح حجازي، مبادى الاجراءات الجنائية في جرائم الكومبيوتر الإنترنيت، دار الكتب القانونية، مصر، 2007.

(10) د.عبد الفتاح حجازي، الإثبات الجنائي في جرائم الكومبيوتر والإنترنيت, دار الكتب القانونية، مصر, 2007.

(11) د.عمار عباس الحسيني, جرائم الحاسوب والإنترنيت(الجرائم المعلوماتية), الطبعة الاولى, بيروت, لبنان, 2017.

(12) د.فتحي محمد أنورعزت, الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية للمجتمع المعلوماتية، دار الكتب القانونية, ط2، القاهرة ،2010.

(13) د.قصي علي عباس, مدى إمكانية تطبيق نصوص الجنائي على الجرائم المعلوماتية.

(14) د.محمد امين الرومي, جرائم الكومبيوتر والإنترنيت, الإسكندرية, 2004.

(15) محمد امين أحمد الشوابكة, جرائم الحاسب والإنترنيت, الاردن, 2004.

(16) د.محمد حماد مرهج الهيتي, جرائم الحاسب ماهيتها وموضوعها واهم صورها, ط1, دار المناهج للنشر والتوزيع, عمان, 2006.

(17) د.محمد سامي الشوا, ثورة المعلومات وانعكاساتهاعلى قانون العقوبات, دار النهضة العربية, القاهرة, 1994.

(18) محمد عبدالله ابو بكر سلامة, موسوعة جرائم المعلوماتية جرائم الكومبيوتر والإنترنيت, منشاة المعارف, الاسكندرية, 2006.

(19) د.محمد عبيد الكعبي, الجرائم الناشئة عن الإستخدام غيَر المَشروع لشبكة الإنترنيت, (دراسة مقارنة), دار النهضة العربية, مصر, 2009.

(20) د.محمد علي العريان, الجرائم المعلوماتية, دار الجامعة الجديدة للنشر والتوزيع, الاسكندرية, مصر, 2004.

(21) د.محمد علي العريان, الجرائم المعلوماتية, دار الجامعة الجديدة للنشر والتوزيع, القاهرة, 2011.

(22) د.محمود محمود مصطفى, شرح قانون الإجراءات الجنائية, الطبعة الأولى, 1976.

(23) د.منصورعمرالمعايطة, الإدلة الجنائية والتحقيق الجنائي، ط1, دار الثقافة للنشروالتوزيع, الأردن, 2007.

(24) منير محمد الجنبيهي وممدوح محمد الجنبيهي, امن المعلومات الإلكترونية, دار الفكر الجامعي, الإسكندرية, 2006.

(25) منير محمد الجنبيهي وممدوح محمد الجنبيهي, جرائم الإنترنيت والحاسوب الآلي وسائل مكافحتها, دار الفكر الجامعي, الاسكندرية, الطبعة الأولى, 2006.

(26) د.ميسون خلف حمد الحمداني، مشروعية الأدلة الإلكترونية في الإثبات الجنائي, كلية الحقوق، جامعة النهرين, 2016.

(27) نبيلة هبة هروال, الجوانب الإجرائية لجرائم الإنترنيت في مرحلة جمع الأستدلالات (دراسة مقارنة), الاسكندرية , 2007.

(28) نهلا عبدالقادر المومني, الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع, الاردن, 2008.

(29) د.هلالي عبد اللاه احمد, تفتيش نظم الحاسوب الآلي وضمانات المتهم المعلوماتي, مصر, الطبعة الثانية, 2008.

رابعاً:- الرسائل والاطاريح

(1) الهام بو الطمين, الإثبات الجنائي في مجال الجرائم الإلكترونية, رسالة ماجستير, مقدمة الى جامعة العربي بن مهيدي, كلية الحقوق والعلوم السياسية, قسم الحقوق, سنة 2017 / 2018م.

(2) بشرى عواطة, حجية الدليل الإلكتروني في الإثبات الجنائي, مذكرة نيل شهادة ماجستير في القانون الأعمال, جامعة 8 ماي 1945, كلية الحقوق والعلوم السياسية, 2018/2017.

(3) تغريد سامي إبراهيم الطائي, جرائم الإرهاب الإلكتروني, رسالة الماجستير مقدمة مجلس فاكلتي العلوم الإنسانية, سكول القانون السياسة, قسم القانون, جامعة دهوك, 2010.

(4) ثنيان ناصر ال ثنيان، اثبات الجريمة الإلكترونية - دراسة تاصيلية تطبيقية -,(رسالة الماجستير) جامعة نايف العربية للعلوم الامنية, كلية الدراسات العليا, السعودية, 2012م.

(5) راضية سلام عدنان، مشروعية الدليل الإلكتروني، بحث مقدم الى مجلس كلية الحقوق وهو جزء من متطلبات نيل البكالوريوس في الحقوق، جامعة النهرين،2015.

(6) دلخاز صلاح فرحان, الحماية الجنائية الموضوعية للمعلوماتية في القانون العراقي, دراسة مقارنة, نيل شهادة ماجستير في الحقوق, جامعة الاسكندرية, كلية الحقوق, قسم القانون الجنائي،2015.

(7) سلامة محمد المنصوري, تطبيق مبدأ الاقتناع القضائي على الدليل الإلكتروني, أطروحة مقدمة لإستكمال متطلبات الحصول على درجة ماجستير في القانون العام, جامعة الامارات العربية المتحدة, كلية القانون, نوفمبر, 2018.

(8) شهرزاد حداد, الدليل الإلكتروني في مجال الإثبات الجنائي, مذكرة لنيل شهادة الماجستيرفي الحقوق, تخصص قانون جنائي للأعمال, كلية الحقوق والعلوم السياسية, قسم الحقوق, جامعة العربي بن مهيدي, ام البواقي,2017/2016.

(9) صغير يوسف, الجريمة المرتكبة عبر الإنترنيت, مذكرة لنيل شهادة ماجستير, جامعة مولود معمري, كلية الحقوق والعلوم السياسية, الجزائر, 2013.

(10) عبدالله دغش العجمي, المشكلات العلمية والقانونية للجرائم الإلكترونية, رسالة الماجستير مقدمة الى جامعة الشرق الاوسط, 2014م.

(11) عزيزة رابحي, الأسرار المعلوماتية وحمايتها الجزائية, اطروحة نيل شهادة دكتوراه في القانون الخاص, كليةِ الحقوق والعلوم السياسية, قسم القانون الخاص, جامعة ابو بكر بلقايد- تلمسان, 2017- 2018.

(12) نعيم سعيداني، اليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري،(رسالة الماجستير), جامعة الحاج لخضر- باتنة-، كلية الحقوق والعلوم السياسية، الجزائر، 2013.

(13) هدى طالب علي, الإثبات الجنائي في جرائم الإنترنيت والاختصاص القضائي بها, رسالة الماجستير مقدمة الى كلية الحقوق, جامعة النهرين, 2012م.

خامساً:- البحوث والدوريات

(1) أ سميرة معاشي, الجريمة المعلوماتية (دراسة تحليلية لمفهوم الجريمة المعلوماتية), مجلة المفكر, العدد 17, جامعة محمد خيضر, كلية الحقوق والعلوم السياسية, بسكرة, 2018.

(2) د.جاسم خربيط خلف, التفتيش في الجرائم المعلوماتية، بحث منشور في مجلة الخليج العربي، جامعة البصرة, كلية القانون, المجلد (41)، العدد (3-4)، لسنة (2013).

(3) د.جاسم خربيط خلف، صعوبات الدليل الجنائي في الجرائم المعلوماتية، كلية شط العرب جامعة ذي قار, قسم القانون, مجلة القانون للدراسات والبحوث القانونية, العدد 12, لسنة 2016.

(4) د.رضا هميسي, أحكام الشاهد في الجريمة المعلوماتية, ورقة بحثية مقدمة لأعمال الملتقى الوطني للجريمة المعلوماتية بين الوقاية والمكافحة, يومي 16-17 نوفمبر 2015, كلية القانون, جامعة بسكرة, الجزائر.

(5) طارق محمد الجملي, الدليل الرقمي في مجال الإثبات الجَنائي, محاضر في كليةِ الحقوق, جامعة بنغازي ليبيا, مجلة الحقوق, المجلد(12), العدد(1), 2015.

(6) د.عبادة أحمد , بحث بعنوان (التدمير المتعمد لأنظمة المعلومات الإلكترونية), مركز البحوث والدراسات لدى شُرطة دبي, دولة الإمارات العربية المتحدة, العدد 87, مارس, 1999م.

(7) د.عمارة فتيحة, الجريمة المعوماتية, مجلة أبحاث قانونية, السنة رابعة, العدد السابع, يونيو 2019م.

(8) د.محمد الأمين البشري, الأدلة الجنائية الرقمية(مفهومها ودورها في الإثبات), المجلة العربية للدراسات الامنية والتدريب, الرياض, المجلد17, العدد 33, 2004م.

(9) د.محمد الامين البشري، التحقيق في جرائم الحاسوب الآلي, بحث مقدم الى مؤتمر القانون والكومبيوتر والإنترنيت, المنعقد في الفترة من 1- 3/5/ 2000, كلية الشريعة والقانون, دولة الامارات العربية المتحدة.

(10) محمد علي سالم وحسون عبيد هجيج, الجريمة المعلوماتية, مجلة جامعة بابل, العلوم الانسانية, المجلد 14, العدد 2, 2007.

(11) نادر عبدالكريم العزاوي, الحماية الجنائية من الجرائم الإنترنيت (دراسة مقارنة).

(12) الجريمة الإلكترونية وحجية الدليل الرقمي في الأثبات الجنائي، مركزهردو لدعم التعبيرالرقمي.

(13) د.نضالِ ياسين الحاج حمو, دور الدليل الإلكتروني في الإثبات الجنائي (دراسة تحليلية), مجلة جامعة تكريت للعلوم القانونية والسياسية, المجلد1, العدد19, 2005.

سادساً:- القوانين

(1) قانون العقوبات العراقي رقم 111 لسنة 1969.

(2) قانون اصول المحاكمات الجزائية العراقي رقم 23 لسنة 1971.

(3) مشروع قانون الجرائم المعلوماتية العراقي.

(4) قانون العقوبات الاتحادي الاماراتي رقم 3 لسنة 1987.

(5) قانون الإجراءات الجزائية الاتحادية الإماراتي رقم 35 لسنة 1992.

(6) قانون العقوبات المصري رقم 58 لسنة 1937.

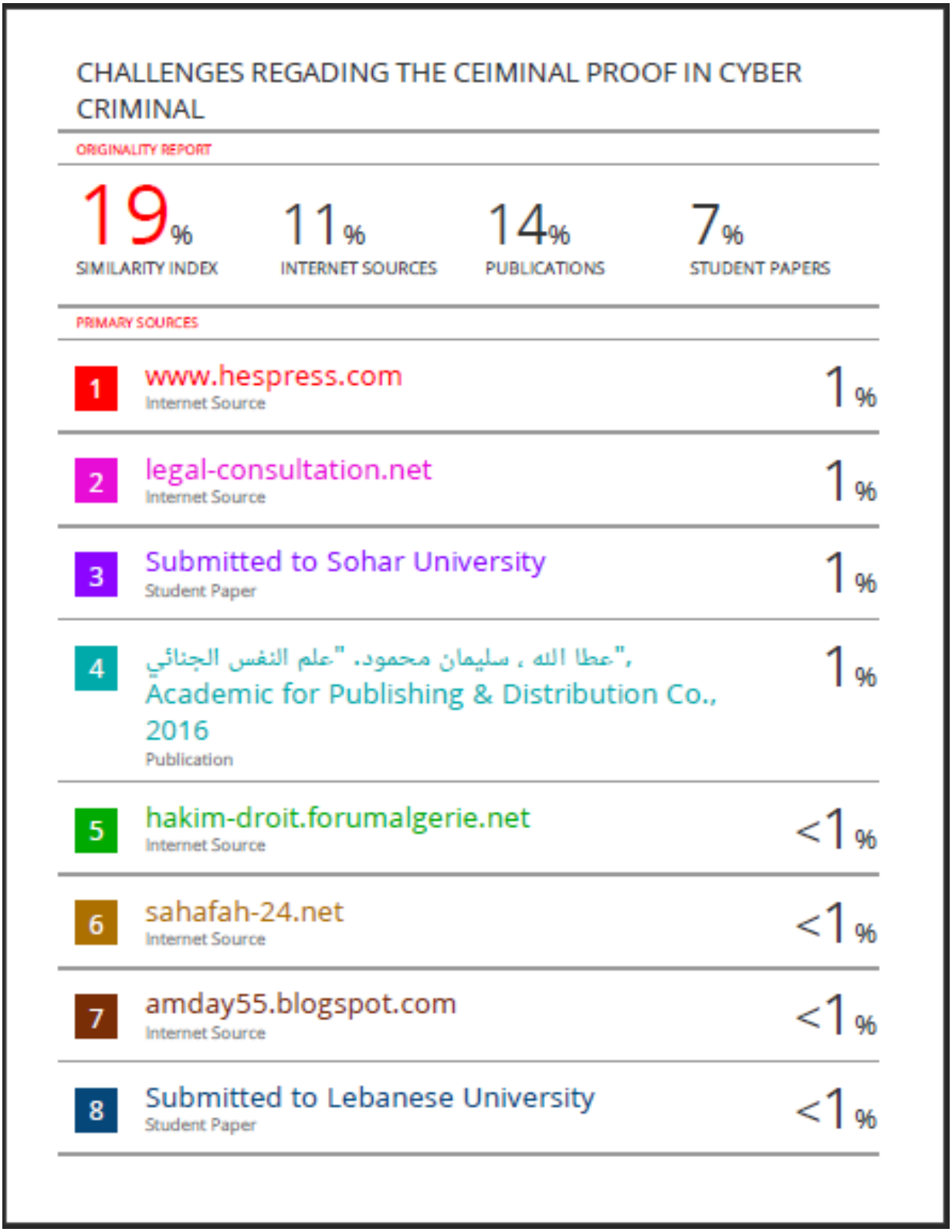
(7) قانون الإجراءات الجنائية المصري رقم 150 لسنة 1950.

(8) قانون الإجراءات الجنائية البحريني رقم 46 لسنة 2002.

سابعاً:- البحوث الإلكترونية.

(1) اشكالية إثبات الجرائم الإلكترونية www.ahewar.org .

تقرير الاستيلال



CHALLENGES REGADING THE CEIMINAL PROOF IN CYBER CRIMINAL

ORIGINALITY REPORT

19%	11%	14%	7%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.hespress.com Internet Source	1%
2	legal-consultation.net Internet Source	1%
3	Submitted to Sohar University Student Paper	1%
4	عطا الله ، سليمان محمود. "علم النفس الجنائي", Academic for Publishing & Distribution Co., 2016 Publication	1%
5	hakim-droit.forumalgerie.net Internet Source	<1%
6	sahafah-24.net Internet Source	<1%
7	amday55.blogspot.com Internet Source	<1%
8	Submitted to Lebanese University Student Paper	<1%

NEAR EAST UNIVERSITY
INSTITUTE OF GRADUATE STUDIES
PUBLIC LAW PROGRAMS / ARABIC

To the Institute of Graduate Studies

Mr. Qahtan Tawfeeq Khaleel Al Wahb (20185703), studying in Public law Arabic Program has finished the master thesis titled "**Difficulties with criminal proof in cyber crimes**" and used literature review in Research Methodology in writing the thesis. For this reason, ethical Review board report permission will be needed for the designed research.

Sincerely,

Prof.Dr. Weadi Sulaiman Ali