Legal regulation of digital fraud

M.M. Alaa Mohammed Al-Akeedi*, Zainab Abdul-Wahid Abdul-Sattar*

College of Law and Political Science / Al-Bayan University*, University of Anbar*

alaa.moh@albayan.edu.iq , Zalbayate80@uoanbar.edu.iq

Abstract

Digital fraud is a modern crime that emerged as a result of technological advancements and the proliferation of electronic means in various areas of life. It refers to any fraudulent behavior carried out using computers, the internet, or any digital means with the aim of seizing others' money or achieving illicit gains. Perhaps the danger of this crime lies in its difficulty in detecting it, the speed of its execution, and its transnational effects. To combat this type of crime, it has become necessary to rely on digital evidence, which is the data and information stored or transmitted electronically that can prove the occurrence of the crime and identify its perpetrator. Digital evidence includes: emails, login records, data stored on devices, and financial transactions.

Keywords: fraud, digital evidence, internet, data.

التنظيم القانوني لجريمة الاحتيال الرقمي

م.م آلاء محمد العكيدي*، زينب عبدالواحد عبدالستار*

كلية القانون و العلوم السياسية / جامعة البيان*، جامعة الانبار*

Zalbayate80@uoanbar.edu.iq * alaa.moh@albayan.edu.iq*

الملخص

يُعَدُّ الاحتيال الرقمي من الجرائم الحديثة التي ظهرت؛ أثر التطور التكنولوجي وانتشار الوسائل الإلكترونية في مجالات الحياة المختلفة. ويُقصد به أي سلوك احتيالي يتم بتشغيل الحواسيب أو شبكات الإنترنت أو أي وسيلة رقمية هادفا الاستيلاء على أموال الغير أو تأمين مكاسب غير مشروعة. ولعل خطورة هذه الجريمة تختبئ في صعوبة اكتشافها وسرعة تنفيذها وامتداد آثارها عبر الحدود. ولمواجهة هذا النوع من الجرائم، أصبح من الضروري الإعتماد على الأدلة الرقمية، وهي تلك البيانات والمعلومات المخزنة أو المنقولة إلكترونيًا والتي يُمكن أن تثبت وقوع الجريمة وتحدد مرتكبها. وتشمل الأدلة الرقمية: رسائل البريد الإلكتروني، سجلات الدخول، البيانات المخزنة في الأجهزة، والمعاملات المالية.

الكلمات المفتاحية: الاحتيال، الادلة الرقمية، الانترنت، البيانات.

المقدمة

أولاً– التعريف بالموضوع:

تُعد الثورة الرقمية –التي بزغت مؤخراً – ثورة جديدة لا تقل أهمية عن الثورة الصناعية، كيف لا وهي التي أحدثت تغييراً كبيراً في حياة الانسان وأثرت على المجتمع والدولة على حداً سواء، فلم يكن أحداً بمنأى عن آثارها، بل اصبح تقدم الدول يُقاس بمدى اعتمادها على الأدوات الرقمية في أداء مهامها بل ان بعض الدول بدأت تتجه إلى الذكاء الإصطناعي الذي يعد أحدث ناتجاً للثورة الرقمية.

وبالرغم من مميزات العصر الرقمي الذي نعيشه الآن إلا انه لا يخلو من المساوئ والتعقيدات، وهذا ما نلمسه من خلال ظهور الجرائم الرقمية التي تتسم بالتعقيد والغموض، فهي تمثل بحق الجانب المظلم في ثورة العالم الرقمي، التي كان الهدف من انشائها منفعة البشرية وتقريب المسافات بينهم وتسهيل تعاملاتهم، بينما تحولت اليوم إلى سلاح يستخدمه البعض للإيقاع بالآخرين واستغلالهم، مما يثير تساؤلات حول الأبعاد القانونية لهذه الممارسات.

من هنا بدأت الدول تستشعر إن العالم الرقمي، رغم بريقه الذي يخطف الأبصار، يخبئ في طياته مساوئ عديدة، ولعل التحايل الرقمي هو أهم تلك المساوئ التي أضحت اليوم ظاهرة سلبية تتفاقم في الدول بصورها التي تتنوع بين الإغراءات الوهمية، وانتحال الشخصيات والاختراق وغيرها من الصور التي تتميز بكونها ضربات ممنهجة تستهدف الثقة التي تربط الناس في فضاء افتراضي، حيث تختلط الحقيقة بالخداع. ومع ازدياد هذه الجرائم في العراق، بات لزامًا علينا الغوص في أعماقها لنفهم دوافعها وآلياتها، ونستنهض أدواتنا القانونية والتقنية لمواجهتها.

ثانياً– أهمية الموضوع:

ان أهمية هذا الموضوع تنبع من تسليط الضوء على جريمة مهمة لم يعد أحداً بمنأى عنها خصوصاً وان حياة البشر بجميع جوانبها أصبحت مرتبطة بالعالم الرقمي والإلكترونيات، فجريمة الاحتيال الرقمي لم يسلم منها الافراد ولا المؤسسات، وبالإضافة إلى ذلك، فإن الإجراءات القانونية الحديثة، التي لم تواكب التغيرات السريعة في الفضاء الرقمي، تعتبر من أبرز العوامل التي تتيح للمحتالين التسلل بسهولة، مما يثير الحاجة الملحة لتطوير قوانين محدثة وفعّالة في مواجهة هذه الجريمة.

ثالثاً– إشكالية الموضوع:

ان ابرز إشكالية يطرحها هذا الموضوع هي ضعف المواجهة القانونية لهذه الجريمة المهمة التي تعد من الجرائم المعقدة جداً نظراً لارتكابها بطرق غير تقليدية فهي تتم في الفضاء الرقمي الذي يستحيل مراقبته أو رصده وهذا ما زاد الحاجة إلى تطوير آليات قانونية لرصدها ومكافحتها.

فالتساؤل الرئيسي الذي يطرحه هذا البحث يتمثل في مدى استجابة القانون العراقي لمعالجة هذه الجريمة؟ وفي ضوء هذا التساؤل تتفرع عدة تساؤلات نوجزها فيما يلي:

١–ما هي جريمة الاحتيال الرقمي؟

٢–ما هي الادلة الرقمية ؟

رابعاً– منهجية الموضوع:

سنعتمد في هذه الدراسة على المنهج التحليلي من خلال البحث في النصوص القانونية العراقية والمقارنة ان استدعى الامر وكذلك اراء الفقه القانوني والتطبيقات القضائية ذات الصلة بموضوع البحث للوصول الى أفضل النتائج.

خامساً– هيكلية الموضوع:

لغرض معالجة موضوع الدراسة فقد قسمنا هذا البحث على مطلبين عالجنا في الأول مفهوم جريمة الاحتيال الرقمي وخصصنا الثاني للادلة الرقمية وحجيتها في الاثبات.

وسبق البحث بمقدمة اوجزنا فيها مفردات البحث وخُتِم بخاتمة تضمنت اهم النتائج والتوصيات.

المطلب الأول

مفهوم الاحتيال الرقمي

نتج عن تطور التقنيات الرقمية الحديثة في مجالات الاتصال والحوسبة إلى تطور جريمة الاحتيال التي ظهرت بهذه الصورة المعاصرة، وللتعريف بها ودراستها وفهمها بشكل جيد لابد من الرجوع الى الماضي القريب لدراسة تطورها التأريخي والتشريعي والتغيرات التي طرأت عليها بالتوازي مع التطور التقني للامكانيات التي يوفرها نظام الحاسوب حتى وصولها الينا بالشكل الحالي.

الفرع الاول

تعريف جريمة الاحتيال الرقمي

سنحاول في هذا الفرع تناول التعريفات اللغوية والتشريعية والفقهية لجريمة الاحتيال عموما وجريمة الاحتيال الرقمي كصورة مستحدثه من جريمة الاحتيال التي لازالت غير واضحة المعالم في اغلب التشريعات وخصوصا التشريعات العربية، وذلك من خلال التالي :

أولاً– التعريف التشريعي:

الاصل ان المشرع لا يلجأ الى تعريف الكلمات أو الالفاظ القانونية لانها الفاظ واردة في نصوص يتعين تطبيقها في الحال والمستقبل ومن ثم لايلزم المشرع نفسه بتعريفات قد تقيده او تؤدي الى افقاد المرونة الواجبة في الاحكام القانونية، والمعلوم ان صياغة التعاريف ليست من مهام المشرع وانما من اختصاص الفقهاء[1]، فالتعريف مهما بذل في صياغته من جهد ودقة فلن يأتي جامعا لكل المعاني المطلوبة، ان جاء كذلك في زمن فقد لا يستمر في زمن آخر.

وبالرغم ان اغلب التشريعات المقارنة لم تورد في متن نصوصها تعريفا لجريمة الاحتيال بشكلٍ عام بل اكتفت ببيان صور ارتكاب الافعال على سبيل الحصر، لكننا نستطيع ان نستشف تعريف جريمة الاحتيال في هذه التشريعات العقابية العربية من خلال تطرقها لمرتكب هذه الجريمة بالرغم من عدم تعريفها لها بشكل مباشر، ومن هذه القوانين القانون العراقي الذي أشار إلى: "١– كل من توصل الى تسلم او نقل حيازة مال منقول مملوك للغير لنفسه اوالى شخص آخر وذلك باحدى الوسائل التالية:

أ. باستعمال طرق احتيالية .

(١) محمد هشام صالح عبدالفتاح ، جريمة الاحتيال ، دراسة مقارنة ،رسالة ماجستير مقدمة الى كلية الدراسات العليا، جامعة النجاح الوطنية في نابلس ، فلسطين، سنة٢٠٠٨،ص٨.

ب. باتخاذ اسم كاذب أوصفة غير صحيحة أو تقرير أمر كاذب عن واقعة معينة متى كان من شأن ذلك خدع المجني علية وحمله على التسليم .

٢- كل من توصل باحدى الطرق السابقة الى حمل آخر على تسليم او نقل حيازة سند موجد لدين او تصرف في مال او ابراء او على أي سند آخر يمكن استعمالة لاثبات حقوق الملكية او أي حق عيني آخر، او توصل باحدى الطرق السابقة الى حمل آخر على توقيع مثل هذا السند او اتلافة او تعديلة"[١].

وبعد ان تعرفنا على جريمة الاحتيال التقليدية نستعرض الان التعريفات التشريعية لجريمة الاحتيال الرقمي فقد سارت التشريعات التي جرمت هذا النوع من الاحتيال بان وضحته من خلال مرتكب الجريمة (الاحتيال) ومنها قانون العقوبات الالماني الذي اشار إلى: "كل من يقوم بنية الحصول لنفسه او لشخص ثالث على منفعة مادية غير مشروعة، بالاضرار بممتلكات الغير، عن طريق التاثير في نتيجة المعالجة الالية للبيانات، من خلال برمجة غير صحيحة، او استعمال بيانات غير صحيحة او غير مكتملة، او عن طريق الاستعمال غير المصرح به للبيانات، او عن طريق التدخل غير المصرح به في عملية المعالجة ذاتها يعاقب...." [٢].

كما حذا المشرع اليوناني حذو المشرع الالماني فقد بين صور ارتكاب جريمة الاحتيال الرقمي التي نستطيع ان نستخلص منها تعريف هذه الجريمة حيث ذكر القانون[٣]: يعد مرتكباً لجريمة الاحتيال الرقمي، كل من يقوم بالتاثير في المعلومات المبرمجة عن طريق برمجة غير سليمة، او عن طريق التدخل اثناء تطبيق البرنامج، او عن طريق استعمال بيانات غير سليمة او غيرمكتملة او بأية طريقة اخرى، مما يترتب علية حدوث اضرار لممتلكات الغير، على ان يكون ذلك بنية اثراء نفسه او غيره بربح غير مشروع. كما اطلقت الاتفاقية الاوربية حول الجريمة الافتراضية (اتفاقية بودابست لسنة ٢٠٠١) Europe Convention On Cyber-Crime تسمية (الاحتيال المرتبط بالحاسوب) على جريمة الاحتيال الرقمي واعتبرت ان جريمة الاحتيال الرقمي تقع: "عندما يقوم شخص عن قصد، وبدون وجه حق، وعلى نحو يسبب خسارة في ممتلكات الغير بما يلي :

أ- أي ادخال او تعديل او حذف او كتم لبيانات الحاسوب.

ب- أي تدخل في وظائف نظام الحاسوب.

---

(٢) المادة (٤٥٦) قانون العقوبات العراقي لسنة ١٩٦٩المعدل النافذ .

(١) المادة (A/263) قانون العقوبات الالماني وله تعديلات كثيرة اخرها سنة ١٩٩٤ ومتوفر على الموقعwww.iuscopm.org ، آخر زيارة ٢٠٢٥\٥\٢٣.

(٢) المادة (A386) قانون العقوبات اليوناني لسنة ١٩٥٠، متوفر على الموقعwww.jurist.law.edu .آخرزيارة ٢٠٢٥\٥\٢٣.

وبنية احتيالية او غير شريفة بغرض الحصول دون حق على منفعة اقتصادية لنفسه او لغيره"[١].

اما (القانون العربي الاسترشادي لمكافحة جرائم تقنية انظمة المعلومات وما في حكمها) المعتمد من جامعة الدول العربية سنة ٢٠٠٣ فقد اورد وصفاً لجريمة الاحتيال الرقمي والتي اطلق عليها تسمية (جريمة الاحتيال عن طريق الشبكة الرقمية والحاسوب) أذ اشار القانون[٢] "كل من توصل عن طريق الشبكة الرقمية او احد اجهزة الحاسب الالي وما في حكمها، الى الاستيلاء لنفسه او لغيره، على مال منقول اوعلى سند او توقيع هذا السند، وذلك بالاستعانة بطريقة احتيالية أو اتخاذ اسم كاذب أو انتحال صفة غير صحيحة، متى كان ذلك من شانه خداع المجني عليه، يعاقب...." .

وقد سار المشرع العراقي على نفس النهج في مشروع قانون جرائم الرقمية الذي لم يصدر حتى تاريخ اعداد هذا الرسالة أذ قام بتحديد اسلوب ارتكاب افعال الاحتيال الرقمي من خلال استخدام نظام الحاسوب او شبكة المعلومات، وذلك للاستيلاء على اموال الغير اوبرامج اوبيانات اوبطاقات الكترونية أو شفرات اوسندات اوعلامة تجارية اواستخدم بطاقة الكترونية غير شرعية، كما قام بتعريف الاحتيال[٣] بانه "التسبب بالحاق الضرر عن قصد وبدون وجه حق، بنية الاحتيال لتحقيق المصالح والمنافع بطريقة غير مشروعة للفاعل او الغيرعن طريق : استخدم عمداً نظام الحاسوب اوشبكة المعلومات....."

ثانياً– التعريف الفقهي:

قبل الدخول بالتعاريف الفقهية لجريمة الاحتيال الرقمي أرتأينا ان ندرج بعض التعاريف الفقهية لجريمة الاحتيال التقليدية كونها الاساس الذي تطورت منة الجريمة موضوع دراستنا فالمستحدث فيها هو وسيلة الاحتيال على المجنى عليه من اجل خداعة والاستيلاء على أمواله بمختلف صور هذه الاموال.

أختلف الفقهاء في الوصول الى تعريف محدد لجريمة الاحتيال التقليدية وذلك باختلاف الزاوية التي ينظر كل منهم لهذه الجريمة وايضاً باختلاف التشريعات العقابية التي ينتمي اليها هؤلاء الفقهاء، وفيما يلي نماذج من هذه التعريفات:

يعرف أحد الفقهاء[٤] جريمة الاحتيال بأنها " الاستيلاء على الحيازة الكاملة لمال الغير بوسيلة يشوبها الخداع تسفر عن تسليم ذلك المال" وعرفها آخر[١]بانها " استعمال وسيلة من وسائل التدليس التي نص

(٣) المادة (٨) من اتفاقية بودابست وبنود الاتفاقية متوفرة على الموقع www.conventions.co.int، اخر زيارة ٢٠٢٥\٥\٢٥.

(٤) المادة (١٠) من القانون العربي الاسترشادي لمكافحة جرائم تقنية انظمة المعلومات وما في حكمها وهو متوفر على الموقع الالكتروني www.protectionproject.org/wp./12، آخر زيارة ٢٠٢٥\٥\٥.

(١) المادة (١٠) مشروع قانون الجرائم المعلوماتية العراقي متوفرعلى الموقع الالكتروني www.slideshare.net/hamzoz/1-25979225 آخر زيارة ٢٠٢٥\٥\١٨.

(٢) د.حسن صادق المرصفاوي ، قانون العقوبات الخاص ، منشأة المعارف ، الاسكندرية ،١٩٧٥،ص٣٩٤.

عليها القانون على سبيل الحصر لحمل المجني علية على تسليم الجاني مالاً مملوكاً لغيرة نتيجة الوقوع في الغلط " وعرفت ايضا[٢]بانها " الاستيلاء على مال منقول مملوك للغير باستعمال طرق احتيالية بنية تملكه "

أما في الفقه العراقي فهناك من عرف جريمة الاحتيال[٣]بانها " تلك الجريمة التي تتحقق من خلال استعمال الجاني لوسيلة من وسائل التدليس المنصوص عليها حصراً في القانون، بقصد ايهام المجنى عليه وتضليله وحمله على تسليم مال منقول مملوك لغير الجاني" وعرفها فقيه عراقي آخر[٤]بانها " تلك الجريمة التي تتحقق من خلال توصل الجاني، او شخص آخر الى تسلم مال منقول مملوك للغير بدون وجه حق، نتيجة استخدام الجاني لأحدى وسائل الخداع المنصوص عليها في القانون على سبيل الحصر، والتي تسفر عن وقوع المجني عليه في الغلط الدافع للتسليم"

وبعد تناول التعريفات الفقهية لجريمة الاحتيال بصورتها التقليدية نتناول تعريفاتها الفقهية بصورتها الرقمية، لقد تعددت ايضاً تعريفات جريمة الاحتيال الرقمي وتعددت كذلك تسمياتها فاستخدم البعض تسمية الغش الرقمي واستخدم آخرون تسمية غش الحاسوب وكذلك أسماه البعض الاحتيال المرتبط بالحاسوب، ولكن كل التسميات والتعاريف تلتقي اغلبها حول وصف الجرم بانه سلوك احتيالي او خداعي مرتبط باستخدام الحاسوب يهدف مرتكبه الى تحقيق فائدة او مصلحة مالية، ومن هذه التعريفات في الفقه[٥] الاحتيال الرقمي هو " أي سلوك احتيالي ينتهج منهج الحوسبة بنية الحصول على امتياز مالي" كذلك عرف البعض الاحتيال الرقمي[٦]بانه " التلاعب العمدي بمعلومات وبيانات تمثل قيما مادية يختزنها نظام الحاسب الالي، او الادخال غير المصرح به لمعلومات وبيانات صحيحة، أو التلاعب في الاوامر والتعليمات التي تحكم عملية البرمجة، او أي وسيلة اخرى من شانها التأثير على الحاسب الالي حتى يقوم بعملياته بناءً على هذه البيانات أو الأوامر أو التعليمات، من أجل الحصول على ربح غير مشروع والحاق الضرر بالغير".

---

(٣) فاديه يحي ابوشهنبه، النظرية العامة للطرق الاحتيالية في القانون المصري المقارن، رسالة دكتوراه كلية الحقوق جامعة عين شمس،١٩٨٤،ص٢٩١.

(٤) احمد شوقي عمرابوخطوة ، شرح قانون العقوبات القسم الخاص ، جرائم الاعتداء على الاموال ، دار النهضة العربية ، القاهرة ،١٩٩٤، ص١٩٦.

[٣](٥) د.حميد السعدي ، جرائم الاعتداء على الاموال ، مطبعة المعارف ، بغداد ،١٩٦٧، ص٤٢٠.

(٦) اياد حسين عباس العزاوي، جريمة الاحتيال في القانون العراقي، ط١، بدون دار نشر، بغداد، ١٩٨٨، ص٣٨.

(١) د.عمر محمد ابوبكر بن يونس ، الجرائم الناشئة عن استخدام الانترنت ، مصدر سابق ،ص٤١١.

(٢) د.نائلة عادل محمد فريد ، جرام الحاسوب الالي الاقتصادي، ط١، منشورات الحلبي الحقوقية، بيروت، ٢٠٠٥، ص٤٢٥.

ومن تعريفات جريمة الاحتيال الرقمي تعريف مكتب التحقيقات الفدرالي الامريكي "أي مخطط أحتيالي عبر الانترنت، يلعب دوراً هاماً في عرض السلع والخدمات غير الموجودة أصلاً أو طلب دفع ثمن تلك الخدمات أو السلع عبر الشبكة"[١] كذلك عرفتها وزارة العدل الامريكية بانها "شكل من التخطيط الاحتيالي، الذي يستخدم محتويات الانترنت، كالدردشة، البريد الالكتروني، المواقع الالكترونية، لتقديم صفقات أحتيالية أو لإرسال نتائج الاحتيال الى المؤسسات المالية"[٢]ونلاحظ من التعريفين السابقين انهما تناولا جانب واحد من جريمة الاحتيال الرقمي وهو الاحتيال عبرالانترنت وأهمل الاحتيال الرقمي في نطاق الحاسوب والشبكات المحلية دون الولوج إلى الانترنت لأن الاحتيال الرقمي يشمل الجانبين ولايقتصر على الاحتيال عبر الانترنت المذكور في التعريفين السابقين، كما أن التعريفين حصرا وسائل الاحتيال بعرض السلع والخدمات غيرالموجودة او تقديم الصفقات الاحتيالية، ويرى الباحث ان طبيعة وسائل الاحتيال صعبة الحصر فالأفضل عدم ذكرها في تعريف الجريمة. كما عرفتها لجنة تدقيق الحسابات في المملكة المتحدة(Audit Commission) حيث أطلقت عليها تسمية (غش الحاسب الآلي) بأنها "أي سلوك احتيالي أو خداعي مرتبط بالكومبيوتر يهدف شخص بواسطته إلى كسب فائدة أو مصلحة مالية"[٣] ولايسلم هذا التعريف من النقد كونه ربط مفهوم الاحتيال بالهدف منه وهو تحقيق الجاني للفائدة المالية لنفسه، فقد يكون الهدف إلحاق الضرر بالمجني عليه فقط .

بناءً على ما تقدم، نستشف ان جريمة الاحتيال الرقمي هي استيلاء عن طريق الشبكة الرقمية وباستخدام طرق الخداع الرقمي الحديثة والمتطورة على مال ما أو معلومات أو برامج أو على سند يتضمن تعهداً أو إبراءً أو أي امتياز مالي آخر، حيث يستخدم المجرم الرقمي أو مرتكب جريمة الاحتيال الرقمي هذه الوسائل التي لا يمكن حصرها أو تحديدها نظراً للتطور المستمر في العالم الرقمي والذي يصاحبه تطور في وسائل الخداع والاحتيال الرقمي ايضاً.

---

(٣) د.محمد طارق عبدالرؤوف الخن ، جريمة الاحتيال عبر الانترنت، منشورات الحلبي الحقوقية، بيروت ، ٢٠١١، ص٣٨.

(4)Micheal Kunzand& Patrick Wilson:computer crime and computer fraud p12.،2004،USA،Maryland

(5) محمود احمد عبابنة ، جرائم الحاسوب وابعادها الدولية ، دار الثقافة للنشر والتوزيع ، عمان، الاردن ، ٢٠٠٥ ، ص٥٥.

الفرع الثاني

خصائص جريمة الاحتيال الرقمي

بما أن جريمة الاحتيال الرقمي كغيرها من الجرائم الرقمية، هي إفراز ونتاج لتقنية المعلومات، فهي ترتبط بها وتقوم عليها، ومع ازدهار حجم ودور هذه التقنية في القطاعات المختلفة أدى ذلك إلى إعطاء هذا النوع من الجرائم، طابعاً قانونياً يميزها عن غيرها وذلك بمجموعة من الخصائص سنحاول توضيحها، ولعل أبرز خصائص جريمة الاحتيال الرقمي و هي مايلي :

أولاً– جريمة الاحتيال الرقمي متعدية الحدود او جريمة عابرة للدول:

بما أن المجتمع الرقمي لا يعترف بالحدود الجغرافية وهو مجتمع منفتح عبر شبكات تخترق الزمان والمكان دون أن تخضع لحرس الحدود، فغالباً ما يكون الجاني في بلد والمجني علية في بلد آخر، كما قد يكون الضرر المتحصل في بلد ثالث في الوقت نفسه، وعليه تعتبر جريمة الاحتيال الرقمي، شكلاً جديداً من الجرائم العابرة للحدود الوطنية أو الاقليمية أوالقارية[١]، وهذه الخصيصة خلقت العديد من المشاكل حول تحديد الدولة صاحبة الاختصاص القضائي بهذه الجريمة، وكذلك حول تحديد القانون الواجب تطبيقه بالاضافه إلى اشكاليات تتعلق بإجراءات الملاحقة القضائية، وغير ذلك من النقاط التي تثيرها الجرائم العابرة بشكل عام، وبالنتيجة لهذه الطبيعة الخاصة لجريمة الاحتيال الرقمي بشكل خاص والجرائم الرقمية بشكل عام، ونظراً للخطورة التي تشكلها على المستوى الدولي، والخسائر التي قد تتسبب بها، تعالت الاصوات الداعية الى التعاون الدولي الكثيف من أجل التصدي لهذه الجرائم[٢]، ويتجسد هذا التعاون في المعاهدات والاتفاقيات الدولية التي تعمل على توفير جو من التنسيق بين الدول الاعضاء الأمر الذي يكفل الايقاع بالمجرم الرقمي وتقديمه إلى القضاء العادل، وتكمن أهم المشاكل المتعلقة بالتعاون الدولي بهذا الشأن، في انه لا يوجد مفهوم عام مشترك بين الدول حول صور النشاط المكون لهذه الجريمة، بالإضافة إلى نقص الخبرة لدى الشرطة وجهات الادعاء والقضاء في هذا المجال لتمحيص عناصر الجريمة وجمع الادلة عنها للإدانة، يشكل عائقاً كذلك أمام التعاون في مجال مكافحة هذا النوع من الجرائم[٣]. وتمثل هذه الخصيصة أهم فارق بين جريمة الاحتيال المرتكبة في العالم المادي(الاحتيال التقليدي) وجريمة الاحتيال المرتكبة في العالم الافتراضي(الاحتيال الرقمي)، أذ تبرز

---

(١) أسامة أحمد المناعسة وآخرون ، مصدر سابق ، ص١٠٦.
(٢) نهلا عبدالقادر المومني ، الجرائم المعلوماتية ،ط١، دار الثقافة ، عمان، ٢٠٠٨، ص٥٢.
(٣) محمد محي الدين عوض ، مشكلات السياسة الجنائية الجنائية المعاصرة في جرائم نظم المعلومات (الكومبيوتر)، ورقة عمل مقدمة الى المؤتمر السادس للجمعية المصرية للقانون الجنائي، دار النهضة العربية، القاهرة،١٩٩٣،ص٣٦٢.

شخصية الجاني في الاولى ويكون هناك اتصال مادي بين الجاني والضحية، اما في الثانية فتتم افعال الاحتيال دون الحاجة الى بروز مادي للجاني اذ يكتفي الجاني بإعداد موقع أو برمجة سمعية مرئية يقوم بإعدادها للاحتيال على المجني عليه بقصد الاستيلاء على أمواله، فعوضاً عن الجسد أو الهيئة في العالم المادي يكون هناك الموقع الالكتروني او الخادم في العالم الرقمي[١].

ثانياً– صعوبة أكتشاف واثبات جريمة الاحتيال الرقمي:

لا تحتاج جريمة الاحتيال الرقمي إلى أي عنف أو سفك للدماء أو اقتحام مكان لسرقة الاموال، وانما هي أرقام وبيانات تتغير أو تمحى تماماً من السجلات المخزونة في ذاكرة الحاسوب، ولأنها –في اغلب الأحيان– لاتترك أي أثر خارجي مرئي لها، فأنها تكون صعبة الاكتشاف، ومما يزيد من صعوبة ذلك، عدم وجود أي أثر خارجي لما يجري خلال تنفيذها من عمليات او افعال إجرامية، حيث تتم بالنبضات الكهربائية نقل البيانات والمعلومات كما ان هذه الجريمة شأنها شان أغلب الجرائم الرقمية الاخرى، ترتكب غالبا –كما سبق ان ذكرنا– على صعيد اكثر من دولة باستخدام شبكة الانترنت ودون تحمل عبء الانتقال[٢]، كما ان المجنى عليه أحيانا يلعب دوراً رئيسيا في صعوبة اكتشاف وقوع جريمة الاحتيال الرقمي أذ تحرص اكثر الجهات التي تتعرض انظمتها الرقمية للإحتيال وتمنى بخسائر فادحة من جراء ذلك، على عدم الكشف حتى بين موظفيها عما تعرضت له وتكتفي بأتخاذ أجراءات ادارية داخلية من دون الابلاغ عنها للسلطات المختصة تجنباً للاضرار بسمعتها ومكانتها وهز الثقة في كفائتها[٣]، وتبدو هذه الحالة اكثر وضوحاً في المؤسسات المالية كالبنوك والمؤسسات الادخارية ومؤسسات الاقراض، حيث تخشى مجالس اداراتها، ان تؤدي الدعاية السلبية التي تنجم عن كشف هذه الجرائم أو اتخاذ الاجراءات القانونية حيالها الى تضاؤل الثقة فيها من جانب المتعاملين معها، كما ان للمجنى عليه دوراً يثير الريبة في بعض الاحوال فهو يشارك في الجريمة بشكل غير مباشر نتيجة القصور الامني في أنظمته الرقمية مع الامكانية بتلافي هذا القصور بتطوير نظم الامن الخاصة بانظمة الحواسيب وشبكاتها[٤].

ومن الجدير بالذكر أنه حتى في حالة اكتشاف وقوع الجريمة والابلاغ عنها، فان اثباتها امر يحيط به الكثير من الصعاب، أذ ان ارتكابها في بيئة الحاسوب والانترنت يجعل عملية طمس الدليل ومحوه

---

(٤) د.محمد الشناوي، جرائم النصب المستحدثة ، دارالكتب القانونية ، المحلة الكبرى ، مصر،٢٠٠٨، ص٨٥.
(١) د هشام محمد فريد رستم ، مصدر سابق ، ص٤٠
(٢) محمد عبدالله أبوبكرسلامه ، موسوعة الجرائم المعلوماتية: جرائم الكومبيوتر والانترنت، المكتب العربي الحديث، الاسكندرية، ٢٠١١، ص٩٧.
(٣) نهلا عبدالقادرالمومني ، مصدر سابق ، ص٥٥.

كلياً، من الفاعل امر في غاية السهولة، فاذا كانت الجريمة التقليدية تخلف اثارا مادية في مسرح الجريمة مما يفسح المجال امام سلطات التحري والتحقيق للكشف عن تفاصيل هذه الجريمة وذلك عن طريق المعاينة والتحفظ على الاثار المادية، لكن فكرة مسرح الجريمة في جريمة معلوماتية يتضاءل دورة في الافصاح عن الحقائق المؤدية للإدلة المطلوبة، ممايلزم البحث عن ادلة جديدة ناتجة من ذات نظام الحاسوب، ومن هنا تبدأ مشكلة قبول هذه الادلة إن وجدت، ومدى مصداقيتها في اثبات وقائع الجريمة[١].

ثالثاً– اسلوب ارتكاب جريمة الاحتيال الرقمي:

تتميز جريمة الاحتيال الرقمي باسلوب ارتكابها الناعم، أذ لا تحتاج الى مجهود عضلي كجرائم القتل والسرقة وغيرها بل كل ما تحتاج اليه هو الدراية الذهنية والتفكير العلمي المدروس القائم على معرفة بتقنيات الحاسوب والاحاطة ببعض البرامج التشغيلية، لذلك يطلق على هذا النوع بجرائم الياقات الزرقاء أو البيضاء، كما تسمى (الجرائم الناعمة)[٢]Soft Crime.

رابعاً– جريمة الاحتيال الرقمي من الجرائم المغرية للمجرمين:

بما ان الجريمة موضوع البحث، تتم دون تجشم عناء الانتقال الى مسرح الجريمة وغالباً مايتمثل الركن المادي منها بكبسة معينة على لوحة المفاتيح في الحاسوب وامام ضخامة الفوائد والمكاسب التي يمكن للجاني تحقيقها باقتراف مثل هذه الجريمة من دون جهد وخوف من اكتشافها بسهولة، أمام ذلك كله شكلت هذه الجريمة ومثيلاتها، اغراءاً كبيراً للمجرمين لاستغلال التكنولوجيا الحديثة، بغية اقترافها خصوصاً عندما يكون الجاني موظفا في شركة تعتمد على النظام الرقمي في اعمالها، اذ يكون لدى الجاني(الموظف) كافة المعلومات اللازمة لتحقيق اختراقات متعددة ومتتالية لأنظمة الحاسوب في الشركة وتحقيق أرباح طائلة، ويكفي أن ندلل على ذلك بحادثة في فرنسا سنة ١٩٨٦حيث كان العائد من ارتكاب جناية سرقة مع حمل سلاح هو(٧٠٠٠فرنك) في حين ان جريمة أحتيال معلوماتي تمت في مجال نظام المعالجة الالية للمعلومات في احدى الشركات، حصل منها الجاني على (٢٧٠٠٠٠فرنك) أي مايعادل ٣٨ مرة المبلغ المتحصل من الجريمة الاولى[٣].

خامساً– خصوصية مرتكبي جريم الاحتيال الرقمي:

---

(٤) محمد عبدالله ابو بكرسلامه ، المصدر السابق ، ص٩٨.
(٥) اسامة احمد المناعسة وآخرون ، مصدر سابق ، ص١٠٧.
(٢) د.احمد خليفة الملط ، مصدر سابق ، ص ٨٩.

يتسم مرتكب جريمة الاحتيال الرقمي بسمات معينة تميزه عن المجرم التقليدي، فاذا كانت جريمة الاحتيال التقليدية تحتاج الى ذكاء المجرم ودهائه، والى هيئة وشخصية تدل على الاحترام، فهو انيق المظهر، مقبول الشكل ويتمتع بضبط النفس وموهبة في حبك الاكاذيب وقد يكون البعض من المحتالين يتكلمون عدة لغات وبطلاقة خاصة ممن احترفوا الاحتيال الدولي والاحتيال خاصة على الاجانب والسياح[١]، فالمحتال التقليدي تبرز شخصيته في مسرح الاحداث ويعتمد عليها في ارتكاب جريمته، فان جريمة الاحتيال الرقمي من الجرائم التقنية التي يرتكبها ذوي اختصاص في مجال تقنية المعلومات، او على الاقل لديه الحد الادنى من المعرفة والقدرة لاستعمال جهاز الحاسوب والتعامل مع شبكة الانترنت[٢].

المطلب الثاني

أدلة الإثبات الرقمية في جريمة الاحتيال الرقمي وحجيتها

إن كشف معالم جريمة الاحتيال الرقمي يتحقق من خلال أدلة الإثبات ، لأنها تلعب دوراً مهماً في إثبات هذه الجريمة، و هذه الادلة التي يمكن الاعتماد عليها هي نفس الأدلة التقليدية في اثبات جريمة الاحتيال عموماً، الا أنه يمكن فيما يتعلق بجريمة الاحتيال الرقمي الاعتماد خاصة على الأدلة المستحدثة (الرقمية) ، لذلك سنتناول الأدلة الرقمية بالبحث لبيان مدى أهميتهما بالنسبة لعملية الاثبات الجنائي في جريمة الاحتيال الرقمي وحجيتها في الاثبات ، وعلى الوجه الآتي :

الفرع الاول

الأدلة الرقمية لإثبات جريمة الاحتيال الرقمي

إن تأثير ثورة المعلومات و التكنولوجيا على طبيعة جريمة الاحتيال الرقمي أدى إلى ظهور نوع جديد من الأدلة الذي يتماشى مع طبيعة هذه الجريمة، وهذه الأدلة تعرف بالأدلة الرقمية، وهي الأدلة الناتجة عن فحص المكونات المعنوية أو البرمجية للحواسيب و شبكة الأنترنيت .

(٣) أياد حسين عباس العزاوي ، مصدر سابق ، ص٤١.
[١] نهلا عبدالقادر المومني ، مصدر سابق ، ص٥٩.

والدليل الرقمي عبارة عن دليل مأخوذ من أجهزة الحاسب الآلي ويكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية ، يمكن تجميعها و تحليلها باستخدام برامج و تطبيقات و تكنولوجيا خاصة ، ويتم تقديمها في شكل دليل يمكن اعتماده أمام القضاء[١].

ومن خلال هذا التعريف يتضح بأن الدليل الرقمي يتم استخراجه من الحاسب الآلي ، ولا شك أن ذلك فيه تضييق لدائرة الأدلة الرقمية، فهي كل شيء يمكن أن يستخرج من الحاسب الآلي أو أي تقنيات إلكترونية أخرى كالهاتف او آلات التصوير و غيرها من الأجهزة التي تعتمد التقنية الرقمية في تشغيلها ويمكن ان تكون مصدراً للدليل الرقمي. الا أن هذا التعريف يخلط بين الدليل الرقمي و مسألة استخلاصه ، حيث تم تعريفه بأنه الدليل المأخوذ من الحاسب الآلي و هذا يعني إن الدليل الرقمي لا تثبت له هذه الصفة الا إذا تم أخذه أو استخلاصه من مصدره ، و هذا ليس صحيحاً ، لأن المجالات المغناطيسية أو الكهربائية قبل فصلها عن مصدرها بواسطة الوسائل الفنية لا تصلح لأن توصف بالدليل الرقمي، بمعنى إن مخرجات الآلة الرقمية لا تكون لها قيمة إثبات مادامت في الوسط الافتراضي الذي نشأت فيه أو بواسطته[٢]، لذلك عرف البعض الدليل الرقمي بأنه الدليل الذي يجد له اساساً في العالم الافتراضي و يقود الى الجريمة [٣].

وعلى أساس التعاريف السابقة نستنتج بأن الدليل الرقمي عبارة عن معلومات أو بيانات رقمية مخزنة في أجهزة الحواسيب ، أو منقولة بواسطتها ، ويمكن استخدامها في إثبات جريمة ما أو نفيها.

ويتميز الدليل الرقمي بالخصائص التالية :

١-إن طريقة نسخ الدليل الرقمي من أجهزة الكومبيوتر تقلل أو تعدم مخاطر إتلاف الدليل الأصلي لأن طريقة النسخ تتطابق مع طريقة الإنشاء[٤].

---

[١] د. ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الحاسب الآلي و الأنترنت، دار الكتب القانونية، القاهرة ، ٢٠٠٦ ، ص ٨٨.

[٢] د. محمود محمد محمود جابر ، الاحكام الاجرائية للجرائم الناشئة عن استخدام الهواتف النقالة جرائم نظم الاتصالات المعلومات ، المكتب الجامعي الحديث ، الاسكندرية، ٢٠١٧، ص ١٢٢-١٢٣.

[٣] د. محمد طارق عبد الرؤوف الخن ، جريمة الاحتيال عبر الانترنت، منشورات الحلبي الحقوقية ، بيروت،٢٠١١، ص ٣٤٠ .

[٤] مصطفى محمد موسى ، التحقيق الجنائي في الجرائم الرقمية ، مطابع الشرطة القاهرة ٢٠٠٩، ص ٢١٧ .

٢- يتميز الدليل الرقمي بالوضوح وذلك عند استخدام التطبيقات والبرامج، إذ يمكن معرفة إذا كان الدليل الرقمي قد عدل أو تم العبث فيه وذلك لإمكانية مقارنته بالأصل.

٣- لا يمكن إزالة أو تحطيم الدليل الرقمي من قبل الجاني ، لأنه يمكن اعادة الدليل الرقمي من خلال دسك[١].

٤- تتكون الأدلة الرقمية من مجموعة دوائر وحقول مغناطيسية و نبضات كهربائية غير ملموسة و لا يدركها الإنسان العادي بحواسه الطبيعية[٢].

وتقسم الأدلة الرقمية الى ثلاث مجموعات و هي :

المجموعة الأولى : السجلات المحفوظة في الحاسوب ، و هي الوثائق المكتوبة و المحفوظة مثل البريد الرقمي وملفات برامج معالجة الكلمات و رسائل غرف المحادثة على الأنترنيت.

المجموعة الثانية :السجلات التي جزء منها تم حفظه بالإدخال و جزء تم انشاؤه بواسطة الآلة مثل البيانات التي تم إدخالها إلى الآلة و تتم معالجتها من خلال برنامج خاص ، كإجراء العمليات الحسابية على تلك البيانات[٣].

المجموعة الثالثة : السجلات التي تم إنشاؤها بواسطة الحاسوب ، و تعتبر مخرجات برامج، و بالتالي لم يلمسها الإنسان مثل سجلات الهاتف و فواتير أجهزة السحب الآلي[٤].

ويمكن للتحقيقات الجنائية الوصول إلى الدليل الرقمي من خلال المصدرين التاليين :-

المصدر الأول : أنظمة الحاسوب و ملحقاتها:

تعد جميع أنظمة الحاسوب، بما فيها الحاسب الشخصي، من أهم المصادر التي يمكن لجهات التحقيق الوصول إليها ، و ذلك لما تحتويه من الأمور الشخصية للأفراد و سلوكياتهم و أفكارهم و مخططاتهم ونشاطاتهم و غيرها من المعلومات الأخرى عن هؤلاء الأشخاص لأن

---

[١] د.هبة حسين محمد زايد ، مصدر السابق ص ٢٤١.

[٢] د. محمد طارق عبد الرؤوف الخن، مصدر سابق، ص ٣٤٣.

[٣] د.ياسر محمد الكومي ، الحماية الجنائية والامنية للتوقيع الالكتروني، منشأة المعارف، الاسكندرية، ٢٠١٤، ص ٢٦٥.

[٤] د.هبة حسين محمد زايد ، الحماية الجنائية للصفقات الالكترونية، دار الكتب القانونية، القاهرة، ٢٠١٥، ص ٢٤٢.

هذه الملفات الشخصية أو ملفات النظام عامة عادة ما تحوي معلومات تتعلق بالجريمة و تفيد في كشف حقيقتها[١].

فضلاً عن ذلك إن المحقق يستفيد كثيراً من حجز الحاسوب وفحصه لأنه من خلال ذلك يكشف جميع خفايا جريمة الاحتيال الرقمي لأن الحاسوب هو وسيلة النفاذ الى هذه الشبكة ، أياً كان شكل هذا الحاسوب، بحيث لابد أن تشمل عملية الفحص جميع البرامج المخزنة في المكونات الصلبة أو أجهزة الذاكرة الملحقة بالحاسوب ، و جميع البرامج التي تم إلغاؤها من قبل ، و على المحقق أن يتأكد من أن مكونات الحاسوب و جميع برامجها تعمل بشكل سليم لأنه في حالة وجود خلل في البرامج أو إصابة الحاسوب بفيروسات فهذا ينال من صحة الدليل الرقمي المستخلص عند عرضه على القضاء[٢].

ونستنتج من خلال ما تقدم إن الدليل الرقمي وما يحتوي من خصائص يعدان نقطة البداية في الكشف عن خفايا جريمة المعلوماتية عامة وجريمة الاحتيال الرقمي خاصة، فمن خلاله يمكن فحص جميع البرمجيات المخزونة في المكونات الصلبة أو ملحقات الحاسوب، وحتى جميع البرامج التي تم الغاؤها من قبل.

المصدر الثاني: أنظمة الاتصال بالأنترنيت

على المحقق أن يقوم بفحص جميع أنظمة الاتصال بالأنترنيت ، وفحص حركة التنزيل والتحميل و درجة الاستيعاب ، و الشبكات المحلية ، و النظام الأمني المحاط بالأنترنيت ، لأن عملية الفحص هذه قد تؤدي الى الحصول على دليل رقمي يفيد في كشف الحقيقة .

ويستفيد المحقق من عملية فحص هذه الأنظمة المتصلة بالأنترنيت في التوصل إلى كشف مكان الجريمة، أو الحاسوب الذي ارتكب بواسطته النشاط الجرمي، فعن طريق الأنترنيت يمكن معرفة الحاسوب ، و يستخدم في هذه العملية نظام فحص الكتروني تطلق عليه تسمية (علم البصمات المعاصر)، و هذا منهج تم استخدامه في العديد من الجرائم، وكذلك في التوصل إلى

---

[١] عبد الله سيف الكيتوب ، الاحكام الاجرائية لجريمة الاحتيال المعلوماتي، دار النهضة العربية، القاهرة، ٢٠١٣، ص١٧٢ .

[٢] د. عمر محمد أبو بكر بن يونس، الاجراءات الجنائية عبر الانترنت في القانون الامريكي، القاهرة، ٢٠٠٥ ص١٠٠٨- ١٠٠٩.

الشخص الذي ابتكر موقع خدمات (بلومبرمج) الأخبار المال، و هو موقع احتيالي يرفع أسعار الأسهم بطريقة الخداع[١].

الا إن الإعتماد على أنظمة الأنترنيت لا يكفي لنسبة الجريمة إلى مالك الحاسوب ، لأنه قد يكون مالك الحاسوب ليس جانيا ، كما لو كان حاسوبه مسروقا أو مؤجراً في أحد مقاهي الأنترنيت أو أن يكون من يستخدم حاسوبه محتالاً أو أن المشتبه به لا يعرف أي شيء عن الأنترنيت ، الأمر الذي يتطلب من المحقق توفير دليل مادي كالاعتراف أو الشهادة أو الخبرة الى جانب الدليل الرقمي، حتى يمكن أن تنسب الجريمة الى مرتكبها[٢].

وعلى المحقق أن يقوم بجمع المعلومات التي توصل اليها عن طريق الدليل الرقمي و أن يشير إلى زمان البحث و مكان المعلومة و كيفية الحصول عليها و أن يستخدم البرمجيات التي تحافظ على مواقع الويب التي عمل بها ، لأنه من المعروف أن المعلومات تتغير على الأنترنيت من لحظة إلى أخرى[٣].

فضلاً عن هذا يستطيع المحقق أن يستخرج الدليل الرقمي المسند من الحاسوب أو الأنترنيت عن طريق الطباعة أو بشكل إلكتروني كالأشرطة و الأقراص الليزرية و غيرها من الأشكال الرقمية [٤].

وتستنتج من خلال ما تقدم إن الدليل الرقمي له دور كبير في عملية كشف معالم الجريمة و ذلك بما يقدمه من تسهيلات وإيضاحات كثيرة، ويمكن الاعتماد عليه كدليل جنائي .

ومع ذلك فان عملية الإثبات في جريمة الاحتيال الرقمي بالدليل الرقمي يعترضها عدد من الصعوبات، ومن أهمها :

أ- غياب الدليل المرئي

إن جريمة الاحتيال الرقمي قد يكون محلها جوانب معنوية تتعلق بالمعالجة الآلية للبيانات، ففي هذه الحالة قد تصعب إقامة الدليل بالنسبة لها بسبب الطبيعة المعنوية للمحل الذي وقعت عليه الجريمة ، لأن إثبات الأمور المعنوية يكون في غاية الصعوبة و ذلك لأنه لا يترك وراءه أي

---

[١] د. محمد طارق عبد الرؤوف الخن، مصدر سابق، ص ٣٤٨ .

[٢] عمر محمد أبو بكر بن يونس ، المصدر السابق، ص ٩٩٩.

[٣] د . محمد طارق عبد الرؤوف الخن، المصدر السابق، ص ٣٤٩ .

[٤] د. هلالي عبد اللاه أحمد ، حجية المخرجات الكومبيوترية في المواد الجنائية ، النشر الذهبي للطباعة ، القاهرة ، ١٥، ٢٠٠٢-١٦ .

آثار تدل عليه أو تكشف عنه ، وأن أغلب المعلومات والبيانات التي تتداول عبر الحسابات الآلية، والتي من خلالها تتم العمليات الرقمية ، تكون في هيئة رموز و نبضات مخزنة على وسائط تخزين ممغنطة بحيث لا يمكن للإنسان قراءتها أو إدراكها الا من خلال هذه الحاسبات[١].

ب–سهولة إخفاء الدليل

كثير من المحققين يواجهون صعوبة في الحصول على الدليل الرقمي، وذلك لأن الجناة في هذه الجرائم يتمتعون بالذكاء و الإتقان الفني ويستطيعون اخفاء أفعالهم غير المشروعة التي يقومون بها باستخدام الوسائل الرقمية ، و يستخدمون في ذلك التلاعب غير المرئي في النبضات أو الذبذبات الرقمية التي يتم تسجيل البيانات عن طريقها.

ت– الحجم الكبير للبيانات التي يوجد فيها الدليل الرقمي

إضافة إلى أن البيانات التي يوجد فيها الدليل الرقمي توجد في القرص الصلب بيانات أخرى بحجم كبير و غير مرئية ، لكن ما يتعلق بالجريمة قد يشكل جزءاً صغيراً فقط من هذه المعلومات، الأمر الذي يجعل من الصعوبة بمكان معرفة الإشارة المطلوبة وترجمتها الى بيانات ،مفهومة فالوصول الى الدليل الرقمي المطلوب يشكل تحدياً أمام الخبير المعلوماتي[٢].

ج صعوبة إجراءات الحصول على الدليل الرقمي

تواجه المحقق صعوبات عند قيامه بإجراءات التحقيق، فمثلاً هناك صعوبات تواجهه عند قيامه بإجراء التفتيش لضبط هذه الجريمة عندما يكون الحاسب الآلي متصلاً بحاسبات أخرى خارج الدولة و يكون تفتيش هذه الحاسبات ضرورياً ومهما لإماطة اللثام عما تشتمل عليه من جرائم[٣].

الفرع الثاني

حجية أدلة الإثبات الرقمية

---

[١] د.هبة حسين محمد زايد، مصدر سابق، ص ٢٥٠-٢٥١.

[٢] محمد طارق عبد الرؤوف الخن، مصدر سابق، ص ٣٤٥ .

[٣] د.هبة حسين محمد زايد، المصدر السابق ، ص ٢٥٢ .

كما تقدم ذكره، إنه ليس من السهل الحصول على الدليل الرقمي في إثبات جريمة الاحتيال الرقمي وكذلك ليس من السهولة تحديد مدى القوة الثبوتية التي يتمتع بها هذا الدليل ، ومدى حرية قاضي الموضوع بالاقتناع به ، و بناء الحكم على أساسه بالبراءة أو الإدانة .

وتكمن الصعوبة في ان القاضي الجنائي لا يستطيع الوصول الى نتائج حاسمة فلا يستطع ان يقف على ماهية إصابات المجنى عليه أو الأداة المستخدمة في إحداثها و كذلك مدى إمكانية اقتناع محكمة الموضوع به لتقول كلمتها فيه بالقبول أو بالرفض، فالمحكمة تقبل الدليل الذي يستمد من الآلة بشكل عام كما هو الشأن في كاميرات المراقبة في المصارف والطرق السريعة و تم ترتيب أحكام القانون في ضوء ما تستقر عنه من نتائج، وهذا ما يجعل منطق قبول الدليل المستمد من الحاسب وارداً لاتحاد كل من الدليلين في الأساس و هما الآلة والمنطق الرقمي أو التكنولوجي ككل[١].

إن الأدلة المستمدة من الأنترنيت ليست على هيئة واحدة و انما هي متنوعة و يمكن الحصول عليها سواء عن طريق فحص نظام الاتصال بالأنترنيت أو فحص مركبات الحاسب الآلي و ذلك على النحو التالي:

١-فحص نظام الاتصال بالأنترنيت

بموجب هذا النظام يتم الفحص إما بتتبع حركة مسار الأنترنيت ويقصد به الحركة التراسلية للنشاط الممارس من خلال شبكة الانترنت ، فالحاسب بمجرد أن يتعرف على المسار يقوم تلقائياً باختيار البرتوكول التراسلي الذي من خلاله يقوم باستدعاء البيانات ، و يستخدم في تتبع حركة مسار الأنترنيت نظام الفحص الرقمي الذي يطلق عليه كما تقدم ذكره (علم البصمات المعاصر) و هو منهج متبع في تتبع الحركة العكسية لمسار الأنترنيت ، و لقد تم تطبيقه بنجاح على أكثر من جريمة معلوماتية ، أيضاً من الطرق المستخدمة في فحص النظام المشار اليه فحص بروتوكول الإنترنيت وهذا بعد الطابع المتميز لاستخدام الإنترنيت فأي شخص يحصل على بروتوكول الإنترنيت يمكنه الولوج اليها ليكون عضواً كاملاً فيها يباشر الحركة خلالها ويحصل على خدماتها[٢].

---

[١] هبه محمد زايد، الحماية الجنائية للصفقات الالكترونية، دار الكتب القانونية ، القاهرة، ٢٠١٥، ص٢٨٩.

[٢] د.حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الأنترنت دراسة مقارنة، دار النهضة العربية القاهرة ٢٠٠٩، ص ٩٠٠.

إن فحص نظام الاتصال بالأنترنيت له طابع مميز ، فأي شخص يمكنه الولوج إلى الأنترنيت و يباشر الحركة خلاله و يحصل على خدماته، لذلك تعد هذه الطريقة من أهم طرق الفحص الذي نحن بصددها، فمن خلالها يمكن التعرف على جهاز الحاسب الذي تمت جريمة الاحتيال الرقمي من خلاله . فضلاً عن هذا توجد طرق أخرى تستخدم في فحص نظام الاتصال بالأنترنيت و منها فحص الخادم أو الملقم، و هو عبارة عن جهاز حاسب الي ضخم وظيفته تحقيق حركة الاتصال بالمواقع و الصفحات التي تتم استضافتها على هيئة رقمية فيه، وهناك من الخوادم ما تكون وظيفتها مقتصرة فقط على القيام بتحقيق التواصل مع حلقات النقاش و الأحاديث المباشرة أو غير المباشرة[١].

٢- فحص مركبات الحاسب الآلي

يقصد بها جميع المكونات المادية الصلبة والمعنوية أو البرامج ، لذلك يجب ضبط و حجز الجهاز لفحصه[٢].

ولكي يكون الدليل الرقمي مقبولاً أمام المحكمة يجب أن تتوافر فيه الشروط التالية :

أ- يجب ان يكون الدليل يقينياً ، أي يجب أن يكون الدليل التي يقدم الى المحكمة هو نفس الدليل الذي تم جمعه من دون أي تغيير أو تعديل أو عبث طاله من قبل أحد ، و يجب أيضاً أن يكون الدليل أقرب إلى الحقيقة وأبعد عن الظنون و التخمينات، وكل هذا يقدره القاضي بما يتفق مع اليقين و يبتعد عن الشك والتخمين، إضافة الى ذلك، يتوجب أن تتم عملية ضبط و جمع الدليل من قبل شخص مؤهل في المعلوماتية الشرعية و أن تكون إجراءات ضبطه موثقة ، و أن يكون الشخص الذي بحوزته هذا الدليل مسؤولاً عن جميع الإجراءات المتعلقة بهذا الدليل[٣].

ب-تتعين مناقشة مخرجات الوسائل الرقمية تطبيقاً لمبدأ شفوية المرافعة ، ذلك أن مخرجات الوسائل الرقمية من الأدلة تكون قائمة في أوراق الدعوى التي ينظرها القاضي، لذا تجب مناقشتها أمام الخصوم ، و هذه المخرجات سواء أكانت مطبوعة أم بيانات معروضة على

---

[١] هبه محمد زايد ،مصدر سابق، ص٢٩٠.

[٢] د.حسين بن سعيد الغافري، المصدر السابق ،ص ٥٠١.

[٣] د. غنام محمد غنام،دور قانون العقوبات في مكافحة جرائم الكومبيوترو الانترنت جرائم الاحتيال المنظم باستعمال شبكة الانترنت، دار الفكر والقانون، المنصورة،٢٠١٠، ص٢١٣.

شاشة الحاسب، أم متخذة على شكل أشرطة و أقراص ممغنطة أو ضوئية أو مصغرات فيلمية جميعها تكون محلاً للمناقشة في حالة الاعتماد عليها كأدلة أمام المحكمة [١]، ولكي يحكم القاضي بقناعته و ليس بقناعة غيره، عليه أن يعيد تحقيق كافة الأدلة القائمة في الأوراق لكي يتمكن من تكوين اقتناع بقربه من الحقيقة الواقعية التي يصبو إليها كل قاض ، و بخلاف ذلك فأن القاضي لا يمكنه أن يحكم في جريمة الاحتيال الرقمي استناداً الى علم شخص آخر الا في حالة واحدة ، وذلك إذا كان الغير هو الخبراء الذين يقدمون تقريراً مجدياً ، فيقرر الاستناد اليه ضمن باقي الأدلة القائمة في أوراق الدعوى، بحيث أن الاقتناع الذي أصدر حكمه بناء عليه يكون متولداً من عقيدته هو ، وليس من تقرير الخبير [٢].

ت- يجب أن تكون الأدلة المتحصلة من الوسائل الرقمية مشروعة، أي إن الحصول على هذه الادلة كان مشروعاً وفقاً لقواعد الأخلاق والنزاهة و احترام القانون والدستور، وبخلاف ذلك تكون الأدلة باطلة ولا يمكن الاعتماد عليها سواء بالإدانة أو بالبراءة ، لأن هذه الادلة حتى و لو كانت علمية أو فنية فأن الإثبات يحتاج الى قاض يتمتع بسلطة تقديرية لأنه من الضروري وجود هذه السلطة التقديرية و ذلك لتنقية الدليل من الغلط أو الخطأ أو الغش لكي تكون الحقيقة العلمية حقيقة قضائية[٣].

ث- في حالة وجود نقص في تقرير الادلة المتحصلة يجوز للمحكمة أن تستكمل هذا النقص بما لها من سلطة على ضوء مجموع الأدلة .

جدير بالذكر يستعد سلطة القاضي الجنائي في تقدير أدلة الاثبات من نظامين القديمين المقارنة للأنظمة الإجرائية وهما :-

١-نظام الإثبات المقيد او المحدد

في هذا النظام يكون الادلة محدد سلفا من قبل المشرع لذلك يسمى هذا النظام بنظام الأدلة القانونية بحيث ان قوتها التدليلية محصورة و لا يجوز للقاضي أن يخرج عليها او يبني حكمه على خلافها اي ان المشرع هو الذي يحدد للقاضي الادلة التي يجوز له أن يقبلها في حالة

---

[١] د. هلالي عبد اللاه أحمد ، حجية المخرجات الرقمية في المواد الجنائية، مصدر سابق، ص ١٠٤ .

[٢] د. حسين بن سعيد الغافري ، مصدر سابق، ص ٦٠٦.

[٣] هبه محمد زايد، مصدر سابق، ص٢٨٩.

معينة فيحظر عليه أن يقبل أدلة سواها، بالإضافة الى ذلك ، يحدد المشرع قيمته القانونية للدليل اذا توافرت شروط معينة عندها يلتزم القاضي الجنائي بالأخذ به و ليس له رفضه ، في هذه الحالة يكون القاضي ملزما بأن يبني اقتناعه و يؤسس حكمه على أساس هذا الدليل حتى و ان لم يكن مقتنعا شخصيا سادت هذا النوع من الانظمة قديما في أوروبا في القرون الوسطى و ما بعدها[١].

٢- نظام الأدلة الاقتناعية

يعرف بنظام حرية الاقتناع هنا لا يحدد المشرع أدلة الإثبات ووسائله قبل يتر للقاضي الحرية في أن يبنى حكمه على أي دليل وفقا لاقتناعه الشخصي دون ان يفرض عليه دليلا بعينه و الاعتراف له سلطة تقدير قيمة الدليل أو قيمة الأدلة مجتمعة ، هنا للقاضي سلطة قبول أي دليل يمكن ان يتولد معه اقتناعه ، او يستطيع حسب قناعته قبول الادلة او لا بشرط ان يكون استنتاجه لحقيقة الواقعة و ما كشف عنها من أدلة لا يخرج عن مقتضيات العقل و المنطق .

فضلاً عن هذا يوجد نظام اخر الذي يقوم على اساس الاستعانة بالأساليب الفنية التي كشف عنها العلم الحديث في إثبات الجريمة و نسبتها الى المتهم ، هنا يكون للخبير دوراً رئيساً و يجعل اهم الادلة هي القرائن التي تخضع للفحص العلمي الدقيق و يستخرج منها ما يثبت الإدانة أو البراءة استخدم هذا النظام عند اصحاب المدرسة الوضعية[٢].

نستنتج من ما سبق أن وجود الخبير بمكان القاضي له مساس بحقوق المتهم ، فانه يحرم من ضمانات الحرية الفردية وحقوقه الانسان التي لا يحسن أن يقررها سوى القاضي الجنائي بالإضافة أن مباشرة الخبير عمله تقترض تحديد عناصر مهمته و تقدير قيمة تقديره و هما وظيفتان قضائيتان، من جانب اخر فان الفصل في الدعوى الجنائية يثر مسائل قانونية و شرعية لا يحس الخبير التعامل معها و البت فيها .

ونستنتج من خلال ما تقدم، إن القاضي يستمد قناعته من أي دليل ما لم ينص القانون على غير ذلك ، سلطته غير ملزمة برأي الخبير استناداً الى مبدأ الاقتناع القضائي و من ثم يكون

---

[١] سعيد عبد اللطيف حسن ، إثبات جرائم الكومبيوتر و الجرائم المرتكبة عبر الإنترنت ،ط١ ،دار النهضة العربية ، القاهرة ، ١٩٩٩ ،ص ١٤٦.

[٢] سعيد عبد اللطيف حسن ، المصدر نفسه ، ص ١٤٦

للقاضي السلطة في تقديره إذ هو شأنه شأن سائر الادلة لقاضي الموضوع كامل الحرية فله أن يأخذ من الأدلة ما يشاء حسب قناعته الشخصية و منها الدليل الرقمي؛ لأنه يندرج تحت قائمة الأدلة الثبوتية فأنه ينطبق عليه ذلك ، أي إن القاضي له السلطة التامة و الحرية الكاملة في أن يأخذ به سواء في إطار البراءة أم الإدانة وفقاً للشروط التي سبق و أن أشرنا اليها.

الخاتمة

توصلنا من خلال بحثنا في "التنظيم القانوني لجريمة الاحتيال الرقمي" الى عدد من النتائج والمقترحات تدرج أبرزها على الوجه الآتي:

أولاً: النتائج

١- جريمة الاحتيال استيلاء عن طريق الشبكة المعلوماتية أو جهاز الحاسوب أو ما في حكمها على مال او معلومات او برامج على سند يتضمن تعهداً او اي امتياز مالي آخر و ذلك عن طريق خداع المجنى عليه او خداع الحاسوب او الآلة الخاضعة لسيطرة المجنى عليه و الحاق الضرر به .

٢- تتميز جريمة الاحتيال الرقمي عن الجرائم الأخرى بعدة خصائص تساعد في التعرف على طبيعتها و أهميتها، فهي جريمة متعدية الحدود وصعبة الاكتشاف و الاشخاص الذين يرتكبون هذه الجريمة من الاشخاص الذين يتمتعون بالذكاء والفطنة و معرفة تقنيات الحاسوب والانترنيت و القدرة على التمثيل و لا يميلون الى العنف المادي .

٣- يستخدم الجاني أدوات علمية دقيقة لتحقيق مشروعه إجرامي بغية التلاعب في البيانات ، و أغلب هذه البيانات تتعلق بالابداعات المصرفية أو قد يكون نتائج الميزانيات و المستحقات المالية في المرتبات والمعاشات ، و أوامر الدفع وغيرها .

ثانياً: المقترحات

١- نقترح تحديث وتوسيع القوانين ومنها قانون العقوبات العراقي ليشمل جرائم الاحتيال الرقمي بشكل صريح.

٢-نقترح على الجهات الرسمية توعية الافراد بوسائل الاحتيال الرقمي واساليب المحتالين في الخداع واثارة الاطماع لايقاع الضحايا.

٣- اصدار قوانين تتعلق بالتجارة الالكترونية حماية المعلومات الشخصية على شبكة الانترنت.

المصادر

اولا: الكتب

١- احمد شوقي عمرابوخطوة ، شرح قانون العقوبات القسم الخاص ، جرائم الاعتداء على الاموال ، دار النهضة العربية ، القاهرة ،١٩٩٤.

٢- اياد حسين عباس العزاوي، جريمة الاحتيال في القانون العراقي، ط١، بدون دار نشر، بغداد، ١٩٨٨.

٣- حسن صادق المرصفاوي ، قانون العقوبات الخاص ، منشأة المعارف ، الاسكندرية ،١٩٧٥.

٤- حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الأنترنت دراسة مقارنة، دار النهضة العربية القاهرة ٢٠٠٩.

٥- حميد السعدي ، جرائم الاعتداء على الاموال ، مطبعة المعارف ، بغداد ،١٩٦٧.

٦- سعيد عبد اللطيف حسن ، إثبات جرائم الكومبيوتر و الجرائم المرتكبة عبر الإنترنت ،ط١ ،دار النهضة العربية ، القاهرة ، ٢٠١٥.

٧- عبد الله سيف الكيتوب ، الاحكام الاجرائية لجريمة الاحتيال المعلوماتي، دار النهضة العربية، القاهرة، ٢٠١٣.

٨- عمر محمد أبو بكر بن يونس، الاجراءات الجنائية عبر الانترنت في القانون الامريكي، القاهرة، ٢٠٠٥.

٩- عمر محمد أبو بكر بن يونس، الاجراءات الجنائية عبر الانترنت في القانون الامريكي، القاهرة، ٢٠٠٥.

١٠- غنام محمد غنام،دور قانون العقوبات في مكافحة جرائم الكومبيوترو الانترنت جرائم الاحتيال المنظم باستعمال شبكة الانترنت، دار الفكر والقانون، المنصورة،٢٠١٠.

١١- محمد الشناوي، جرائم النصب المستحدثة ، دارالكتب القانونية ، المحلة الكبرى ، مصر،٢٠٠٨.

١٢- محمد طارق عبد الرؤوف الخن ، جريمة الاحتيال عبر الانترنت، منشورات الحلبي الحقوقية ، بيروت،٢٠١١.

١٣- محمد طارق عبدالرؤوف الخن ، جريمة الاحتيال عبر الانترنت، منشورات الحلبي الحقوقية، بيروت ، ٢٠١١.

١٤- محمد عبدالله أبوبكرسلامه ، موسوعة الجرائم المعلوماتية: جرائم الكومبيوتر والانترنت، المكتب العربي الحديث، الاسكندرية، ٢٠١١.

١٥- محمود احمد عبابنة ، جرائم الحاسوب وابعادها الدولية ، دارالثقافة للنشر والتوزيع ، عمان، الاردن ، ٢٠٠٥.

١٦- محمود محمد محمود جابر ، الاحكام الاجرائية للجرائم الناشئة عن استخدام الهواتف النقالة جرائم نظم الاتصالات المعلومات ، المكتب الجامعي الحديث ، الاسكندرية، ٢٠١٧.

١٧- مصطفى محمد موسى ، التحقيق الجنائي في الجرائم الرقمية ، مطابع الشرطة القاهرة ٢٠٠٩.

١٨- ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الحاسب الآلي و الأنترنت، دار الكتب القانونية، القاهرة ، ٢٠٠٦.

١٩- نائلة عادل محمد فريد ، جرام الحاسوب الالي الاقتصادي، ط١، منشورات الحلبي الحقوقية، بيروت، ٢٠٠٥.

٢٠- نهلا عبدالقادر المومني ، الجرائم المعلوماتية ،ط١، دار الثقافة ، عمان، ٢٠٠٨.

٢١- هبة حسين محمد زايد ، الحماية الجنائية للصفقات الالكترونية، دار الكتب القانونية، القاهرة، ٢٠١٥.

٢٢- هبه محمد زايد، الحماية الجنائية للصفقات الالكترونية، دار الكتب القانونية ، القاهرة، ٢٠١٥.

٢٣- هلالي عبد اللاه أحمد ، حجية المخرجات الكومبيوترية في المواد الجنائية ، النشر الذهبي للطباعة ، القاهرة ، ٢٠٠٢.

٢٤- ياسر محمد الكومي ، الحماية الجنائية والامنية للتوقيع الالكتروني، منشأة المعارف، الاسكندرية، ٢٠١٤.

ثانيا: الرسائل والاطاريح

١- فاديه يحي ابوشهنبه،النظرية العامة للطرق الاحتيالية في القانون المصري المقارن، رسالة دكتوراه كلية الحقوق جامعة عين شمس،١٩٨٤.

٢- محمد هشام صالح عبدالفتاح ، جريمة الاحتيال ، دراسة مقارنة ،رسالة ماجستير مقدمة الى كلية الدراسات العليا، جامعة النجاح الوطنية في نابلس ، فلسطين، ٢٠٠٨.

ثالثا: البحوث المنشورة

١- محمد محي الدين عوض ، مشكلات السياسة الجنائية الجنائية المعاصرة في جرائم نظم المعلومات (الكومبيوتر)، ورقة عمل مقدمة الى المؤتمر السادس للجمعية المصرية للقانون الجنائي، دار النهضة العربية، القاهرة.

رابعا: القوانين

١- قانون العقوبات العراقي لسنة ١٩٦٩المعدل النافذ .

٢- قانون العقوبات الالماني وله تعديلات كثيرة اخرها سنة ١٩٩٤.

٣- قانون العقوبات اليوناني لسنة ١٩٥٠.

خامسا: المصادر الاجنبية

1-Micheal Kunzand& Patrick Wilson:computer crime and computer fraudf p12.،2004،USA،Maryland

References

First: Books

1- Ahmed Shawqi Omar Abu Khatwa, Explanation of the Penal Code, Special Section, Crimes of Assault on Property, Dar Al Nahda Al Arabiya, Cairo, 1994.

2- Ayad Hussein Abbas Al Azzawi, The Crime of Fraud in Iraqi Law, 1st ed., no publisher, Baghdad, 1988.

3- Hassan Sadiq Al Marsafawi, Special Penal Code, Mansha'at Al Maaref, Alexandria, 1975.

4- Hussein bin Saeed Al Ghafri, Criminal Policy in Confronting Internet Crimes: A Comparative Study, Dar Al Nahda Al Arabiya, Cairo, 2009.

5- Hamid Al Saadi, Crimes of Assault on Property, Al Maaref Press, Baghdad, 1967.

6- Saeed Abdel Latif Hassan, Proving Computer Crimes and Crimes Committed via the Internet, 1st ed., Dar Al Nahda Al Arabiya, Cairo, 2015.

7- Abdullah Saif Al-Kaitoub, Procedural Provisions for the Crime of Information Fraud, Dar Al Nahda Al Arabiya, Cairo, 2013.

8- Omar Muhammad Abu Bakr Bin Younis, Criminal Procedures via the Internet in American Law, Cairo, 2005.

9- Omar Muhammad Abu Bakr Bin Younis, Criminal Procedures via the Internet in American Law, Cairo, 2005.

10- Ghanem Muhammad Ghanem, The Role of the Penal Code in Combating Computer and Internet Crimes: Organized Fraud Crimes Using the Internet, Dar Al Fikr Wal Qanun, Mansoura, 2010.

11- Muhammad Al-Shinawi, New Fraud Crimes, Dar Al-Kotob Al-Qanuniyah, Al-Mahalla Al-Kubra, Egypt, 2008.

12- Muhammad Tariq Abdul-Raouf Al-Khan, The Crime of Internet Fraud, Al-Halabi Legal Publications, Beirut, 2011.

13- Muhammad Tariq Abdul Raouf Al-Khan, The Crime of Internet Fraud, Al-Halabi Legal Publications, Beirut, 2011.

14- Muhammad Abdullah Abu Bakr Salama, Encyclopedia of Cybercrimes: Computer and Internet Crimes, Modern Arab Office, Alexandria, 2011.

15- Mahmoud Ahmad Ababneh, Computer Crimes and Their International Dimensions, Dar Al-Thaqafa for Publishing and Distribution, Amman, Jordan, 2005.

16- Mahmoud Muhammad Mahmoud Jaber, Procedural Provisions for Crimes Arising from the Use of Mobile Phones: Information Communication Systems Crimes, Modern University Office, Alexandria, 2017.

17- Mustafa Muhammad Musa, Criminal Investigation in Digital Crimes, Police Press, Cairo, 2009.

18- Mamdouh Abdul Hamid Abdul Muttalib, Digital Criminal Investigation and Research in Computer and Internet Crimes, Dar Al-Kotob Al-Qanuniyah, Cairo, 2006.

19- Naila Adel Mohamed Farid, Economic Computer Grammar, 1st ed., Al-Halabi Legal Publications, Beirut, 2005.

20- Nahla Abdel Qader Al-Momani, Cybercrimes, 1st ed., Dar Al-Thaqafa, Amman, 2008.

21- Heba Hussein Mohamed Zayed, Criminal Protection of Electronic Transactions, Dar Al-Kotob Al-Qanuniya, Cairo, 2015.

22- Heba Mohamed Zayed, Criminal Protection of Electronic Transactions, Dar Al-Kotob Al-Qanuniya, Cairo, 2015.

23- Hilali Abdel-Allah Ahmed, The Validity of Computer Outputs in Criminal Matters, Golden Publishing for Printing, Cairo, 2002.

24- Yasser Mohamed Al-Komi, Criminal and Security Protection of Electronic Signatures, Maaref Establishment, Alexandria, 2014.

Second: Theses and Dissertations

1- Fadia Yahya Abu Shehanbeh, The General Theory of Fraudulent Methods in Comparative Egyptian Law, PhD dissertation, Faculty of Law, Ain Shams University, 1984.

2- Muhammad Hisham Saleh Abdel Fattah, The Crime of Fraud: A Comparative Study, Master's thesis submitted to the Faculty of Graduate Studies, An-Najah National University in Nablus, Palestine, 2008.

Third: Research Papers

1- Mohamed Mohi El-Din Awad, Problems of Contemporary Criminal Policy in Information Systems (Computer) Crimes, a working paper presented to the Sixth Conference of the Egyptian Society of Criminal Law, Dar Al-Nahda Al-Arabiya, Cairo.

Fourth:Laws

1- The Iraqi Penal Code of 1969, as amended and in effect.

2- The German Penal Code, with numerous amendments, the last of which was in 1994.

3- The Greek Penal Code of 1950.

Fifth: Foreign Sources

1-Micheal Kunzand& Patrick Wilson:computer crime and computer fraudf Maryland،USA،2004،p12.