جامعة دمشق
كلية الحقوق

# جريمة الاحتيال عبر الإنترنت

## (الأحكام موضوعية والأحكام إجرائية )

رسالة لنيل درجة الدكتوراه

مقدمة من
القاضي محمد طارق بن عبد الرؤوف الخن

المشرف
أ.د.بارعة القدسي

المشرف المشارك
د.عماد الصابوني

عام 1430 هـ
2010 م

**بسم الله الرحمن الرحيم**

**﴿ قالوا سبحانك لا علم لنا إلاّ ما علّمتنا إنك أنت العليم الحكيم﴾**

**صدق الله العظيم**

**(سورة البقرة– آية 32)**

**نُوقشت هذه الأطروحة بتاريخ 2010/2/1 في جامعة دمشق ونالت درجة جيد جداً، مع التوصية بطباعتها على نفقة الجامعة وتبادلها مع الجامعات الأخرى.**

## إهــداء

**بخالص العرفان أهدي هذه الرسالة إلى روح والدي وإلى روح شقيقتي.....**

**وإلى والدتي وإخوتي وأخواتي وزوجتي وجميع أفراد عائلتي الذين قدموا لي الدعم خلال سنوات العمل الطويل، كما أهديها إلى كل من ساهم معي في وضع لَبِنَات هذه الرسالة.**

# كلمة شـــكر

**يشرفني أن أتقدم بأسمى آيات الشكر والعرفان إلى:**

**الأستاذة الدكتورة بارعة القدسي.**

التي تفضّلت وأشرفت على هذه الرسالة، فأعطتني الكثير من وقتها الثمين وجهدها الكبير، ولم تبخل بالاطلاع على تفاصيل الرسالة، وتوجيهها في الطريق القانوني السليم، فكانت لي معلماً ومشرفاً، ولها مني كل الحب والتقدير وأسمى آيات المودة والاحترام.

**والامتنان كل الامتنان إلى:**

**السيد وزير الاتصالات والتقانة الدكتور عماد الصابوني.**

الذي تفضل مشكوراً بالإشراف على الجانب التقني لهذه الرسالة– بوصفه أحد رموز الجمعية العلمية السورية المعلوماتية– والذي استفدت من خبرته الطويلة، فأغنى رسالتي بآرائه وتوجيهاته، وكان لي خير مرشد ومعين. فكل الشكر له على ما بذله من جهد كبير لإنجاز هذا العمل.

# مقدمة

تعد شبكة الإنترنت أكثرَ التقنياتِ أهميةً في عصرٍ يسمى بعصر المعلومات، وهي وليدة التزاوج بين نظم الحوسبة ونظم الاتصالات. فقد أحدثت هذه الشبكة قفزةً نوعيةً في نشر المعلومات بين الأفراد في كافة أرجاء العالم، حتى اندمج العالم بأسره، فبدا وكأنه أسرةٌ واحدةٌ، بعد أن تحرر من قيود المكان والزمان.

ولقد أدى التطور المتسارع لشبكة الإنترنت، إلى إحداث تحولات في مختلف جوانب الحياة، بحيث يمكن مقارنتها بالتحولات التي أحدثتها الثورة الصناعية أو ما أحدثه اكتشاف الكهرباء والهاتف والتلفاز....الخ.

وأسوة بهذه الثورات، وبقدر ما كان لشبكة الإنترنت من إيجابيات في مجال الاتصالات وتبادل المعلومات، راحت تظهر سلبيات هذا العالم الافتراضي في مجال الإجرام. حتى احترف البعض ارتكاب شتى أنواع الجرائم التقليدية والمستحدثة عبر هذه الشبكة. ونتيجة لذلك دفعت أكثر المجتمعات ضريبة باهظة لقاء هذه التكنولوجيا المتطورة، التي قدمت للمجرمين اختصاراً لمفهومي الزمان والمكان.

كما صاحب الانتشار الواسع لاستخدام الإنترنت وتزايد حجم التعامل عبرها، نموٌ مضطردٌ في الجرائم المرافقة لهذا الاستخدام، خاصة أن الإنترنت تعتبر سوقاً رائجة في مجال التبادل التجاري، وهذا ما فسح المجال أمام ظهور جريمة الاحتيال المرتكبة عبر الإنترنت.

ولما كان النظام القانوني يتصف بأنه يعكس احتياجات المجتمع ورغباته، ويتصدى لجميع الظواهر الإجرامية، فقد أدركت الدول المتقدمة خطورة هذه

الجرائم، فسنّت التشريعات الجزائية التي تهدف إلى الحد من مخاطرها والردع لمرتكبيها. كما حاولت الدول العربية استيعاب هذه الظاهرة الإجرامية، وذلك بحسب قدراتها وظروفها ومصالحها ومعارفها. فبعضها سارع لمواجهة هذا التحدي بسن تشريعات على استحياء، وبعضها الآخر فسح المجال أمام اجتهاد الباحثين لتأصيل ما أفرزته ثورة المعلومات من ظواهر إجرامية، ريثما تأزف ساعة التصدي التشريعي لها.

## أولاً: موضوع البحث وأهميته:

يعد موضوع الاحتيال عبر الإنترنت من الموضوعات الجديدة والمهمة جداً في إطار القسم الخاص من قانون العقوبات. فلا يخفى على أحدٍ ما لهذه الجريمة من أثار سلبية على المستوى الاقتصادي للفرد والمجتمع بشكل عام.

وموضوع الاحتيال عبر الإنترنت من الموضوعات التي لا تزال بكراً، والتي لم تنل حظها من البحث والتمحيص على مستوى الفقه الجزائي، إذ إن معظم جوانب هذه الجريمة لا تزال غامضة، تحتاج إلى من يسبر أغوارها، خاصةً في ظل غياب النص التشريعي الذي يكافح هذا النوع من الإجرام المستحدث في بعض الدول مثل سورية، فأغلب الدراسات المنشورة في مجال جرائم الإنترنت، اقتصرت على البحث في عموم هذه الجرائم دون الغوص في أعماقها، فلم تتناول مختلف الجوانب المتعلقة بكل جريمة على حدة، لمعرفة ما يعتريها من غموض وأبعاد، كما اكتفت معظم هذه الأبحاث بدراسة الجانب النظري فقط لهذه الجرائم المستحدثة.

ومن هنا تأتي أهمية موضوع هذا البحث، الذي يمكن الاستفادة منه على أرض الواقع، حيث يتناول التصورات والرؤى المتعلقة بالجوانب الموضوعية والجوانب الإجرائية للاحتيال عبر الإنترنت، في محاولةٍ لتقديم الحلول القانونية

الممكنة لمكافحة هذه الجريمة في ظل النصوص التشريعية الحالية في سورية. فالدراسة التي ليس لها صلة بالواقع تكون دراسة جافة وجامدة ولا فائدة منها.

## ثانياً: مشكلة البحث:

إن البحث في جريمة الاحتيال عبر الإنترنت – التي يصفها الفقهاء بأنها جريمة الأموال الأولى المرتكبة عبر هذه الشبكة من حيث الحجم– يثير الكثير من الجدل الفقهي نظراً لحداثة هذه الجريمة خاصةً في سورية، ذلك لأنه لا يوجد في بلدنا حتى تاريخ إعداد هذه الأطروحة، تشريعٌ جزائيٌ معلوماتيٌ يضع الحلول المناسبة للجرائم الناشئة عن استخدام الإنترنت، وعلى رأسها جريمة الاحتيال، في الوقت الذي بدأت تعرض على قضائنا السوري العديد من القضايا المتعلقة بهذا الموضوع[1]، وعليه فإن إشكالية البحث يمكن صياغُتها على النحو التالي:

**كيف سيفصل القضاء في سورية في قضايا الاحتيال عبر الإنترنت التي وصلت إلى دواوين المحاكم في ظل غياب النص التشريعي دون أن يتعارض ذلك مع مبدأ شرعية الجرائم والعقوبات؟ وإلى أي مدى يمكن تطبيق النصوص التقليدية لجريمة الاحتيال على مختلف صور الاحتيال عبر الإنترنت؟ وهل النصوص الإجرائية التقليدية تسمح بالكشف عن هذه الجريمة وإثباتها؟**

إضافةً إلى ذلك، فإذا كانت سجلات المحاكم في الوقت الحاضر تشير إلى وجود عدد قليل من قضايا الاحتيال عبر الإنترنت في سورية، فإن هذه السجلات لا يمكن أن تعطي الصورة الحقيقية لحجم هذه الجريمة، لأن هناك العديد من القضايا المتعلقة بهذه الجريمة لم يصل نبأ وقوعها إلى مسامع النيابة

---

[1] سنشير خلال هذه الدراسة إلى بعض قضايا الاحتيال عبر الإنترنت التي وصلت إلى سجلات النيابة العامة في السورية, والتي أُرسِلت إلى محاكم الأساس. إلا أن محكمة النقض لم تقل كلمتها الأخيرة فيها, لأنها لم تصل بعد إلى ديوانها.

العامة لأسباب مختلفة، كالإحجام عن التبليغ عنها حفاظاً على سمعة المجني عليه، أو لأن الجريمة ترتبط بدولة أخرى تم تقديم الشكوى فيها..الخ. والتساؤل المطروح هنا:

**كيف سيتعامل القضاء في سورية مع الاحتيال عبر الإنترنت إذا وصلت هذه المشكلة إلى مستوى الظاهرة الجرمية؟**

ولما كانت إشكالية البحث تلعب دوراً رئيسياً في اختيار المنهج الذي سيتبعه الباحث، فإن هذه الدراسة ليست مجرد شرحٍ لنصوص قانونية، ولا عرضٍ لبعض النظريات الفقهية، إنما هي دراسة **تحليلية تأصيلية**، حاول الباحث فيها معرفة مدى انسجام الاحتيال عبر الإنترنت مع مفهومه التقليدي، وذلك من خلال دراسة الأحكام الموضوعية لهذه الجريمة. كما أن هذه الدراسة لم تقنع ببحث الجانب الموضوعي فقط، بل تجاوزت ذلك إلى الأحكام الإجرائية، في محاولة للبحث عن الحلول الأكثر واقعية من الناحية العملية لجريمة الاحتيال عبر الإنترنت.

وقد اقتضى منا هذا البحث عدم الاكتفاء بدراسة الجانب النظري، بل امتد إلى طرح الأمثلة الواقعية والعملية، مع تسليط الضوء على بعض التشريعات الأجنبية والعربية والاتفاقيات الدولية في هذا المضمار، لاستخلاص النتائج العلمية والعملية، التي يمكن الاستفادة منها في نظامنا القانوني.

## ثالثاً: صعوبات البحث:

يواجه البحث في الاحتيال عبر الإنترنت العديد من الصعوبات، التي يمكن تلخيصها بالنقاط التالية:

1) عدم وجود مراجع قانونية متخصصة في الفقه السوري، وقلة المراجع العربية التي تبحث في هذا الموضوع.

2) عدم وجود تشريع جزائي في سورية يعاقب على الجرائم الناشئة عن استخدام الإنترنت.

3) صعوبة الحصول على المراجع الأجنبية، إذ إننا كثيراً ما كنا نجلس لساعات طويلة وراء الإنترنت للبحث عن المراجع الأجنبية، وبعد الوصول للعناوين المطلوبة، كنا نصطدم عند طلبها بعدم إمكانية إرسالها إلى سورية بسبب المقاطعة الأمريكية، لأن غالبية هذه الكتب تعود إلى دور نشر أمريكية، أو دور نشر مرتبطة بها. وقد تجاوزنا هذه الصعوبة من خلال طلب هذه الكتب عن طريق الدول العربية المجاورة، وعن طريق شراء الكتب الإلكترونية عبر الإنترنت.

4) عدم كفاية التخصص القانوني في مثل هذه الأبحاث، إذ يجب على الباحث أن يكون ملمّاً بالجوانب التقنية للحاسوب وشبكة الإنترنت، حتى يتيسر له الفهم الجيد لمختلف جوانب البحث؛ فهذه الشبكة متجددة باستمرار، وهي لا تعرف التوقف عن النمو، كما تحتوي على كمٍ هائلٍ من الرموز والمصطلحات التقنية، التي تحتاج إلى شخص متخصص في هذا المجال لتحديد المقصود بها. وقد حاولت تجاوز هذه العقبة بمساعدة وفضل من الله سبحانه وتعالى، إذ منّ الله عليّ بأن سبق لي التخرج من معهد الإلكترون التابع لوزارة التعليم العالي قبل دراسة الحقوق، كما أتاحت لي الفرصة شرف مشاركة الدكتور عماد الصابوني وزير الاتصالات والتقانة بالإشراف على هذا البحث لجهة الجانب التقني.

## رابعاً: إعلان خطة البحث:

تتناول هذه الرسالة دراسة الاحتيال عبر الإنترنت من خلال بابين رئيسين هما: الرؤية الموضوعية والرؤية الإجرائية لهذه الجريمة، بحيث يسبق هذين البابين فصل تمهيدي خصص لفهم ماهية الإنترنت، والتعريف بجرائم الإنترنت عموماً و الاحتيال خصوصاً.

وتتضمن الرؤية الموضوعية، عرض لأبرز أساليب الاحتيال عبر هذه التقنية من خلال القضايا الواقعية، مع إلقاء الضوء على الاتجاهات التشريعية في الدول الأجنبية والعربية، والاتفاقيات الدولية المتعلقة بجرائم الإنترنت. ومن ثم دراسة مدى انسجام الاحتيال عبر الإنترنت مع مفهومه التقليدي.

أما الرؤية الإجرائية، فتتضمن القواعد المتعلقة بالاختصاص الجزائي الدولي، والتحقيق في جريمة الاحتيال عبر الإنترنت، ومدى فعالية أدلة الإثبات التقليدية في إثبات هذه الجريمة، ثم الوقوف على ماهية الدليل الرقمي وخصائصه وحجيته.

وأخيراً تنتهي هذه الدراسة بخاتمة تتضمن نتائج ومقترحات موضوعية وإجرائية، نرجو أن تلقى قبولاً لدى المشرع السوري عند وضع تشريعٍ يعاقب على جرائم الإنترنت في بلادنا.

## فصل تمهيدي

## طبيعة شبكة الإنترنت والجرائم المرافقة لاستخدامها

إن معرفة ماهية شبكة الإنترنت، والفهم الجيد لآلية عمل هذه الشبكة، ثم التعرف على جرائم الإنترنت الناشئة عن الاستخدام السيئ لها، مسألة ضرورية للوقوف على مختلف جوانب الاحتيال عبر الإنترنت. وبناءً على ذلك سوف نقسم هذا الفصل التمهيدي إلى المبحثين التاليين:

**المبحث الأول:** ماهية الإنترنت.

**المبحث الثاني:** القانون الجزائي والإنترنت.

# المبحث الأول

# ماهية الإنترنت

يتطلب التعرف على ماهية شبكة الإنترنت ، إلقاء الضوء على المراحل التي مرت بها هذه الشبكة منذ نشأتها، ثم معرفة آلية تنظيمها وكيفية عملها. لذلك سنتناول هذا المبحث من خلال المطلبين التاليين:

المطلب الأول: التعريف بالإنترنت.

المطلب الثاني: تنظيم الإنترنت.

# المطلب الأول
# التعريف بالإنترنت

إن الحديث عن الإنترنت يدفعنا للعودة إلى جذور هذه الشبكة منذ الستينيات؛ للتعرف على الأب الشرعي لها، ومتابعة مراحل نموها منذ الولادة، ثم استعراض التعريفات الفقهية التي تناولت شبكة الإنترنت، والتي تضمنت سمات هذه الشبكة. وهذا ما سنلقي الضوء عليه في هذا المطلب.

## أولاً– نشأة الإنترنت[1]:

نشأت فكرة الإنترنت نتيجة الحرب الباردة بين الولايات المتحدة الأميركية والاتحاد السوفييتي في الستينيات، حيث كان المسؤولون في وزارة الدفاع الأميركية يبحثون عن إجابة لسؤال كان يتبادر إلى أذهانهم، **وهو كيف يمكن للمسؤولين في الولايات المتحدة الأميركية الاتصال فيما بينهم، في حال حدوث كوارث أو في حال حدوث هجوم نووي؟**

---

(1) د.عبد الحسن الحسيني: القاموس الموسوعي في المعلومات والاتصالات والمعلوماتية القانونية، الطبعة الأولى، مكتبة صادر، بيروت، عام 2004، ص79–80.

- د.طوني ميشال عيسى: التنظيم القانوني لشبكة الإنترنت، الطبعة الأولى، منشورات صادر الحقوقية، بيروت، عام 2001، ص40 .
- القاضي الدكتور إيهاب السنباطي: موسوعة الإطار القانوني للتجارة الإلكترونية، دار النهضة العربية، القاهرة، عام 2007، ص81.
- د.سليمان أحمد فضل: المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، دار النهضة العربية، القاهرة، عام 2007، ص4 .
- د. عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت، الطبعة الأولى، دار النهضة العربية، القاهرة، عام 2004، ص25.

على إثر ذلك، عهدت وزارة الدفاع الأميركية في عام 1964 إلى وكالة مشاريع الأبحاث المتطورة (ARPA) [1] بمهمة إنشاء شبكة من الحواسيب تكون قادرة على الاستمرار في العمل في حال حدوث مثل هذه الكوارث.

في عام 1969، قامت وكالة مشاريع الأبحاث المتقدمة، بإنشاء شبكة متخصصة لهذا الغرض حملت اسم أربانت (ARPANET)، وكانت هذه الشبكة التجريبية في البداية تربط أربعة حواسيب آلية ضخمة فيما بينها.

في عام 1972، تمّ إيصال الأربانت إلى معظم الجامعات الأميركية، وفي عام 1973 بدأت الاتصالات الدولية بهذه الشبكة من إنكلترا والنروج. وهنا بدت الحاجة ملحة لإيجاد وسيلة تخاطب تسمح للحواسيب التي تعمل بلغات مختلفة بأن تتصل فيما بينها، فتمّ في هذا العام اكتشاف بروتوكول الإنترنت (TCP/IP)[2].

في عام 1986، تمّ نقل تشغيل أربانت من وزارة الدفاع إلى شبكة مؤسسة العلوم الوطنية NSFNET إضافةً إلى إدارة الطيران المدني والفضاء الأميركية، وكذلك إلى إدارة الطاقة، وبذلك أصبحت أربانت متاحة لجميع أشكال البحث العلمي.

---

(1) وهو اختصار Advanced Research Projects Agency وهو مركز أبحاث عسكرية وعلمية تابع لوزارة الدفاع الأميركية.

(2) وهو بروتوكول تقني حول الاتصالات، يتضمن بروتوكولين مستقلين هما:
بروتوكول التحكم في النقل Transfer Control Protocol
وبروتوكول الإنترنت Internet Protocol
د.عبد الحسن الحسيني: المرجع السابق, ص792.

في عام 1990، ومع انهيار الإتحاد السوفيتي وانتهاء الحرب الباردة، لم تعد تجد وزارة الدفاع الأمريكية أن هناك فائدة في حصر استعمال هذه الشبكة في الأمور العسكرية فقط، فأطلقت حرية استخدامها، وبدأ نطاق استعمالها يتسع، وأصبح لها إدارة خاصة لا ربحية، ثم تحولت أربانت إلى الإنترنت Internet كتسمية جديدة.

وفي عام 1991، تمكن مهندس الاتصالات السويسري "تيم بيرنرز لي" من اختراع تقنية الوبّ[1] world wide web (w.w.w) التي تساعد على تصفح المعلومات واستعراضها بسهولة على شبكة الإنترنت.

## ثانياً- تعريف الإنترنت:

تعددت المحاولات الفقهية لتعريف الإنترنت، ومن هذه التعاريف:

أن الإنترنت هي "عبارة عن آلية اتصال مكونة من مفاتيح وأسلاك وأماكن تخزين للبيانات، و دواعم توصيل، و روابط اتصال، تعمل في بوتقة واحدة بفضل بروتوكول الإنترنت (TCP/IP)"[2].

وفي تعريف آخر "بأنها شبكة الشبكات، حيث تتكون من عدد كبير من شبكات الحاسوب المترابطة والمتناثرة في أنحاء العالم، ويحكم ترابط تلك الأجهزة وتحادثها بروتوكول موحد يسمى بروتوكول تراسل الإنترنت"[3].

وهي أيضاً من وجهة نظر تقنية إنسانية، "بأنها تلك الوسيلة أو الأداة التواصلية بين شبكات المعلومات، دون اعتبار للحدود الدولية"[4].

---

(1) الوبّ web. هو نسيج العنكبوت .وقد سميت به هذه التقنية من باب المجاز. والوبّ هو الاسم المعرب لهذه التقنية. د.عبد الحسن الحسيني: المرجع السابق, ص860.

(2) القاضي الدكتور إيهاب السنباطي، المرجع السابق، ص78.

(3) د.عبد الفتاح مراد: شرح جرائم الكومبيوتر والإنترنت، بلا دار نشر، بلا عام, ص26.

(4) د.عمر بن يونس: المرجع السابق، ص38.

والحقيقة إن جميع هذه التعاريف تعبر عن حقيقة الإنترنت، التي يمكن تعريفها ببساطة بأنها "**شبكة تتألف من عدد كبير من الحواسيب المتوضعة عبر العالم، والمترابطة مع بعضها البعض، والتي تستخدم في تواصلها بروتوكول تراسل الإنترنت**".

## ثالثاً– شبكة الإنترنت و الوبّ (w.w.w ):

يظن الكثير من الناس بأن الإنترنت والوبّ w.w.w شيء واحد، غير أن ذلك ليس صحيحاً، لأن الإنترنت كما بيّنا هي عبارة عن شبكة تربط جميع شبكات الحاسوب المتصلة مع بعضها البعض. أما الوبّ w.w.w ، فهو أحد تطبيقاتها فقط ، أو إحدى الآليات التي تستعمل في الاتصال.

فالإنترنت تحتوي على عدة تطبيقات و وسائل للتواصل، مثل البريد الإلكتروني e-mail والماسنجر messenger والتي تستعمل في أفق الإنترنت، ولكنها ليست هي والإنترنت شيئاً واحداً. فالإنترنت تشبه الطريق التي تكون بين المدن، في حين أن تلك التطبيقات المذكورة وعلى رأسها الوبّ ، هي أنواع وسائل المواصلات التي تستخدم هذه البنية الأساسية، مثل السيارات أو الحافلات أو الدراجات النارية[1].

وقد سبق وأشرنا بأن مهندس الاتصالات الإنكليزي "تيم بيرنز لي" هو من اخترع نظام الوبّ www، حيث يرتكز هذا النظام على بروتوكول(HTTP)[2] أي بروتوكول نقل النصوص الترابطية، الذي يسمح بربط مواقع الوبّ الموصولة بالشبكة فيما بينها والتجول فيها، وهو لا يعمل إلاّ بواسطة برامج تصفح خاصة[3].

---

(1) القاضي الدكتور إيهاب السنباطي: المرجع السابق، ص80.

(2) وهو اختصار لـ Hypertext Transfer Protocol. د.عبد الحسن الحسيني:المرجع السابق,ص408.

(3) د.طوني عيسى: المرجع السابق، ص60.

# المطلب الثاني

# تنظيم الإنترنت

يتطلب التعرف على تنظيم الإنترنت، معرفة آلية عمل بروتوكول تراسل الإنترنت، ثم التعرف على الجهات التي تشرف على شبكة الإنترنت ودور هذه الجهات، خاصة الجهات المانحة للعناوين على الإنترنت، وهذا ما سنبحثه على التتالي:

## أولاً– بروتوكول تراسل الإنترنت (TCP/IP)[1]:

تعتمد آلية عمل شبكة الإنترنت، على وسيلة التخاطب الرقمي، وذلك بواسطة بروتوكولين رئيسيين هما:

- بروتوكول التحكم في النقلTCP.
- برتوكول الإنترنت IP. ويسميان في التطبيق، بروتوكول تراسل الإنترنت TCP/IP.

حيث يقوم بروتوكول التحكم في النقل TCP بتجزئة الرسالة المراد إرسالها إلى رزم من المعلومات، بحيث تحمل هذه الرزم معلومات تعريفية حول المرسل والمرسل إليه.

---

(1) د.عبد الحسن الحسيني: المرجع السابق, ص792. القاضي الدكتور إيهاب السنباطي: المرجع السابق، ص79. د.طوني عيسى: المرجع السابق، ص44. د.محمد سعيد أحمد إسماعيل: أساليب الحماية القانونية لمعاملات التجارة الإلكترونية، رسالة دكتوراه مقدمة إلى جامعة عين شمس في القاهرة، عام 2005، ص37.

أما بروتوكول الإنترنت IP، فهو مسؤول عن عنونة وترقيم وتوجيه الرسائل إلى عناوينها المقصودة، كما يقوم بمنح كل جهاز أو موقع على الشبكة رقماً معيناً، قد يصل إلى 32 رقماً، حتى يتواصل مع بقية أطراف الشبكة. ونتيجة النمو المتزايد في المنظومات المتصلة بالشبكة، تمّ زيادة هذه الأرقام إلى 128 رقماً. وأي شبكة لا تستخدم هذين البروتوكولين لن تتمكن من الاتصال بالإنترنت.

بناء على ذلك، فإن الرسالة على الإنترنت تتحرك حاملة العنوان المقصود، وتنقسم إلى رزم قد ينطلق كل منها في اتجاه ومسار معين، فإذا وجدت إعاقة، سلكت طريقاً آخر. وتجري عند العنوان المقصود إعادة تكوين هذه الرسالة عن طريق تجميع الرزم المستلمة المكونة لها.

## ثانياً- الجهات المشرفة على الإنترنت:

شبكة الإنترنت ليست ملكاً لأحد، ومن حيث المبدأ لا توجد هيئة رسمية وحيدة – حكومية أو غير حكومية- للإشراف على الإنترنت، ذلك لأن البنية الأساسية تدار بإشراف جهات غير حكومية، أخذت على عاتقها جعل الإنترنت مساحة حرة متاحة للجميع.

وتتصدر هذه الهيئات جمعية الإنترنت (Internet Society) ISOC، وهي مؤسسة أميركية أنشئت عام 1991، تهدف إلى تنسيق عمليات الاتصال والارتباط فيما بين الشبكات[1].

أما الجهات التي تقوم بإدارة البنية الأساسية للإنترنت فهي:

(1) د:عبد الحسن الحسيني: المرجع السابق, ص 454. د.طوني عيسى: المرجع السابق، ص47.

- الاتحاد الدولي للاتصالات ITU[1]، الذي يشرف على منظومات الاتصالات العالمية.
- منظمة الآيكان Icann[2]، وهي تشرف على أسماء المواقع وعناوينها (أسماء النطاقات).

ودون الدخول في الجدل حول مدى سيطرة هذه الجهات على الأركان الثلاثة للإنترنت (حواسيب وكابلات اتصال وأسماء النطاقات)، فإننا نكتفي بالقول بأنه: بدون هذه الأركان فلا حياة للإنترنت[3].

## ثالثاً- العناوين على شبكة الإنترنت والهيئات المانحة لها:

لكي يتم تبادل ونقل البيانات والمعلومات عبر الإنترنت، يجب أن يكون لكل حاسوب أو نظام موصول بالشبكة عنوان خاص به وهو IP address ، يسمح بالتعرف عليه وتعيين مركزه، كما هي الحاجة لمعرفة عنوان المرسل والمرسل إليه في البريد العادي.

وقد ذكرنا سابقاً بأن الإنترنت تمنح كل جهاز أو موقع على الشبكة عنواناً معيناً يصل إلى 32 رقماً، وبسبب طول هذه الأرقام، فإن مسألة تذكرها واسترجاعها تصبح أمراً عسيراً، لذلك فقد تمّ اختراع نظام أسماء النطاقات التي تعبر عن هذه الأرقام، فبدلاً من أن تدخل الرقم الطويل، يكفي أن تكتب مثلاً: www.tareq.com، أو أن تنقر عليها نقرة واحدة، وبفضل نظام يعرف بـ http على الوبّ ، سيتحول الاسم إلى العنوان الرقمي حتى يستكمل التواصل عبر

---

(1) وهو اختصار لـ International Telecommunication Union د:عبد الحسن الحسيني: المرجع السابق, ص 456.

(2) وهو اختصار لـ Internet Corporation For Assigned Name And Numbers. د:عبد الحسن الحسيني: المرجع السابق, ص 414.

(3) القاضي الدكتور إيهاب السنباطي: المرجع السابق، ص90.

الشبكة. وخلال هذه الرحلة يمر العنوان عبر مخدمات عملاقة[1]، مهمتها التعرف على هذه الأسماء وتمريرها.

ويمر أي اتصال في الشبكة بواحد من هذه المخدمات العملاقة (وتعدادها ثلاثة عشر على مستوى العالم)، فإن تعرفت عليه تواصل مع غيره، وإن لم تتعرف فلن يغادر الجهاز المرسل منه.

ويطلق على عنوان الإنترنت IP address تسمية عنوان البريد الإلكتروني، إذا كان يتعلق ببريد إلكتروني، ويسمى اسم النطاق إذا كان يختص بعنونة مواقع الوبّ.

وهناك معياران لتقسيم أسماء النطاقات، هما: المعيار الجغرافي، والمعيار النوعي. فبالمعيار الجغرافي، تعطى كل دولة رمزاً من حرفين للدلالة عليها مثل sy. لسورية ، و eg. لمصر، وuk. للملكة المتحدة، وfr. لفرنسا... وذلك باستثناء الولايات المتحدة الأميركية، حيث لا تحتاج مواقعها إلى تعريف جغرافي. وعلى ذلك فإن اسم أي نطاق لا يحمل تعريفاً جغرافياً سيكون حتماً مسجلاً في الولايات المتحدة الأميركية.

أما المعيار الثاني فهو يتعلق بنوع النشاط، ويضم تقسيمات سارية على مستوى العالم مثل edu. للجهات التعليمية، و gov. للجهات الحكومية، وcom. للجهات التجارية وغيرها، باستثناء اسم int. فهو محجوز للهيئات الدولية[2].

---

(1) **المخدّم** server , هو عبارة عن حاسوب بمواصفات عالية، مزود بذاكرة كبيرة، وقنوات وأدوات اتصال. وفي حال وجود شبكة، فإن هذا الحاسوب يلعب دوراً رئيسياً، في مجال تقديم مختلف الخدمات للمستخدمين. د.عبد الحسن الحسيني: المرجع السابق، ص738.

(2) القاضي الدكتور إيهاب السنباطي: المرجع السابق، ص91-92.

ولا بدّ من الإشارة إلى أن كل دولة موصولة بشبكة الإنترنت، تكون مسؤولة عن إدارة النطاق الخاص بها، كما يمكن أن تخلق نطاقات ثانوية ضمن نطاقها الأساسي ، كأن تخلق مثلاً نطاقاً ثانوياً باسم gov، للدلالة على المواقع الحكومية في القطاع الأساسي sy. الذي يشير إلى الدولة السورية[1].

أما بالنسبة إلى الهيئات المانحة للعناوين على الشبكة، فهناك لجنة تسمى لجنة منح الأرقام على الإنترنت، وتعرف بـ IANA[2]، وهي تتولّى تنظيم عناوين المواقع في النطاقات التي ترمز إلى أسماء الدول، في حين أن صلاحية منح العناوين المستقلة يقع تحت إشراف الآيكان ، وهي شركة أميركية خاصة لا تبتغي الربح تأسست في أيلول عام 1998، مركزها ولاية كاليفورنيا، وتتعامل مع العديد من الهيئات المتخصصة في عملية التسجيل الموزعة حول العالم[3].

---

(1) د.طوني عيسى: المرجع السابق، ص72.

(2) وهو اختصار لـ .Internet Assigned Number Authority د.عبد الحسن الحسيني: المرجع السابق، ص413.

(3) د.طوني عيسى: المرجع السابق، ص69.

# المبحث الثاني

# القانون الجزائي والإنترنت

لما كانت جرائم الإنترنت من المواضيع الحديثة التي شغلت رجال القانون على اختلاف مشاربهم، الأمر الذي دفعهم للبحث في أغوارها بغية فهم طبيعتها. لذلك فقد كان من الواجب أن نخصص هذا المبحث لإزالة هذا الغموض، إضافةً إلى أن دراسة جرائم الإنترنت و التعرف على خصائصها، أمر لا بدّ منه للتمهيد لجريمة الاحتيال عبر الإنترنت، أي للانتقال من الكل إلى الجزء.

لذلك سنقسم هذا المبحث إلى المطلبين التاليين:

المطلب الأول: جرائم الإنترنت.

المطلب الثاني: مفهوم الاحتيال عبر الإنترنت.

# المطلب الأول

# جرائم الإنترنت

تعدّ جريمة "دودة موريس" التي تعود واقعتها إلى 1988/11/2، هي الجريمة الأولى التي ارتكبت عبر الإنترنت حسب التاريخ القانوني، حيث استطاع الشاب "موريس" أن ينشر فيروس إلكتروني[1] تمكّن من مهاجمة آلاف الحواسيب عبر الإنترنت، وقد تسبّب بأضرار بالغة، أبرزها: توقف آلاف الأنظمة عن العمل، وتعطيل الخدمة... وقد قدرت الخسائر لإعادة إصلاح هذه الأنظمة وتشغيل المواقع المصابة بحوالي مائة مليون دولار[2].

ومنذ ذلك الحين ورجال القانون يبحثون عن تعريف لجرائم الإنترنت، لفهم طبيعتها وخصائصها. كما أن رجال الفقه الإسلامي لم يقفوا مكتوفي الأيدي أمام هذه الظاهرة الإجرامية، بل على العكس قدموا الدراسات التي تبين موقف الشريعة الإسلامية من هذه الجرائم.

لذلك سنبحث في هذا المطلب تعريف جرائم الإنترنت وخصائصها ثم موقف الشريعة الإسلامية منها.

## أولاً- تعريف جرائم الإنترنت:

تعددت محاولات الفقهاء في تعريف جرائم الإنترنت، ومنها:

---

(1) الفيروس: هو عبارة عن برنامج صغير يؤدي إلى تدمير الملفات المعلوماتية وأنظمة التخزين من أقراص مغناطيسية وغير ذلك. ويمكن أن ينتج الفيروس عن خطأ ما في البرمجة، كما يمكن أن يكون صادراً عن مبرمجين محترفين يبغون إلحاق الضرر بالآخرين. د.عبد الحسن الحسيني: المرجع السابق، ص 851.

(2) د.علي جبار الحسيناوي: جرائم الحاسوب والإنترنت، الطبعة الأولى، دار اليازوري العلمية للنشر والتوزيع، عمان، 2009، ص10.

- هي "ذلك النوع من الجرائم التي تتطلب إلماماً خاصاً بتقنيات الحاسب الآلي ونظم المعلومات، لارتكابها أو التحقيق فيها ومقاضاة فاعليها[1]".
- أنها "الجرائم التي لا تعرف الحدود الجغرافية، والتي يتم ارتكابها بأداة هي الحاسب الآلي عن طريق شبكة الإنترنت، وبواسطة شخص على دراية فائقة[2]".
- وفي تعريف آخر "كل اعتداء يقع على نظم الحاسب الآلي وشبكاته أو بواسطتها[3]".
- كما أنها "الجرائم الناشئة عن استعمال التواصل بين الشبكات[4]".
- وهي أيضاً "تلك الجرائم العابرة للحدود والتي تقع على شبكة الإنترنت أو بواسطتها من قبل شخص على دراية فائقة بها[5]".

والباحث يؤيد هذا التعريف الأخير؛ لأنه يبرز خصائص جرائم الإنترنت. إلاّ أنه من الأفضل عدم تحديد هذه الجرائم بأنها عابرة للحدود، لأنها من الممكن أن تكون جرائم داخلية أو دولية أو ذات بعد دولي كما سنرى لاحقاً. لذلك نرى أن يكون تعريف جرائم الإنترنت بأنها: **تلك الجرائم التي تقع على شبكة الإنترنت أو بواسطتها من قبل شخص ذي معرفة تقنية.**

---

(1) د.عبد الفتاح مراد: المرجع السابق، ص40.

(2) المحاميان منير وممدوح الجنبيهي: جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، عام 2005، ص13.

(3) المحامي محمد أمين الشوابكة: جرائم الحاسوب والإنترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، عام 2006، ص10.

(4) د.عمر بن يونس :المرجع السابق, ص 71.

(5) نبيلة هبة هروال: الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، عام 2007، ص30.

## ثانياً- خصائص جرائم الإنترنت:

من خلال التعريف الذي أوردناه لجرائم الإنترنت يمكننا تحديد خصائص هذه الجرائم كما يلي:

### أ-جرائم تُرتكب عبر شبكة الإنترنت أو عليها:

إن اتساع حجم شبكة الإنترنت وسهولة الولوج إليها، والتزايد المستمر في استخدام هذه الشبكة، جعل منها مسرحاً لكثير من الأفعال الإجرامية. فمعظم الجرائم التقليدية أصبحت تُرتكب عبر الإنترنت كالاحتيال مثلاً، إضافة إلى أن هذه الشبكة لم تسلم بحد ذاتها من اعتداءات المجرمين التي تناولت أنظمتها ومعلوماتها.

### ب-مرتكب جرائم الإنترنت ذو معرفة تقنية:

تعد المهارة التقنية المطلوبة لتنفيذ جرائم الإنترنت أبرز خصائص مجرمي الإنترنت، فتنفيذ هذه الجرائم يتطلب قدراً من المهارات التقنية، سواء تم اكتسابها عن طريق الدراسة المتخصصة، أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات. إلا أن ذلك لا يعني ضرورة أن يكون مجرم الإنترنت على قدرٍ كبيرٍ من العلم في هذا المجال، فالواقع العملي أثبت أن أشهر مجرمي الإنترنت لم يحصلوا على مهاراتهم التقنية عن طريق التعليم أو الخبرة المكتسبة من العمل في هذا المضمار[1].

---

(1) د.نائلة عادل محمد فريد قورة: جرائم الحاسب الآلي الاقتصادية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، عام 2005, ص57.

## ج- الحاسوب هو أداة ارتكاب جرائم الإنترنت:

يعدّ الحاسوب وسيلة النفاذ إلى شبكة الإنترنت، ومن ثم لا يمكن تصور ارتكاب جريمة إنترنت من دونه، ولا عبرة هنا لشكل الحاسوب الذي قد يتخذ شكله التقليدي أو شكل الحاسوب النقال، أو قد يكون ضمن الهاتف النقال أو حتى ضمن ساعة اليد...الخ.

ولا بدّ هنا من التمييز بين جريمة الحاسوب وجريمة الإنترنت، **فجريمة الحاسوب** هي التي تُرتكب بواسطة الحاسوب أو على مكوناته المعنوية، فقد تُرتكب من خلال حاسوب واحد أو من خلال شبكة داخلية تضم عدة حواسيب دون أن يكون هناك ولوج إلى الإنترنت، كما هو الحال في جرائم التزوير أو التزييف التي تستخدم الحواسيب، أو الجرائم التي تهدف إلى سرقة معلومات الحاسوب أو إتلافها. أما **جرائم الإنترنت** فإن شرطها الأساسي هو اتصال الحاسوب بالإنترنت، فالحاسوب هو الوسيلة التي لا مفر منها للولوج إلى هذه الشبكة.

ولا بدّ من الإشارة هنا، إلى أن جانباً من الفقه يستخدم مصطلح **الجريمة المعلوماتية أو الجريمة الإلكترونية**، للدلالة على جرائم الحاسوب والإنترنت معاً، بحيث يشمل هذان المصطلحان كلا النوعين. ومن ثم فإن مصطلح الجريمة المعلوماتية أو الجريمة الإلكترونية، أكثر شمولاً من جريمة الإنترنت[1].

## د- جريمة الإنترنت لا تعرف الحدود الجغرافية:

(1) نبيلة هبة هروال: المرجع السابق، ص31 و 54. د.نائلة قورة: المرجع السابق، ص35. المحامي محمد أمين الشوابكة :المرجع السابق, ص10.

لا تعرف جريمة الإنترنت الحدود الجغرافية، أي أنها من الممكن أن تكون جريمة داخلية أو دولية أو ذات بعد دولي.

فهي جريمة **داخلية** عندما تقع كاملة في نطاق إقليم دولة معينة.

وجريمة **دولية** عندما تتعلق بالقانون الدولي، أي عندما يكون أحد أطرافها شخصاً دولياً، على نحو ما حدث في التجسس الذي قامت به الولايات المتحدة الأميركية، عندما انتهكت أنظمة أعدائها الحاسوبية، وذلك بواسطة أسلحة معلوماتية فتّاكة، أثناء القصف الجوي للحلف الأطلسي في كوسوفو[1].

وقد تكون جريمة **ذات بعد دولي**، إذا اتفق المجتمع الدولي– بمقتضى اتفاقية دولية– بأن جريمة معينة تشكّل عدواناً على كل دولة، أو عندما ترتكب الجريمة داخل دولة معينة إلاّ أنها تمتد خارج إقليم تلك الدولة مثل جريمة ترويج المخدرات عبر الإنترنت[2].

## هـ– صعوبة اكتشاف وإثبات جرائم الإنترنت:

تتصف جرائم الإنترنت بأنها صعبة الاكتشاف، لأن الجاني من الممكن أن يستخدم اسماً مستعاراً، أو أن يرتكب جريمته من خلال إحدى مقاهي الإنترنت. إضافة إلى أنها صعبة الإثبات لأنها لا تترك أثراً مادياً، بسبب إمكانية حذف الآثار المعلوماتية المستخدمة في ارتكاب الجريمة خلال ثوان[3].

## ثالثاً– موقف الشريعة الإسلامية من جرائم الإنترنت:

لا شكّ أن رجال الفقه الإسلامي معنيون بما يستجد في الحياة من ظواهر، خاصة إذا كانت هذه الظواهر تتصل بأفراد المجتمع اتصالاً وثيقاً، لأن

---

(1) د.عمر بن يونس: المرجع السابق، ص 195– 197.

(2) د.عمر بن يونس: المرجع السابق، ص195.

(3) د.سليمان أحمد فضل: المرجع السابق، ص21.

الفقيه يجب أن لا يقبع خلف النص الفقهي، بل يجب عليه أن يضع أحكاماً تتماشى مع الوقائع المستحدثة التي لم يرد فيها نص من قرآن أو سنة. لذلك فقد وضع الفقهاء منذ زمن طويل قاعدة فقهية هي " تغير الأحكام بتغير الأعراف والعادات والأزمنة والأمكنة"[1].

و هناك من يرى من فقهاء الشريعة بأنه إذا كانت شبكة الإنترنت من النظم المستحدثة، فإن ذلك لا يعني أن الشريعة ترفضها، ما دام هناك فوائد تعود على البشرية بفضل استخدامها، فالعلم النافع أمر تحبذه الشريعة وتحثّ عليه، ولا يمكن هنا إعمال القاعدة الفقهية القائلة: "دفع المفاسد مقدم على جلب المصالح"، لأن لشبكة الإنترنت فوائد عظيمة، والمفسدة تأتي بالاستغلال السيئ لها. فشبكة الإنترنت نفع في ذاتها. ولو أنه تمّ الأخذ بقاعدة دفع المفاسد، لما أخذت الشريعة بأي تقنية علمية، لأنه ما من اكتشاف إلاّ وله أضرار مثلما له فوائد. وإذا كانت الأضرار تأتي من خلال استعمال الفرد للإنترنت استعمالاً سيئاً، فيجب أن يعاقب هذا الفرد إذا كان فعله يعد جريمة من الجرائم، إذ إن نظرية العقاب في الشريعة الإسلامية تمتاز بالمرونة، ذلك أن نظام التعزير يصلح لكل زمان ومكان، إذا لم يشكل الفعل جريمة حد أو قصاص[2].

أما جريمة الاحتيال، فهي جريمة تعزيرية لم تحدد الشريعة الإسلامية لها عقوبة محددة، وإنما تُرك تحديد عقوبتها لولي الأمر، أي إلى السلطة التشريعية المختصة في البلاد[3].

---

(1) د.الشحات إبراهيم محمد منصور: الجرائم الإلكترونية في الشريعة الإسلامية والقوانين الوضعية، دار النهضة العربية، القاهرة، بلا عام، ص80.

(2) د.الشحات إبراهيم محمد منصور: المرجع السابق، ص80-81-82.

(3) د.الشحات إبراهيم محمد منصور: المرجع السابق، ص69.

# المطلب الثاني
# مفهوم الاحتيال عبر الإنترنت

تقسم جرائم الإنترنت إلى نوعين[1]: **الأول: الجرائم التقليدية التي ترتكب بواسطة الإنترنت**، وهي تلك الجرائم التي كانت موجودة قبل ظهور الإنترنت، ولكن بعد ظهور هذه التقنية أصبحت ترتكب بواسطتها، فراحت تبدو وكأنها جرائم جديدة. ومن هذه الجرائم: جريمة التهديد بالقتل المرتكبة عبر البريد الإلكتروني، والجرائم المخلّة بالأخلاق والآداب العامة التي ترتكب عبر المواقع الإباحية، وجريمة الذم والقدح، وغير ذلك من الجرائم.

أما **النوع الثاني: فهي الجرائم المستحدثة**، والتي يقصد بها تلك الجرائم التي ظهرت بعد اختراع الإنترنت ولم تكن معروفة من قبل، ومن أمثلة هذه الجرائم : جريمة الدخول غير المصرح به إلى أنظمة الحاسوب أو المواقع الإلكترونية، وجريمة تعطيل أو عرقلة نظام معلوماتي، وجريمة إتلاف المعلومات عن طريق زرع الفيروسات وغيرها.

ويعدّ الاحتيال عبر الإنترنت من الجرائم التي تنتمي إلى طائفة الجرائم التقليدية التي ترتكب بواسطة الإنترنت.

وبناء على ذلك، سوف نتناول في هذا المطلب التطور التاريخي للاحتيال عبر الإنترنت، وتعريفه، ثم حجم ارتكاب هذه الجريمة.

---

(1) د.حسين بن سعيد الغافري, السياسة الجنائية في مواجهة جرائم الإنترنت (دراسة مقارنة),دار النهضة العربية– القاهرة,عام 2009, ص 79 و 217.

## أولاً- التطور التاريخي لجريمة الاحتيال عبر الإنترنت:

في العقد السابع من القرن العشرين، كان الاحتيال باستعمال الحاسوب من الجرائم الأولى التي بدأت تعرف على نحو واسع على أنها نوع جديد من الجرائم. ونتيجة لذلك، تمت أول مواجهة تشريعية لهذه الجرائم، من خلال "قانون فلوريدا" لجرائم الحاسوب، فهو أول قانون جرّم الاحتيال على الحاسوب. وقد صدر هذا القانون في عام 1978، وذلك بعد حادثة ذائعة الصيت في أحد الأحداث الرياضية، حيث قام البعض بطباعة بطاقات مزوّرة.

في ذلك الوقت، تمّ تبنّي هذه المواجهة التشريعية من أغلب الولايات الأمريكية، عدا ولاية فيرمونت.

ومع بداية الثمانينيات، بدأت معظم حكومات العالم بسن قوانين مماثلة، فكانت كندا من أوائل الدول التي سنّت قانوناً اتحادياً يخاطب جرائم الحاسوب، وذلك عن طريق تعديل القانون الجزائي عام 1983.

كما صدر القانون الأميركي للاحتيال وإساءة استخدام الحاسوب في عام 1984[1]، وتمّ تعديله في الأعوام: 1986 – 1988 – 1989- 1990.

كما صدر في بريطانيا قانون إساءة استخدام الحاسوب عام 1990، الذي جرّم الاحتيال في الفصل الثالث منه.

وفي بداية التسعينيات، ومع شيوع الإنترنت وظهور الوبّ، امتدت جرائم الحاسب إلى الشبكة العالمية، وأصبح التركيز منذ ذلك الوقت على جرائم الإنترنت، وخاصة الاحتيال عبر الشبكة[2].

## ثانياً- تعريف جريمة الاحتيال عبر الإنترنت:

---

(1) يعرف اختصاراً بـ Computer Fraud And Abuse Act (CFAA)

(2) Eoghn Casey: Digital Evidence And Computer Crime, second edition, Acadimic Press, 2004, chapter 2, P2.

تعددت التعريفات التي تناولت الاحتيال عبر الإنترنت، نذكر منها على سبيل المثال:

أنها "أي سلوك احتيالي ينتهج منهج الحوسبة بنيّة الحصول على امتياز مالي[1]".

كما عرّف البعض الاحتيال المعلوماتي بأنه: "التلاعب العمدي بمعلومات وبيانات تمثّل قيماً مادية يختزنها نظام الحاسب الآلي، أو الإدخال غير المصرح به لمعلومات وبيانات صحيحة، أو التلاعب في الأوامر والتعليمات التي تحكم عملية البرمجة، أو أيّة وسيلة أخرى من شأنها التأثير على الحاسب الآلي، حتى يقوم بعملياته بناءً على هذه البيانات أو الأوامر أو التعليمات، من أجل الحصول على ربح غير مشروع وإلحاق الضرر بالغير[2]".

وعرّف مكتب التحقيقات الفدرالي الأميركي الاحتيال عبر الإنترنت بأنه: "أي مخطط احتيالي عبر الإنترنت، يلعب دوراً هاماً في عرض السلع أو الخدمات غير الموجودة أصلاً أو طلب دفع ثمن تلك الخدمات أو السلع عبر الشبكة[3]".

أما وزارة العدل الأميركية فعرّفته بأنه: "شكل من التخطيط الاحتيالي الذي يستخدم محتويات الإنترنت، مثل: الدردشة، البريد الإلكتروني ، المواقع الإلكترونية... لتقديم صفقات احتيالية أو لإرسال نتائج الاحتيال إلى المؤسسات المالية[4]".

---

(1) د.عمر بن يونس: المرجع السابق، ص411. د.سليمان فضل: المرجع السابق، ص197.

(2) د.نائلة عادل محمد فريد قورة: المرجع السابق، ص425.

(3) On line fraud and crime: Are consumers safe? Hearing before the subcommittee on commerce trade and consumer protection, 2001, P6.

(4) Micheal Kunz and Patrick Wilson: computer crime and computer fraud, University of Mayland, 2004, P12.

ويلاحظ على هذه التعاريف، بأن التعريفين الأول والثاني، لم يفرقا بين الاحتيال المعلوماتي والاحتيال عبر الإنترنت، إذ إن مفهوم الاحتيال المعلوماتي أوسع من مفهوم الاحتيال عبر الإنترنت، لأنه يشمل الاحتيال عن طريق الحاسوب والاحتيال عبر الإنترنت، أما الاحتيال عبر الإنترنت فلا يشمل سوى الاحتيال عبر الشبكة.

أما التعريفين الثالث والرابع، وإن كانا قد أشارا إلى ضرورة أن يكون الاحتيال عبر الإنترنت، إلاّ أنهما قد حصرا وسائل الاحتيال بعرض السلع والخدمات غير الموجودة، أو تقديم الصفقات الاحتيالية، أو إرسال نتائج الاحتيال إلى المؤسسات المالية.

**ويرى الباحث** أنه من الأفضل عدم ذكر وسائل الاحتيال وصوره عند تعريف هذه الجريمة، نظراً إلى طبيعة وسائل الاحتيال عبر الإنترنت التي يمكن أن تتخذ صوراً لا حصر لها.

بناء على ما تقدم ، يمكن تعريف الاحتيال عبر الإنترنت بأنه: **الاستيلاء على مال الغير بالخداع عبر تقنية الإنترنت.**

## ثالثاً– حجم جريمة الاحتيال عبر الإنترنت:

هناك العديد من الدراسات التي أُجريت لرصد حجم جريمة الاحتيال عبر الإنترنت والخسائر الناجمة عنها. وقد أشارت هذه الدراسات إلى أن الاحتيال عبر الإنترنت له النصيب الأكبر من جرائم هذه الشبكة.

وقد كشفت إحدى الدراسات التي أُجريت في الولايات المتحدة الأميركية، بأن خسائر المبيعات بسبب الاحتيال عبر الإنترنت كانت أكثر من /700/ مليون دولار في عام 2001. وفي دراسة أخرى ، تبين بأن 1% من جرائم الحاسوب تمّ اكتشافها، وأن 7% من الجرائم تمّ الإبلاغ عنها إلى الجهات

المسؤولة عن تطبيق القانون في أميركا، وأن 3% من تلك الجرائم تمّ التحقيق بها وانتهت المحاكمة بها إلى السجن[1].

وفي تقرير جديد حول جرائم الإنترنت، صادر عن مركز شكاوى جرائم الإنترنت IC3 لعام 2007 والتابع لمكتب التحقيقات الفيدرالية الأمريكية، حيث استلم المركز /206.884/ شكوى عبر موقعه الإلكتروني خلال عام 2007، وعالج المركز معظم هذه الشكاوى وأحالها إلى الجهات المختصة لمتابعة التحقيقات. وقد تضمنت هذه الشكاوى العديد من أشكال الاحتيال، مثل الاحتيال التجاري عن طريق عدم تسليم البضائع، والاحتيال ببطاقات الائتمان وغير ذلك من أشكال الاحتيال، و كان إجمالي الخسائر المالية للقضايا الاحتيالية /239.09/ مليون دولار[2].

كما أشار هذا التقرير إلى أن نسبة المرتكبين للجرائم من الذكور 75.2% إلى نسبة 24.8% من الإناث ، كما وضع قائمة بأكثر عشرة دول تُرتكب فيها جرائم الإنترنت حسب الإحصائيات، وهي حسب الترتيب التالي[3]:

1- الولايات المتحدة الأميركية.

2- المملكة المتحدة.

3- نيجيريا.

4- كندا.

---

(1) Joseph W. Koletar : Fraud Exposed, What you don't know could cost your company millions, John Wiley & Sons, in 2003, P-48.

(2) Internet crime complaint center (Ic3), 2007 internet crime report, P-1.

(3) Internet crime complaint center, op- cit, P 7-9.

5- رومانيا.

6- إيطاليا.

7- إسبانيا.

8- جنوب أفريقيا.

9- روسيا.

10- غانا.

**تقسيم:**

أما وقد انتهينا من تسليط الضوء على ماهية الإنترنت وما يُرتكب من جرائم عبر هذه التقنية، سنشرع إلى البحث في الاحتيال عبر الإنترنت من خلال البابين التاليين:

الباب الأول: الاحتيال عبر الإنترنت رؤية موضوعية.

الباب الثاني: الاحتيال عبر الإنترنت رؤية إجرائية.

# الباب الأول

# الاحتيال عبر الإنترنت رؤية موضوعية

إن دراسة قضايا الاحتيال عبر الإنترنت ذات الطابع الواقعي أمرٌ في غاية الأهمية للتعرف على أساليب ارتكاب هذه الجريمة، ومن ثم تسليط الضوء على المواجهة التشريعية لهذا النوع من الإجرام في بعض الدول الأجنبية

والعربيـة. وكيـف واجـه القضـاء هـذه الجـرائم فـي بعـض الـدول التـي لـم تسـن تشريعات لمواجهة هذه الجرائم المستحدثة.

وأمام غيابِ النصَ التشريعي الذي يعاقب على هذه الجريمة في بلادنا، كان لزاماً علينا دراسة مدى إمكانية تطبيق نصوص التجريم التقليدية على هذه الجريمة، والبحث والتمحيص في المشكلات الذي يثيرها هذا التطبيق، في الوقت الذي بدأت تُعرض على قضائنا السوري العديد من هذه القضايا.

وعلى ذلك سنقسم هذا الباب إلى الفصلين التاليين:

الفصل الأول: الإطار الواقعي والتشريعي للاحتيال عبر الإنترنت.

الفصل الثاني: مدى انسجام الاحتيال عبر الإنترنت مع مفهومه التقليدي.

# الفصل الأول
# الإطار الواقعي والتشريعي للاحتيال عبر الإنترنت

إن دراسة صور الاحتيال عبر الإنترنت، من خلال استعراض القضايا ذات الطابع الواقعي، أمر يهدف **أولاً** إلى التنبيه والتوعية من أجل تفادي الوقوع في مثل هذه الطرق الاحتيالية. ويهدف **ثانياً** إلى الإلمام بمختلف أشكال الاحتيال، للحيلولة دون الوقوع في قصور تشريعي عندما يجرم المشرع السوري الاحتيال عبر الإنترنت.

كما إن التعرف على بعض تشريعات الدول الأجنبية والعربية والاتفاقيات الدولية في مجال جرائم الإنترنت وخاصة الاحتيال، أمرٌ في غاية الأهمية لمعرفة أسلوب صياغة هذه التشريعات، ومدى شمولها لمختلف أساليب ارتكاب هذه الجريمة، أملاً في أن يستأنس بها المشرع السوري عند سنه لمثل هذه التشريعات.

واستناداً لذلك، سوف نقسم هذا الفصل إلى المبحثين التاليين:

المبحث الأول: صور الاحتيال عبر الإنترنت.

المبحث الثاني: المواجهة التشريعية.

# المبحث الأول

# صور الاحتيال عبر الإنترنت

يرافق تطور نظم الحوسبة والاتصالات تطوراً مماثلاً في أساليب ارتكاب الاحتيال عبر الإنترنت، وهو تلازم يشبه إلى حد كبير مرافقة الإنسان لظله. لذلك فإنه من العسير حصر أساليب الاحتيال عبر الإنترنت، إلا أنه يمكن تصنيف هذه الأساليب ضمن مجموعات رئيسية عامة، تتضمن أبرز صور هذا الاحتيال، مثل الاستيلاء على أموال المصارف، والاحتيال التجاري، والاحتيال عن طريق البريد الإلكتروني، واحتيال الاتصالات... الخ.

والحقيقة أن هناك صورة بارزة من صور الاحتيال عبر الإنترنت، هي الاحتيال عن طريق بطاقات الائتمان. لذلك رأينا أن نتناول هذه الصورة بشيء من التفصيل، لنتعرف على أنواع هذه البطاقات، وأساليب الحصول على أرقامها السرية، وأفعال الاحتيال التي ترتكب بواسطتها.

وبناءً على ذلك، سوف نقسم هذا المبحث إلى المطلبين التاليين:

المطلب الأول: الصور العامة للاحتيال عبر الإنترنت.

المطلب الثاني: الصور الخاصة للاحتيال عن طريق بطاقات الائتمان.

# المطلب الأول
# الصور العامة للاحتيال عبر الإنترنت

إن أساليب الاحتيال عبر الإنترنت متنوعة ومتجددة، وهي تساير التقدم التكنولوجي. وإذا كان الأمر كذلك فإن ما نرمي إليه في هذا المطلب هو تسليط الضوء على الصور العامة فقط للاحتيال عبر الإنترنت، لأن الإحاطة بجميع الأساليب التقنية للاحتيال أمر يشبه ملاحقة السراب في الصحاري الشاسعة. وعليه يمكن أن نتناول صور الاحتيال عبر الإنترنت من خلال المجالات الرئيسية التالية:

## أولاً– الاستيلاء على أموال المصارف:

أتاحت الإنترنت لعملاء المصارف والبنوك الاطلاع على حساباتهم وإجراء التحويلات المالية المرغوب بها من خلال المواقع الإلكترونية العائدة لهذه المصارف على الشبكة، إلا أن هذه المؤسسات المصرفية كانت الهدف المفضل للهكرة[1]، الذين يقتحمون الأنظمة المعلوماتية للمصارف عبر الشبكة، ثم يتلاعبون في كشوف وحسابات العملاء، ويقومون بنقل الأرصدة من حساب إلى آخر، أو إضافة بضعة أصفار إلى رقم ما، في هذا الحساب أو ذاك.

وقضية "بنك الباسيفيك الوطني" في الولايات المتحدة الأمريكية تعد نموذجاً لهذا النوع من الجرائم، فقد كان المواطن الأمريكي "ستانلي مارك" يعمل أخصائياً للحاسبات في هذا البنك، واكتشف مصادفة شفرة تحويل حسابات العملاء بين البنك وغيره من البنوك التي تتعامل معه، فقام بإصدار أوامر

(1) Hacker هو اسم للشخص الذي يدخل إلى نظام المعلومات أو قاعدة المعطيات أو إلى شبكة, دون أن يكون مسموحاً له بذلك. د.عبد الحسن الحسيني: المرجع السابق، ص 389.

إلكترونية لعدة فروع للبنك بتحويل مبالغ قدرت بأربعة ملايين دولار لحسابه الذي قام بفتحه في أحد المصارف السويسرية، ثم انتقل إلى جنيف وسحب المبلغ المذكور، واشترى به ماساً وأودعه في خزانة خاصة به بأحد البنوك هناك، ومرت شهور دون أن يكتشف أحد حقيقة ما حدث، لولا أن المتهم نفسه قد اعترف بالواقعة وهو مخمور.

كما تمكن مراهق من اليهود الصهاينة دون العشرين من عمره من اختراق مصرف "ستي بنك" بواسطة برنامج إلكتروني، يقوم بإجراء حسابات منطقية للتوفيق والتبديل، حتى يتصادف الرقم السري الصحيح مع نظام المصرف الإلكتروني، وقد استخدم الجاني حصيلة هذا الاختراق في شراء سيارة فاخرة وملابس ومعدات إلكترونية من الولايات المتحدة، ولم يتم اكتشاف هذا الاحتيال إلا بعد وصول السيارة عبر الشحن البحري، وشكوك رجال الجمارك حول هذا الصبي، وعلى أثر ذلك اعترف بمصدر حصوله على الأموال، وشرح الوسيلة التي اخترق بها المصرف، وكيفية تحويل الأموال.

وفي فرنسا تم ضبط عمليات احتيال بنكية عن طريق الحاسوب والإنترنت، شملت حوالي ثلاثين مليون حساب بنكي[1].

## ثانياً- الاحتيال التجاري:

يتم الاحتيال التجاري عبر الإنترنت عند عدم تسليم البضائع للمشتري بعد أن يقوم بدفع ثمنها، أو عدم أداء الخدمة التي تم استيفاء أجورها. وقد انتشرت عبر الإنترنت المواقع المتخصصة في بيع البضائع والسلع، حيث يتم من خلال هذه المواقع عرض صور البضائع والمنتجات للبيع المباشر أو عن طريق

(1) راجع في هذه الأمثلة د.جميل عبد الباقي الصغير: الإنترنت والقانون الجنائي، دار النهضة العربية- القاهرة، عام 2002، ص35 . د. محمد الشناوي: جرائم النصب المستحدثة، دار الكتب القانونية، مصر المحلة الكبرى عام 2008، ص88.

المزاد، غير أنه في كثير من الأحيان لا يتم تسليم هذه البضائع، بعد أن يتم استيفاء الثمن عن طريق بطاقات الائتمان أو التحويلات المصرفية.

وطبقاً لإحصائيات لجنة التجارة الفيدرالية ولجنة مراقبة الاحتيال عبر الإنترنت، فإن هذه الطريقة في الاحتيال تعد الأكثر انتشاراً في العالم الافتراضي[1].

ومن أمثلة هذا الاحتيال أنه في 10 أيار عام 2001، أدانت هيئة المحلفين الاتحادية في مقاطعة "كولورادو" المتهم "دانيال كتلسن" Daniel Ketelsen بالاحتيال عبر الإنترنت، حيث قام "كتلسن" باستعمال اسماً كاذباً واستلام المال كثمن لقطع حاسوب عرضها للبيع من خلال موقع e-bay ، ولكنه لم يقم بتسليم البضائع. وبعد استلام الكثير من الشكاوى بحق "كتلسن"، قام هذا الأخير برفع شكوى ضد شركة التأمين، زاعماً أن البضاعة سرقت من مرآبه، ولكن التحقيق الذي قام به المحققون في مؤسسة البريد الأمريكية، كشف أن "كتلسن" لا يملك أية بضاعة، وأنه كان يحاول أيضاً الحصول على المال بشكل غير شرعي من شركة التأمين[2].

وفي قضية أخرى، تم استدعاء أربعة متهمين إلى المحكمة بتهمة الاحتيال عبر الإنترنت في جورجيا، وذلك لقيامهم بالاحتيال عبر موقع e-bay، حيث قاموا باستخدام الموقع لبيع إطارات السيارات، وقام الزبائن بالتفاوض على السعر والدفع عن طريق تحويل الأموال عبر الإنترنت، أو عبر موقع "ويسترن يونين" western union، ولكن البضائع لم ترسل للضحايا. ومنذ تموز عام 2003 حتى تشرين الأول عام 2006، دفع حوالي

---

(1) د. عمر بن يونس: المرجع السابق، ص415

(2) On line fraud and crime,op-cit, p.33.

215 شـخص للمتهمـين مـا يعـادل 539.000 دولار ثمنـاً لبضـائع لـم يـتم إرسالها[1].

ولتفادي عمليات الاحتيال عند الشراء عبر الإنترنت، فإن هذه الشبكة تقدم خدمة يطلق عليها Escrow House، وهي عبارة عن مؤسسات مالية تُرسل إليها النقود التي يراد شراء المنتجات بها من أي موقع إلكتروني، حيث تقوم بتجميد الأموال لديها حتى يصلها إخطار من المشتري بأنه قد تسلم المنتجات التي طلبها، وأنها مطابقة للمواصفات المطلوبة. عند ذلك تقوم هذه المؤسسات بتحويل الأموال إلى المواقع التي تم الشراء منها. وفي حال عدم وصول المنتجات التي طلبها العميل، أو كانت غير مطابقة للمواصفات، فإنه يمكن استرداد هذه الأموال[2].

## ثالثاً- الاحتيال عن طريق الأوراق المالية Securities Fraud:

أدى النمو السريع للإنترنت إلى تغيرات هامة في مجال صناعة الأوراق المالية. ويلاحظ المراقبون تزايد شعبية الإنترنت عند المستثمرين، لأنها تسمح لهم ببيع وشراء الأسهم من منازلهم عن طريق حواسيبهم الشخصية مع نسب منخفضة من العمولات التجارية.

ولسوء الحظ فإن الإنترنت توفر للمحتالين عدة وسائل يمكن الاستفادة منها في الاحتيال على المستثمرين، ومن هذه الوسائل:

أ- تقدم الإنترنت للمحتالين القدرة على الاتصال الإلكتروني قليل الكلفة بملايين الضحايا حول العالم، وذلك من خلال المواقع الاحتيالية، التي تظهر وكأنها توفر معلومات استثمارية صحيحة.

---

(1) IC3, Internet crime report 2007, p-15

(2) ومن مواقع هذه المؤسسات www.iescrou.com د.جميل عبد الباقي الصغير: المرجع السابق، ص39.

ب–يستطيع المحتالون أن يبقوا مجهولي الهوية على الإنترنت، وأن يرتكبوا جرائمهم من أي مكان في العالم، الأمر الذي يجعل من الصعب ملاحقتهم والقبض عليهم ومحاكمتهم[1].

أما الأسلوب الأكثر استعمالاً في الاحتيال عن طريق الأوراق المالية، فيتم بنشر المحتالين لمعلومات كاذبة عن أسهم بعض الشركات، لكي يزيدوا من شراء المستثمرين. وهذه الزيادة في الطلب تزيد من قيمة الأسهم. وغالباً ما يكون هؤلاء المحتالون يملكون كمية كبيرة من هذه الأسهم، حيث يحصلون على ربح سريع عند بيعها بسعر مرتفع. وبالمقابل، فإن المستثمرين الذين اشتروا هذه الأسهم بناء على المعلومات الكاذبة سيواجهون خسارة كبيرة عندما يقومون بالبيع.

ومن أمثلة هذا الأسلوب في الاحتيال عبر الإنترنت، أن أحد سماسرة البورصة، أخبر زبائنه بأنه قادر على تحقيق أرباح ضخمة من خلال تجارة الأسهم السريعة، وذلك باستخدام برنامج حاسوب سري يعمل ضمن الحاسوب الضخم في بورصة "وول ستريت". وبالرغم من أنه لم يكن لديه البرنامج المزعوم للدخول إلى الحاسوب المذكور، فقد اقتنع مئات الزبائن باستثمار ما لا يقل عن (100.000) دولار لكل منهم[2].

وفي قضية أخرى، قامت إحدى شركات الهاتف الخلوي المسبق الدفع، بإدراج إعلان عبر الإنترنت عن بيع أسهم في الشركة بسعر (5.000) دولار للسهم الواحد، وبدلاً من أن تستخدم هذه المبالغ لبناء شبكة هاتف خلوي في

---

(1) Richard Hillman: securities fraud, The internet poses challenges to Regulateres and Investors, United States General Accounting Office, 1999, P4.

(2) Eoghan Casey, op-cit, chapter 1, p.26

منطقة "بوسطن" كما كان معلناً، فإن المال الذي تمّ تحصيله من هذه المبيعات قد تم تحويله إلى حسابات مالكي الشركة[1].

وفي أيار عام 1997 تم نسخ الموقع الإلكتروني العائد لشركة سمسرة مرخصة عبر الإنترنت، بما فيه من معلومات واسم الشركة وعنوانها وأرقام الهواتف التي تم تعديلها فيما بعد، ثم استخدم هذا الموقع المنسوخ لخداع المستثمرين، وخاصة الأجانب الذين قاموا بإرسال المبالغ على العناوين الموجودة على الموقع. وقد استمرت هذه العملية لمدة 10 أشهر، إلى أن قام المنتهكون بالانتقال إلى موقع إلكتروني آخر[2].

ويعرف أسلوب الإعلان المزيف عن الوضع المالي لمؤسسة اقتصادية بأسلوب (Pump and dump)، فالتأثير بالسوق ورفع قيمة أسهم شركة ما (The Pump)، ثم القيام ببيعها بمجرد بروز أثر إيجابي على هذه الخديعة (The dump)[3].

## موقف المشرع السوري من الاحتيال عن طريق الأوراق المالية:

(1) Richard Hillman, op-cit, p.8.

(2) Richard Hillman, op-cit, p.9.

(3) د.عمر بن يونس: المرجع السابق ص416. د.محمد الشناوي:المرجع السابق، ص88.

ضاعف المشرع السوري عقوبة الاحتيال[1] في ظرفين: الأول يتعلق بتأمين وظيفة عامة، والثاني يتعلق بالاحتيال بمناسبة إصدار أسهم أو سندات، وهذا ما نصت عليه المادة 642 من قانون العقوبات بقولها:

(تضاعف العقوبة إذا ارتكب الجرم في إحدى الحالات التالية:

أ- بحجة تأمين وظيفة أو عمل في إدارة عمومية.

ب- بفعل شخص يلتمس من العامة مالاً لإصدار أسهم أو سندات أو غيرها من الوثائق لشركة أو لمشرع ما).

وفيما يخص الفقرة (ب)، فإنه يجب لتشديد العقوبة أن يتوفر العنصران التاليان[2]:

**العنصر الأول:** توجيه أساليب الخداع إلى جمهور الناس، أي يجب أن يقوم المحتال باستعمال وسيلة علنية لمخاطبة الناس ودعوتهم إلى الاكتتاب في الأسهم أو السندات التي أصدرها. ويقصد بوسيلة العلانية، كل أسلوب يتجه الخطاب فيه إلى عدد غير محدود من الناس، مثل النشر في صحيفة دورية أو توزيع منشورات في الطريق العام أو لصق إعلانات على الجدران، أو الجهر بالدعوة في مكان عام، أو عن طريق الإذاعة والتلفزيون...، ومن ثم فإنه لا يرتكب هذا الاحتيال من يتحدث مع أحد رجال المال على انفراد ليحمله على

---

(1) عقوبة الاحتيال حسب المادة 641 من قانون العقوبات هي الحبس من ثلاثة أشهر إلى سنتين والغرامة من مائة إلى خمسمائة ليرة سورية. وتصبح العقوبة عند مضاعفتها حسب المادة /642/ من قانون العقوبات, الحبس من ستة أشهر إلى أربع سنوات, والغرامة من مائتي ليرة إلى ألف ليرة سورية.

(2) د.محمود نجيب حسني: جرائم الاعتداء على الأموال في قانون العقوبات اللبناني، الطبعة الثالثة، منشورات الحلبي الحقوقية، بيروت، عام 1998، المجلد الأول، ص404. د.علي عبد القادر القهوجي: قانون العقوبات – القسم الخاص، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2001، ص823.

الاكتتاب، أو يتحدث إلى مجموعة محدودة العدد من رجال المال ليدعوهم إلى الاكتتاب، أو يوجه رسائل خاصة إلى كل منهم.

**العنصر الثاني:** وهو يفترض أن يكون الغرض من مخاطبة جمهور الناس الحصول على مال من أجل تمويل عملية إصدار الأسهم أو السندات. ويقصد بالإصدار، الدعوة إلى الاكتتاب في الأوراق المالية المطروحة للتداول، سواء بقصد إنشاء شركة جديدة أم زيادة رأسمال شركة قائمة. ومن ثم فإنه لا يعتبر إصداراً، بيع أسهم أو سندات موجودة من قبل أو رهنها، إذ ليس من شأن ذلك جلب رأسمال جديد للشركة.

وعليه فإن الظرف المشدد للاحتيال يتحقق إذا تضمن الخطاب الموجه إلى الجمهور زعماً بتأسيس شركة وهمية، أو تضمن مبالغة في تقدير أرباح شركة قائمة، أو نشرت بهذا الطريق موازنة مزورة. فهذا الخطاب الذي انطوى على الكذب، كاف ليقوم به الخداع، إضافةً إلى أنه استهدف إيقاع المجني عليهم المحتملين في الغلط[1].

بناءً على ما تقدم، فإن مفهوم الوسيلة العلانية يتوفر في الدعوة للاكتتاب عن طريق الإنترنت، بل إن الإنترنت توفر للمحتالين الاتصال بملايين الضحايا أكثر من أي وسيلة أخرى. وتطبيقاً لذلك، فمن يقوم بطرح أسهم وهمية للاكتتاب عن طريق الإنترنت ليحمل الناس على الاكتتاب بها، فإن الظرف المشدد للاحتيال المنصوص عليه بالمادة 642 من قانون العقوبات ينطبق على فعله.

ولابد من الإشارة هنا بأن المشرع السوري قد تناول مسألة التلاعب بالأوراق المالية في قانونين هما: قانون الشركات الجديد رقم3 لعام 2008، وقانون هيئة الأوراق والأسواق المالية السورية رقم 22 لعام 2005.

---

(1) د. محمود نجيب حسني: جرائم الاعتداء على الأموال في قانون العقوبات اللبناني، الطبعة الثالثة، عام 1998, المرجع السابق، ص405.

لذلك ستتناول النصوص المتعلقة بالتلاعب في الأوراق المالية في كلا القانونين:

## القانون الأول: المادة 203 من قانون الشركات رقم 3 لعام 2008:

تناول المشرع في الفقرة الأولى من المادة 203 من قانون الشركات رقم 3 لعام 2008 العديد من أساليب التلاعب بأسهم الشركات، وعاقب عليها بعقوبة جنحية، فقد نصت هذه الفقرة على ما يلي:

(مع عدم الإخلال بالعقوبة الأشد المنصوص عليها في القوانين الأخرى:

1- يعاقب بالحبس من سنة إلى ثلاث سنوات وبغرامة لا تقل عن ثلاثمائة ألف ليرة سورية ولا تزيد على ثلاثة ملايين ليرة سورية، كل من ارتكب أياً من الأفعال التالية:

أ- إصدار الأسهم أو تسليمها لأصحابها أو عرضها للتداول قبل تأسيس الشركة أو زيادة رأسمالها وفقاً لأحكام هذا القانون.

ب- طرح اكتتابات صورية للأسهم أو قبول اكتتابات فيها بصورة غير حقيقية.

أ- تسديد رأسمال الشركة بشكل صوري.

ب- إصدار سندات قرض وعرضها للتداول بصورة مخالفة لأحكام هذا القانون.

ج- تنظيم ميزانية الشركة وحسابات أرباحها وخسائرها بصورة غير مطابقة للواقع، أو تضمين تقرير مجلس إدارتها أو مديريها أو تقرير مفتشي الحسابات بيانات غير صحيحة بصورة متعمدة.

د– كتم المؤسسين أو أعضاء مجلس الإدارة أو المديرين أو مفتشي الحسابات لمعلومات وإيضاحات يوجب القانون ذكرها، بقصد إخفاء حالة الشركة الحقيقية عن ذوي العلاقة.

هـ– توزيع أرباح صورية أو غير مطابقة لحالة الشركة الحقيقية.

و–قيام الجهة التي قامت بتقدير قيمة المقدمات العينية بتأسيس تقريرها على معلومات تعلم أنها غير صحيحة، أو تضمينه مثل هذه المعلومات.

ز– نشر وقائع كاذبة لحمل الجمهور على الاكتتاب بالأسهم أو بأسناد القرض.

ح– تقديم عضو مجلس الإدارة أو المدير أو مفتش الحسابات، معلومات غير صحيحة في تصريحه المقدم استناداً لأحكام هذا القانون.

ط– قيام عضو مجلس الإدارة أو الشخص المكلف بتمثيل الشركة أو مفتش الحسابات بعمليات التلاعب في أسعار أسهم الشركة في أسواق الأوراق المالية، أو شراء وبيع الأسهم استناداً لمعلومات حصلوا عليها في معرض ممارستهم لوظيفتهم وغير متاحة للعامة، أو نقل هذه المعلومات لأي شخص آخر بقصد إحداث تأثير في أسعار أسهم هذه الشركة).

ومن الملاحظ أن هذه المادة تناولت في الفقرتين /ب و ط/ مسألة طرح اكتتابات صورية للأسهم، أو حمل الجمهور على الاكتتاب بها تحت تأثير نشر الوقائع الكاذبة. وهو ما يدخل أيضاً ضمن نطاق تطبيق الفقرة /ب/ من المادة 642 من قانون العقوبات التي سبقت الإشارة إليها. ولما كانت المادة 203 من قانون الشركات توجب على القاضي الأخذ بالعقوبة الأشد المنصوص عليها في القوانين الأخرى، فإن القاضي الجزائي يكون هنا أمام العقوبتين التاليتين:

**العقوبة الأولى:** عقوبة الحبس من ستة أشهر إلى أربع سنوات، والغرامة من مائتي ليرة إلى ألف ليرة. (المادة 642 من قانون العقوبات).

**العقوبة الثانية:** عقوبة الحبس من سنة إلى ثلاث سنوات، والغرامة لا تقل عن ثلاثمائة ألف ليرة سورية ولا تزيد عن ثلاثة ملايين ليرة سورية. (المادة 203 من قانون الشركات).

ومن الملاحظ أن الحد الأعلى للعقوبة الأولى أشدّ من نظيره في العقوبة الثانية، أما الحد الأدنى للعقوبة الأولى فهو أخف من نظيره في العقوبة الثانية. والسؤال المطروح هنا هو: **أي العقوبتين أشدّ من الأخرى؟**

عالج الفقه هذه الحالة في صدد معرفة القانون الأصلح للمتهم، حيث ذهب الرأي الراجح إلى أنه على القاضي أن يحدد موقفه من المدعى عليه سلفاً، فإذا كان متجهاً إلى تخفيف العقوبة بحقه، وجب عليه أن يأخذ بالقانون الذي هبط بالحد الأدنى. أما إذا كان متجهاً إلى تشديد العقوبة، تعيّن عليه أن يأخذ بالقانون الذي هبط بالحد الأعلى[1].

أما في حالة البحث عن العقوبة الأشد، **فيرى الباحث** أنه يجب على القاضي الأخذ بالعقوبة التي ترتفع بالحد الأعلى، أي العقوبة المنصوص عليها في المادة 642 من قانون العقوبات، والتي تصل إلى الحبس مدة أربع سنوات، لأن في ذلك احترام لإرادة المشرع التي تتجه إلى تشديد العقاب. فالعقوبة التي ترتفع بالحد الأعلى هي التي تؤمن تشديد العقاب على المدعى عليه.

**القانون الثاني: المادتان 17 و18 من قانون هيئة الأوراق والأسواق المالية السورية رقم 22 لعام 2005:**

تناول المشرع في المادة 17 من قانون هيئة الأوراق والأسواق المالية السورية أربعة عشر مخالفة لأحكام هذا القانون، حيث عاقب على بعض هذه المخالفات بعقوبة الحبس لمدة لا تقل عن ثلاثة أشهر ولا تزيد عن ثلاث

(1) د. عبود السراج: شرح قانون العقوبات، القسم العام، منشورات جامعة دمشق,عام 2007، ص 152. د.محمود نجيب حسني: شرح قانون العقوبات اللبناني، القسم العام، المجلد الأول، طبعة ثالثة جديدة (معدلة ومنقحة)، منشورات الحلبي الحقوقية، بيروت، عام 1998، ص 163.

سنوات، وبغرامة مالية لها صفة التعويض، مع عدم الإخلال بالعقوبة الأشد. كما عاقب على البعض الآخر بغرامة مالية فقط (المادة 18).

**فقد نصت المادة /17/ على ما يلي:**

(يعتبر مخالفة لأحكام هذا القانون، كل ما يلي:

1- مخالفة الأنظمة والتعليمات والقرارات الصادرة عن الهيئة وفقاً لأحكام هذا القانون.

2- عدم استجابة أي شخص أو جهة خاضعة لرقابة الهيئة وإشرافها، بتقديم الوثائق أو المستندات اللازمة خلال المدد والمهل المحددة.

3- تقديم معلومات أو بيانات غير صحيحة أو مضللة في أي من الوثائق أو المستندات المقدمة للهيئة.

4- عرض أوراق مالية أو بيعها بالاستناد إلى بيانات أو معلومات غير صحيحة أو مضللة، سواء فيما يتعلق بالحقوق والمزايا التي تمنحها هذه الأوراق، أو حول طبيعة النشاط والأوضاع المالية للشركات المصدرة لهذه الأوراق.

5- استغلال شخص ما بحكم وظيفته أو مركزه لمعلومات داخلية أو سرية تتعلق بأوراق مالية، لتحقيق مكاسب مادية أو معنوية، أو إفشاء هذه المعلومات لغير مرجعه المختص أو القضاء.

6- بث وتوزيع الشائعات أو إعطاء معلومات أو بيانات غير صحيحة أو مضللة حول أية ورقة مالية، بغرض التأثير على سعرها أو سمعة الشركة المصدرة لهذه الورقة.

7- تصديق مدقق الحسابات أو المحاسب على بيانات مالية غير صحيحة أو مضللة، أو مخالفة للمعايير المحاسبية ومعايير التدقيق المعتمدة.

8- اعتماد تحاليل مالية مغرية تتعارض مع المركز المالي للشركة، والقناعات الحقيقية لمكتب الاستشارات المالية والاستثمارية.

9- بيع أوراق مالية أو التصرف بها دون تفويض خطي من مالكها أو دون وجود اتفاقية تخوّله بذلك.

10- عدم توزيع نشرة الإصدار المعتمدة من الهيئة على الجمهور المستثمرين.

11- مخالفة التعليمات الصادرة عن الهيئة بشأن طبيعة المعلومات والبيانات الواجب تضمينها في نشرة إصدار الأوراق المالية.

12- بيع أوراق مالية دون نشرة إصدار معتمدة من قبل الهيئة.

13- تقديم أية خدمات مالية أو استثمارية أو وساطة مالية مرتبطة بالأوراق المالية دون الحصول على ترخيص، أو قبل اعتمادها من الهيئة.

14- أي خداع أو تدليس أو تلاعب يتعلق بنشاط إصدار أو تداول أو انتقال ملكية الأوراق المالية أو أية ممارسة محظورة أو تضليل إعلامي فيما يتعلق بالأنشطة والأعمال المرخص لها من قبل الهيئة).

**أما المادة /18/ فنصت على ما يلي:**

(مع عدم الإخلال بأي عقوبة أشد منصوص عليها في القوانين والأنظمة النافذة:

أ- يعاقب بالحبس لمدة لا تقل عن ثلاثة أشهر ولا تزيد عن ثلاث سنوات، وبغرامة مالية[1]، كل من ارتكب المخالفات المنصوص عليها

(1) راجع المرسوم التشريعي رقم /151/ الصادر بتاريخ 2007/4/5 المتعلق بتحديد الغرامات التي تُفرض على المخالفات المنصوص عليها في المادة /17/ من قانون هيئة الأوراق والأسواق المالية السورية.

في الفقرات /3، 4، 5، 6، 7، 9، 12، 13، 14) من المادة السابعة عشر من هذا القانون.

ب- أما باقي المخالفات فتفرض بحق مرتكبيها غرامة مالية.

ج- يُحكم بالغرامات المبينة في الفقرتين /أ و ب/ لصالح الهيئة بصفة تعويض.

د- يعتبر أعضاء مجلس الإدارة وأعضاء هيئة المديرين والشركاء المتضامنون والموظفون المعنيون لدى الشخص الاعتباري المخالف، مسؤولين عن المخالفة ما لم يثبت عدم علمهم بارتكابها).

**ويرى الباحث** أن المشرع كان موفّقاً في الإحاطة بمختلف الأساليب الاحتيالية المتعلقة بالأوراق المالية، وخاصة ما يتعلق بالنص العام الذي أورده في الفقرة /14/ من المادة 17 من هذا القانون، والتي تطال مختلف أشكال الاحتيال التي يمكن ارتكابها في مجال إصدار أو تداول أو انتقال ملكية الأوراق المالية، أو أي تضليل إعلامي يتعلق بهذه الأنشطة.

وبناء على ما تقدم، يمكن أن نميّز في صدد الاحتيال عن طريق الأوراق بين أمرين:

**الأمر الأول:** إذا كان الاحتيال يتعلق بالاكتتاب على الأسهم أو إصدارها، فإن نص المادة /642/ من قانون العقوبات هو الواجب التطبيق، لأنه النص الأشد كما رأينا.

**الأمر الثاني:** إذا كان الاحتيال يتعلق بتداول الأسهم (أي البيع والشراء)، أو التضليل الإعلامي للتأثير على أسعار هذه الأسهم، فإن نص المادة /17/ من قانون هيئة الأوراق المالية رقم /22/ لعام 2005 هو الواجب التطبيق، لأن عقوبة هذه الأفعال هي الحبس لمدة لا تقل عن ثلاثة أشهر ولا تزيد عن ثلاث

سنوات والغرامة المالية (المادة 18)، وهذه العقوبة هي أشدّ من العقوبة المنصوص عليها للاحتيال البسيط في المادة /641/ من قانون العقوبات.

ولا بدَّ من الإشارة هنا إلى أن جميع أساليب الاحتيال المتعلقة بالأوراق المالية يمكن ارتكابها عبر الإنترنت، كإصدار الأسهم أو تداولها أو التضليل الإعلامي للتأثير على أسعارها..، ففي جميع هذه الحالات يجب مراعاة القواعد المتقدمة المشار إليها.

وفي إحدى القضايا الحديثة في سورية، التي تتلخص وقائعها بأن شركة وهمية للوساطة والاستثمارات المالية، اتخذت لنفسها مقراً في دمشق، وموقعاً على الإنترنت، وادعت بأنها وكيلة لشركة "cib" الأمريكية للأوراق المالية، وقد استجرت هذه الشركة مبالغ مالية كبيرة من عدة أشخاص، بحجة فتح رصيد باسم كل عميل، وبرقم خاص به، لشراء وبيع الأسهم في البورصة العالمية، حيث يستطيع العميل الدخول إلى موقع الشركة على الإنترنت، وبيع وشراء الأسهم بعد أن يقوم بإدخال الرقم الخاص به.

وقد فوجئ جميع العملاء بأنهم وقعوا ضحية عملية احتيال، عندما قاموا بمراجعة مقر الشركة لسحب المبالغ التي تم دفعها سابقاً، فتبين لهم – حسب جواب موظفي الشركة– بأن الأسهم التي تم شراؤها قد هبطت أسعارها، وأن جميع هذه المبالغ قد ذهبت مع الريح. وبعد إجراء التحريات تبين أن هذه الشركة غير مرخصة، ولا يوجد لدى القائمين عليها ما يثبت بأنه تم شراء أسهم للعملاء أصلاً. ولدى تفتيش حواسيب هذه الشركة تم ضبط العديد من البرامج المخصصة لمتابعة مؤشرات البورصة عبر الإنترنت، إضافةً إلى ضبط عدة نسخ من الوثائق الشخصية للعديد من العملاء والضحايا من جنسيات مختلفة.

وقد قامت النيابة العامة بتحريك الدعوى العامة بحق القائمين على هذه الشركة الوهمية بجرم ممارسة الوساطة المالية المرتبطة بالأوراق المالية دون

ترخيص حسب المادة 18 من قانون هيئة الأوراق والأسواق المالية السورية رقم 22 لعام 2005، وجرم الاحتيال وفق المادة 642 عقوبات[1].

## رابعاً- الاحتيال بأسلوب انتحال الشخصية phishing:

يمكن تعريف انتحال الشخصية أو الصفة بأنه:

(شكل من أشكال سرقة الهوية على الإنترنت، باستخدام بريد إلكتروني مغشوش لإغواء المتلقين، من أجل أن يتصلوا بمواقع إلكترونية احتيالية، وذلك بغية خداعهم وجعلهمُ يفشون بياناتهم الشخصية والمالية، مثل أرقام بطاقات الائتمان وكلمات السر وأرقام الضمان الاجتماعي..)[2].

والمثال على هذه العملية عندما يستلم أحد الأشخاص رسالة إلكترونية تتضمن طريقة اتصال بموقع إلكتروني (link)، فعندما ينقر المستلم على هذا الربط (link) فإنه يدخل إلى موقع مثل موقع e-bay، ولكن هذا الموقع يكون مزيفاً، إلا أنه وبالتفحص الجيد يمكن أن يظهر أن عنوان الصفحة مختلف عن الموقع الحقيقي. ولكن الضحية لن يلاحظ هذا الفرق، وسوف يقوم بإعطاء معلومات عنه، مثل كلمة السر وعنوان البريد. ومن أمثلة هذا الأسلوب، أن شخصاً يدعى "ويليام جاكسون" استلم رسالةً إلكترونيةً تظهر أنها من موقع paypal، وهذه الرسالة تحذره بأن حسابه سوف يغلق ما لم يجدده بمعلومات مالية محددة، وكان يوجد في هذه الرسالة ربط (link) بالموقع الذي يستطيع من خلاله تجديد هذه المعلومات. وقد قام "جاكسون" بإدخال أرقام بطاقة الإئتمان والحسابات المصرفية وأرقام الضمان الاجتماعي الخاصة به،

(1) القضية رقم موجوداً 12823/ م تاريخ 20/ 7/ 2008 سجلات النيابة العامة في دمشق.

(2) Micheal kunz and Patrick Wilson, op-cit, p-15.

ومعلومات شخصية أخرى، وانتهت هذه العملية الاحتيالية بخسارة "جاكسون" مئات الدولارات[1].

كما تمّ تجريم الأخوين "ستيفينز" من "هيوستن" لقيامهما بتنصيب موقع إلكتروني مزيف لجيش الانقاذ Salvation Army، وقاما بجمع أكثر من 48000 دولار باسم جمعية إعصار كاترينا[2].

وفي قضية أخرى، ورد بلاغ إلى إدارة جرائم الحاسوب بوزارة الداخلية المصرية عبر البريد الإلكتروني، من إحدى شركات مكافحة جرائم الاحتيال العالمية، التي تمثّل قانوناً أحد البنوك البريطانية الكبرى، بوجود موقع مزيف على الإنترنت لهذا البنك البريطاني، يستخدم لخداع عملاء البنك وجمع المعلومات عنهم، والاستيلاء على أرصدتهم بطريقة احتيالية.

ونتيجة البحث والمتابعة، تم إلقاء القبض على طالب بكلية الهندسة مقيم بالإسماعيلية ،لإنشائه هذا الموقع المزيف الذي يحمل نفس مواصفات الموقع الرئيسي للبنك، وقد استطاع الطالب خداع عملاء البنك في الخارج، كما استطاع بمعاونة أشخاص مقيمين في أوربا الشرقية وروسيا تحويل بعض أرصدة العملاء، عن طريق شركات تحويل الأموال وتقسيمها فيما بينهم، وقد ارتكب هذا الطالب جريمته عن طريق مقهى إنترنت عائد لوالده في الإسماعيلية[3].

## خامساً– الاحتيال عن طريق البريد الإلكتروني:

هناك العديد من أشكال الاحتيال عبر البريد الإلكتروني، ومن أبرز هذه الأشكال، البريد الإلكتروني **النيجيري** Neigeran letter fraud ، وفيه يتلقى

---

(1) Micheal kunz and Patrick Wilson, op-cit, p- 16.

(2) IC3, op-cit, p-15.

(3) د. محمد الشناوي: المرجع السابق، ص97.

الضحية رسالةً إلكترونيةً من شخص يدّعي أنه الوريث لابن رئيس دولة نيجيريا الميت، وأنه سيرث ملايين الدولارات المخبأة في عدة حسابات في جميع أنحاء العالم، وأن مستلم هذه الرسالة سيحصل على جزء من هذه الثروة، وكل ما يطلب منه هو آلاف من الدولارات كأجر للمحامي من أجل الحصول على الثروة، والأشخاص الذين وقعوا ضحية لهذه الجريمة أرسلوا نقودهم ولم يحصلوا على الثروة المتوقعة[1].

ومن الرسائل الشهيرة أيضاً، رسالة تصل من شركة تطلق على نفسها اسم **E. A. A. S Lottery Watergate inc**، ومركزها "جوهانسبورغ"، وهي رسالة محترمة جداً، وكأنها صادرة فعلاً عن شركة تجارية، حيث تُعلمك بأنك ربحت 5.2 مليون دولار، وتطلبُ منك تأكيد نيتك باستلام المبلغ، كما تطلبُ منك المعلومات التالية :

1- الاسم الثلاثي. 2- عنوان المسكن. 3- رقم الهاتف. 4- رقم الفاكس. 5- صورة عن الهوية.

وعندما ترسل هذه المعلومات، يرسلون إليك فاتورة باسمك تطالبك بمبلغ معين لقاء خدمات بريدية، وإذا أعطاهم الشخص المعني رقم حسابه أو رقم بطاقة الائتمان، فسوف يجد مفاجأة كبيرة في كشف المصرف آخر الشهر. والأكثر إثارة في هذا النوع من الرسائل هو مدى جديته، فقد طلبت إدارة هذه الشركة الوهمية من أحد الأشخاص ألا يرسل أي أوراق عبر البريد، وإنما يمكنه أن يحضرها بنفسه عند زيارته إلى مكاتب الشركة المنتشرة في 11 دولة بين آسيا وأوروبا والولايات المتحدة[2].

---

(1) Micheal kunz and Patrick Wilson, op-cit, p- 12.

(2) محمد عبيد الكعبي: الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، رسالة ماجستير مقدمة إلى جامعة القاهرة، عام 2004، ص176.

ومن أساليب الاحتيال عن طريق البريد الإلكتروني أيضاً، ما يعرف باسم **الرسائل المتسلسلة** chain letters أو طريقة الهرم.

وتتم هذه الطريقة بإرسال بريد إلكتروني إلى الغير يتضمن أسماء عدد قليل من الأشخاص، واحداً تلو الآخر على شكل قائمة ، وعلى مستقبل الرسالة أن يرسل مبلغاً معيناً عبر البريد العادي إلى عنوان الشخص الوارد اسمه في أعلى القائمة، ثم يقوم بتسجيل اسمه في أسفل القائمة بعد أن يحذف الاسم الأول الذي تم إرسال المال له، ثم يقوم بإرسال الرسالة إلى عدة أشخاص آخرين، ليقوموا بنفس الخطوات. والهدف من هذه العملية هو أن يصل اسم المرسل إليه المدرج في أسفل القائمة إلى الأعلى، أي إلى مرتبة الاسم الأول، وهنا سيتلقى مبالغ مالية من عدد غير محدد من الأشخاص الذين ساهموا في هذه السلسلة. إلا أنه سيكتشف أنه كان ضحية عملية احتيال، وأن الأسماء جميعها ربما تكون لشخص واحد قام بالاستيلاء على جميع الأموال[1].

ومن أشكال الاحتيال عبر البريد الإلكتروني، **أسلوب العروس الروسية.** ويعرف بهذا الاسم، لأن مرتكبي هذا الأسلوب هم رجال من روسيا في أغلب الأحيان. ومن أشهر المحتالين في هذا المجال، رجل روسي في الأربعين من عمره، اسمه "روبرت ماك كوي" Robert Mc Coy، الذي كان يتعرف على ضحاياه، عن طريق الإعلانات الشخصية التي ينشرها عن نفسه عن طريق بعض المواقع الإلكترونية، مثل America on line . وقد كان "روبرت" ينتحل في رسائله الإلكترونية صفة امرأة روسية تبحث عن الحب، ويقوم بإرسال صور لعارضة جميلة إلى ضحيته. وتستمر هذه العلاقة لفترة من الزمن، ثم يقوم بإخبار الضحية بأن الفتاة الجميلة ترغب برؤية عشيقها، وتحتاج إلى مبلغ /1800/ دولار أميركي لتغطية مصاريف التأشيرة وتذكرة الطائرة.

---

(1) محمد عبيد الكعبي: المرجع السابق، ص177.
Micheal kunz and Patrick Wilson, op-cit, p-15

وبعد أن يتم إرسال هذا المبلغ، وفي اليوم الذي يتوقع فيه الضحية وصول الفتاة الجميلة، تصله رسالة منها تدعي فيها ، أن هناك مشكلة تتعلق بالقوانين الروسية الحديثة التي لا تسمح لها بالمغادرة إلاّ إذا كان معها /1500/ دولار أميركي نقداً، وبعد أن يرسل الضحية هذا المبلغ. يتم تجاهل رسائله الإلكترونية، أو تُعاد إليه رسائله لأن حسابات المشتركة الروسية قد أُغلقت. عندها يعلم أنه وقع ضحية عملية احتيال.

وبعد إلقاء القبض على "ماك كوي"، اعترف بالاحتيال على أكثر من /250/ رجلاً، كان معظمهم من الولايات المتحدة الأميركية، وحصل منهم على ما يزيد على مليون دولار أميركي، وقد حُكم عليه بالسجن مدة خمس سنوات[1].

## سادساً- الاحتيال المهني:

من أكثر صور الاحتيال عبر الإنترنت هو الاحتيال المهني، أي الاحتيال الذي يرتكبه العاملون داخل المؤسسة.

وحسب ما جاء على لسان السيد "هاورد كوس" Haward Cox ، نائب المستشار في مكتب التفتيش في الخدمة البريدية بأمريكا:

(إن بعض الموظفين الداخليين يستخدمون الإنترنت لكي يصلوا إلى بيانات ليست ذات صلة بوظائفهم، وبعد ذلك يستخدمونها على نحو سيئ لأهدافهم الشخصية، ويعّرضون المؤسسة للخطر. وهؤلاء الناس يكونون عادة على حافة الطرد من العمل، أو أنهم غير سعداء في أعمالهم)[2].

---

(1) هذه القضية متوفرة على الموقع www.russian-detective. com/scams وقضية أخرى:
Joseph T. wells, Computer Fraud Casebook, Published by John Wiely @sons. Inc, Hoboken, New Jersey, 2009, P 35 - 45.

(2) Joseph W. Kotar, op- cit, p- 48.

وهناك عدة دراسات أجريت على الاحتيال المرتبط بالتلاعب باليبانات، وقد تبين أن معظم حالات هذا الاحتيال، قد تم عن طريق أشخاص من داخل المؤسسات المجني عليها، وأن نسبة هذه الحالات قد يصل إلى ثلاثة أرباع الحالات التي تم دراستها، حتى أن البعض يطلق على هذا النوع من الاحتيال اسم "**الجريمة الداخلية**" in-house offence، وذلك إشارة إلى حدوثه داخل المؤسسة المجني عليها بواسطة أحد المنتمين إليها[1].

## **سابعاً- احتيال الاتصالات** Telecommunications Fraud:

أصبح الاحتيال في مجال الاتصالات من المسائل الحساسة في السنوات الماضية. وهذا لا يعني أن الاحتيال في الاتصالات ظاهرة حديثة، ولكن أصبحت مؤسسات الاتصالات والمجتمع برمته يرى من الضروري ملاحقة هذه الأنشطة الاحتيالية، بعد أن كانت الخسارات الناجمة عنها يتم امتصاصها في كثير من الأحيان.

والواقع أن صناعة الاتصالات قد تطورت في العشرين سنة الماضية بصورة ملحوظة، وذلك بسبب الانتشار الواسع للتكنولوجيا، مثل أجهزة الموبايل والانتشار الواسع للمقاسم الشخصية الخاصة (PABX)، وتطور إرسال الصوت والفاكس عبر شبكة الإنترنت، وتقنية الجيل الثالث للخلوي (3g)، وتطور البنية التحتية لأنظمة الاتصال الخلوي العالمية (UMTS) وغيرها.

وقد رافق هذه التطورات التقنية ارتفاع مستوى الاحتيال في مجال خدمات الاتصالات، وأصبح من الممكن خرق الحدود الوطنية من قبل المجرمين، مما يعرقل عمل الجهات المختصة.

---

(1) د. نائلة قورة: المرجع السابق، ص427.

والحقيقة أن هناك أشكالاً مختلفة من الاحتيال الذي يرتكب في مجال الاتصالات، وأبرز هذه الأشكال:

## أ- الاحتيال الهاتفي البعيد المسافة عبر الإنترنت:

وهو يعرف بـ Long Distance Telephone Fraud Via The Internet، وهو من أنواع الاحتيال الحديثة نسبياً. وفيه تقوم الضحية بإنزال برنامج من شبكة الإنترنت، على أنه برنامج له خواص مميزة، ويقوم البرنامج بتنصيب نفسه تلقائياً، وبمجرد انتهاء التنصيب، يقوم البرنامج بالدخول إلى المودم ويقطع الاتصال مع مزود خدمة الاتصال، ثم يقوم بإعادة الاتصال بمزود خدمة اتصال آخر في مكان بعيد، حيث تكون كلفة الاتصالات من الدرجة الأولى، أي أنها عالية الكلفة. وأكثر ما تؤثر هذه الطريقة بالاحتيال على الأشخاص الذين يستخدمون نظام dial up للدخول إلى الإنترنت[1].

ففي إحدى القضايا التي عُرفت باسم ( love ball )، والتي تتلخص بأنه في عام 2000 قُدم إلى الشرطة البرتغالية العديد من الشكاوى حول استلام بعض الأشخاص لفواتير تلفونية عالية جداً، مقابل خدمة الهاتف من الدرجة الأولى[2] التي لم يقوموا باستخدامها. ونتيجة التحقيقات، تبين بأن جميع المشتكين كانوا قد دخلوا إلى مواقع إباحية عبر الإنترنت سبق وأن تم الإعلان عنها عبر الشبكة. حيث تتم عملية الاحتيال عندما يدخل أحد الأشخاص إلى هذا الموقع، فُيطلب منه تحميل برنامج يسمح له برؤية الصور الإباحية، وهذا البرنامج هو في الحقيقة عبارة عن برنامج يجري اتصالات هاتفية، ويُنصب

---

(1) Robin Bryant: Investigating Digital Crime, John Wile& Sons, ltd, 2008, p- 159.

(2) تسمى هذه الخدمة في مؤسسة الاتصالات السورية، بخدمة التعرفة المخصوصة .

نفسه على حاسوب المشترك على شكل أيقونة على سطح المكتب، وعند الضغط على هذه الأيقونة مرتين يجري بسرية ما يلي:

1- إيقاف تشغيل المودم الصوتي.
2- وقف اتصال المستخدم بشبكة الإنترنت.
3- إعادة اتصال المستخدم بمزود خدمة إنترنت آخر، ولكن من خلال خدمة الهواتف من الدرجة الأولى.
4- السماح بالدخول إلى المواد المعروضة.

وعندما يقوم المستخدم بالخروج من الموقع، يقوم بتخزين هذه العمليات دون علم المشترك، وإعادة الاتصال بمزود الخدمة الأول، وتكون كلفة الدخول إلى المواقع الإباحية حوالي 190 جنيهاً استرلينياً بالساعة، يحصل عليها الأشخاص الذين قاموا بالمخطط الاحتيالي.

وقد تم إلقاء القبض على المحتالين، وهم عبارة عن أربعة أشخاص من جنسيات مختلفة (هولندي- مكسيكي- سلوفاني- برتغالي). وقد قدرت خسائر هذا الاحتيال بنحو 4 ملايين جنيهاً استرلينياً حصل عليها المحتالون قبل الاعتقال[1].

## ب- الاحتيال عن طريق الخدمة غالية الثمن Premium rate service Fraud:

وهنا يكون ضحايا الاحتيال إما المشتركين أو مزودي خدمة الاتصالات، حيث يتم إقناع هؤلاء الضحايا بالاتصال بأرقام من خدمة الدرجة الأولى للحصول على جوائز وهمية. وهنا يتم تحويل مودم الحاسوب للاتصال إلى الخارج، وإجراء مكالمات بعيدة المدى و باهظة الكلفة[2].

---

(1) Robin Bryant, op- cit, p- 80.

(2) Robin Bryant, op- cit, p- 161.

ففي إحدى القضايا التي تم التحقيق بها، قام مجموعة من المحتالين بإرسال بريد إلكتروني لآلاف الأشخاص، يتضمن بأن كل مستلم لهذا البريد سيدفع له مبلغ ابتداءً من 250 إلى 899 دولاراً، عن طريق بطاقة الائتمان الخاصة به، وقد طُلب من الضحايا في هذا البريد الإلكتروني الاتصال بالرقم 767 من أجل أي استفسار، ولم يكن الضحايا يعلمون أن 767 هو رمز الاتصال بمنطقة "دومونيكا" في جزر الهند الغربية، وعندما اتصل هؤلاء الضحايا بالرقم المذكور تم وصلهم بخدمة التسلية التي تحمل مضمون جنسي (Audio text)، ومن ثم كان عليهم دفع فواتير غالية الثمن[1].

## ج- احتيال المقاسم الداخلية الخاصة PABX fraud:

أنظمة PABX[2] هي عبارة عن مقاسم داخلية خاصة، غالباً ما تستخدم في الشركات والإدارات وغيرها. وهي أنظمة معقدة تعتمد على لوحة مفاتيح متصلة بالحاسوب.

ويتم وصل هذا النظام بشبكة الهاتف الثابتة العامة PSTN[3]، حيث يتم تزويد المؤسسة بخطوط مكالمات داخلية، ومن ثم يمكن تحويل المكالمات الواردة إلى الجهة المطلوبة في الشركة. ومن خواص هذا النظام أيضاً أنه يسمح للمستخدم المخول بالدخول إلى الشبكة الداخلية من خارج الشركة، وإجراء مكالمات هاتفية على حساب الشركة[4].

---

(1) On line fraud and crime, op- cit, p- 23.

(2) وهو اختصار لـ .Private Automatic Branch exchange د.عبد الحسن الحسيني: المرجع السابق, ص599.

(3) وهو اختصار لـ .Public switched telephone Network د.عبد الحسن الحسيني: المرجع السابق, ص663.

(4) Robin Bryant, op- cit, p- 163.

وبالرغم من أن هذه الأنظمة توفر المرونة لمستخدميها، إلا أنها تعرض الشركات للاقتحام من قبل الهكرة، حيث يستطيعون الدخول إلى مقسم الشركة واستخدامه لإجراء مكالمات ذات كلفة عالية. وهكذا يتم الاحتيال على الشركة، لأنها سوف تتلقى فواتير هاتفية عالية من غير أن تعرف أية معلومات عن المجرمين[1].

وهناك العديد من التهديدات التي يمكن أن تتعرض لها المؤسسات التي تستخدم نظام المقسم الداخلي الخاص (PABX) ومنها:

- سرقة الخدمة.
- مراقبة حركة هذا النظام، التي تسمح بجمع معلومات عن الشركة.
- عدم معرفة من هاجم الخدمة.
- تعديل البيانات.
- إفشاء المعلومات عن طريق التنصت على المكالمات.
- الدخول غير المخول وإجراء مكالمات دولية.

ولابد من الإشارة إلى أن القضايا المتعلقة بهذا النوع من الاحتيال قد تسببت في خسارات مادية كبيرة تصل إلى ملايين الدولارات.

وأخيراً وبعد أن انتهينا من دراسة الصور العامة للاحتيال عبر الإنترنت، سنشرع في دراسة الاحتيال عن طريق بطاقات الائتمان في المطلب القادم.

---

(1) Robin Bryant, op- cit, p- 165.

## المطلب الثاني

## الصورة الخاصة للاحتيال عن طريق بطاقات الائتمان

شاع في الآونة الأخيرة استعمال بطاقات الائتمان على اختلاف أنواعها، وذلك من أجل التيسير على الأفراد في معاملاتهم المالية. وقد ساعدت الثورة المتسارعة لنظم الحوسبة ونظم الاتصالات وخاصة الإنترنت على نقل المعلومات عبر العالم خلال لحظات معدودات، فأصبحت بطاقات الائتمان أكثر وسائل الدفع استخداماً وانتشاراً محلياً وعالمياً، فقد ربطت الإنترنت المصارف بنقاط البيع الإلكترونية، وأجهزة سحب النقود أينما وجدت.

وقد صاحب انتشار هذه البطاقات وتزايد حجم التعامل بها، نمواً مضطرداً في الجرائم المرافقة لاستخدامها، كتزويرها وسرقتها والاحتيال بواسطتها، وغير ذلك من أشكال الإجرام.

والواقع أن الاحتيال بواسطة بطاقات الائتمان لا يشكل دائماً احتيالاً عبر الإنترنت، إلا إذا كان هناك ولوجٌ إلى الإنترنت عند استخدامها، كالشراء ببطاقة ائتمانية مزورة أو مسروقة عبر الإنترنت، أو عند استخدام بطاقة ائتمانية مزورة أو مسروقة في سحب النقود من الصراف الآلي، إذا كان هذا الأخير موصولاً مع المصرف المصدر للبطاقة عبر الإنترنت، أو إذا استخدمت هذه البطاقات في الشراء من التجار الذين يستخدمون أجهزة إلكترونية موصولة عبر الإنترنت مع المصرف المصدر للبطاقة، والتي تستخدم عادةً للتأكد من صلاحية البطاقة ورصيدها....الخ.

**وغني عن البيان** أن ما يتعلق بموضوع البحث، هو ذلك النوع فقط من احتيال البطاقات الائتمانية المرتبط بالإنترنت.

وقبل الدخول في صور هذا الإجرام لابد لنا من التعرف على ماهية بطاقة الائتمان وأنواعها، وأساليب الاستيلاء على أرقامها. وهذا ما سنبحثه على التتالي:

## أولاً- ماهية بطاقة الائتمان[1]:

هي بطاقة مستطيلة الشكل ذات أبعاد قياسية، مصنوعة غالباً من مادة البلاستيك، ومسجل على وجهيها مجموعة من البيانات الأساسية وهي:

1- اسم وشعار المنظمة الدولية (فيزا Visa، ماستر كارد Master Card....)

2- اسم وشعار المصرف المصدر: وهو المصرف الذي يحق له إصدار البطاقات، مثل المصرف التجاري السوري الذي يقوم بإصدار بطاقات الفيزا في سورية.

3- رقم البطاقة: وهو الرقم المطبوع على صدر البطاقة، وهو رقم تعريف مكون من 16 خانة، ولا يُعطى عشوائياً، وإنما وفقاً لمعادلة رياضية معينة، ويسمى هذا الرقم (pan)[2].

4- اسم حامل البطاقة.

5- تاريخ الإصدار.

6- تاريخ الصلاحية.

7- صورة حامل البطاقة في بعض أنواع البطاقات.

---

(1) د. جميل عبد الباقي الصغير: الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة، دار النهضة العربية- القاهرة، عام 2003، ص12. وائل الدبيسي: البطاقة المصرفية، مطبعة صادر- بيروت، عام 2004، ص33 .

Robin Bryant, op- cit, p- 136 .

(2) وهو اختصار لـ Primary account Number

8- الشريط الممغنط: وهو شريط ممغنط يقع على ظهر البطاقة وعلى طولها، مسجل عليه بيانات غير مرئية يمكن قراءتها بواسطة أجهزة الصراف الآلي ATM ،أو عن طريق نقاط البيع التي تتضمن آلة إلكترونية تعرف بـ POS مخصصة لذلك[1]. وهذه البيانات هي التي يحتاجها الحاسوب للتعرف على رقم البطاقة والحد المسموح به للسحب، والرقم الشخصي، والتواريخ والرموز الأخرى الخاصة بالمعاملات التجارية.

9- شريط التوقيع: وهو شريط يقع على ظهر البطاقة ، حيث يقوم حامل البطاقة بالتوقيع عليه أمام موظف المصرف مصدر البطاقة عند تسلمه لها. والفائدة من وجود توقيع الحامل على هذا الشريط هي تمكين التاجر المتعامل مع حامل البطاقة من التأكد من هوية هذا الأخير عن طريق مضاهاة التوقيع الموجود على البطاقة مع توقيع الحامل أمامه.

10- رقم التعريف الشخصي: وهو رقم سري لا يظهر على البطاقة، ويتكون عادة من أربع خانات، ويرمز له بـ pin[2]، ويسلم هذا الرقم للعميل في ظروف مغلق عند استلامه للبطاقة، وذلك ليستخدمه عند السحب من الصراف الآلي، أو عند الشراء من نقاط البيع الإلكترونية. ويعد هذا الرقم صورة مبسطة من صور التوقيع الإلكتروني.

ويمكن التمييز هنا بين نوعين من البطاقات البلاستيكية حسب طريقة تصنيعها ، هما:

**أ- البطاقة الممغنطة التقليدية** Swipe Card:

وهي البطاقة المغناطيسية التي تكون فيها المعلومات مخزنة على الشريط الممغنط الذي أشرنا إليه سابقاً .

---

(1) ATM هو اختصار لـ Automatic Teller Machine والمقصود بها جهاز الصراف الآلي، أما POS فهو اختصار لـ Point Of Sale أي نقطة البيع.

(2) وهو اختصار لـ Personal Identification Number

**ب- البطاقات الذكية Smart Card:**

هذه البطاقات تشبه الحواسيب المصغرة، لأنها تقوم بعدة عمليات حسابية، وهي عالية الأمان ولا يمكن تزويرها.

ويمكن التمييز بين نوعين من هذه البطاقات، فهناك بطاقات ذكية تحوي على بطاقة ذاكرة، وبطاقات ذكية أخرى تحوي على رقاقة معالجة.

أما البطاقات الذكية ذات الذاكرة، فهي تحتفظ بالمعلومات على ذاكرة قابلة لإعادة الكتابة. ومن أمثلة هذه البطاقات، بطاقات الهواتف العادية التي تستعمل في الهواتف العمومية، وفيها تقوم الذاكرة بتسجيل الزمن والمبلغ المتبقي في كل مرة يتم استعمالها.

أما البطاقات الذكية ذات الرقاقة، فهي أكثر تعقيداً، وهي تحتوي على معالج يتضمن ذواكر حية وساكنة Rom and Ram، ومن أمثلة هذه البطاقات، بطاقات الائتمان والديون [1].

**ثانياً- أنواع بطاقات الائتمان[2]:**

يمكن تقسيم بطاقات الائتمان حسب وظائفها إلى الأنواع التالية:

**أ- بطاقات سحب النقود:**

جميع بطاقات الائتمان تتمتع بوظيفة سحب النقود، إلا أن بعض أنواعها تقتصر على هذه الوظيفة، وقد تخول هذه البطاقة حاملها وظيفة سحب النقود داخل القطر الواحد، أو سحب النقود في الخارج، وذلك ضمن الحد الأقصى

---

(1) Robin Bryant, op- cit, p- 134.

(2) د. نائلة قورة: المرجع السابق، ص508 . وائل الدبيسي: المرجع السابق، ص34. د. جميل عبد الباقي الصغير: الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة ، المرجع السابق, ص15. د.الفتاح بيومي حجازي: التجارة الإلكترونية وحمايتها القانونية، دار الفكر الجامعي، الإسكندرية، عام 2004، الكتاب الأول، ص111.

المحدد المسموح بسحبه يومياً أو أسبوعياً. ويسجل المبلغ المسحوب في الجانب المدين من حساب العميل مباشرة (on- line).

**ب- بطاقات الوفاء Debit Card:**

وهي البطاقة التي تسمح لحاملها وفاء ثمن السلع والخدمات التي يحصل عليها من التجار المتعاملين بها دون حاجة للوفاء نقداً. فبواسطة هذه البطاقة يستطيع التاجر أن يستوفي ثمن السلع أو الخدمات عن طريق المصرف المصدر للبطاقة بطريقتين : إحداهما مباشرة والأخرى غير مباشرة.

ففي الطريقة غير المباشرة ، يقدم فيها العميل بطاقته إلى التاجر، الذي يقوم بالحصول على بيانات البطاقة من خلال تمريرها على آلة يدوية، تحتوي على ثلاثة إشعارات بيع، ثم يقوم العميل بالتوقيع على هذه الإشعارات أو الفواتير، حيث يتم إرسال إحدى هذه النسخ إلى مصرف العميل لتسديد قيمة المشتريات.

أما الطريقة المباشرة، فيقدم فيها العميل بطاقته إلى التاجر، حيث يمرر هذا الأخير البطاقة على آلة إلكترونية ترتبط بالمصرف الذي يتعامل معه ، وذلك من أجل التأكد من وجود رصيد كافٍ للعميل في المصرف ، حتى يستطيع التاجر الحصول على قيمة المشتريات. وهنا لا تتم هذه العملية إلا بعد قيام العميل بإدخال رقمه السري في هذه الآلة، فإذا كان رصيد العميل كافياً تتم عملية التحويل مباشرة من حساب العميل إلى حساب التاجر عن طريق عمليات حسابية في مصرف كل منهما، وإلا ترفض العملية.

وتنقسم بطاقات الوفاء حسب علاقة حامل البطاقة بمصدرها إلى نوعين، هما:

**بطاقات الاستيفاء الفوري**، وهي بطاقة لا يستفيد الحامل فيها من مهلة للوفاء، ويكون دور البطاقة هنا أداة وفاء فقط، إذ تتطلب هذه البطاقة أن يقوم

حاملها بتزويد حسابه برصيد كافٍ دائماً، لأن استيفاء ما يحصل عليه الحامل من سلع أو خدمات يتم فوراً من حسابه دون انتظار، أي دون منح مهلة للوفاء.

أما النوع الثاني فهو **بطاقات الاستيفاء المؤجل**، وهي بطاقات تُستخدم كأداة وفاء وأداة ائتمان، حيث تسمح للحامل بوفاء ثمن ما حصل عليه من سلع وخدمات مستفيداً من مهلة زمنية، وهي الفترة الواقعة بين تاريخ تنفيذ المشتريات وتاريخ الوفاء. وهذه المهلة لا تتعدى عادة ستة أسابيع.

**ج- بطاقات السداد المؤجل أو بطاقات الائتمان** Credit Card[1] **أو بطاقات الاعتماد:**

وهي تسمح لحاملها باستعمال ائتمان في حدود الاتفاق المبرم بينه وبين المصرف المصدر. فبدلاً من أن يقوم حاملها بتسوية حسابه فوراً، فإنه يستطيع أن يسدد ثمن مشترياته على دفعات خلال أجل متفق عليه مع المصرف، وذلك في حدود مبلغ مكشوف معين مسبقاً. فحامل هذه البطاقة يُفترض أن يكون مديناً، إلا أنه في حاجة إلى الحصول على سلع وخدمات يقوم المصرف بتسويتها مع التاجر، ثم يسترد ما دفعه من حامل البطاقة بعد ذلك.

والجهات المصدرة لهذه البطاقات تحصل على فوائد مقابل توفير اعتماد لحاملها. ولذلك فهذه البطاقات أداة ائتمان حقيقية، ويتحدد هذا الائتمان بحد أقصى لكل حامل تبعاً لائتمانه الشخصي. والمصارف لا تمنح هذه البطاقات إلا بعد التأكد من ملاءة العميل أو الحصول منه على ضمانات عينية أو شخصية كافية.

---

(1) يطلق معظم الفقهاء مصطلح بطاقات الائتمان بصفة عامة على جميع أشكال البطاقات على اختلاف أنواعها، على الرغم من أن بطاقة الائتمان هي واحدة من هذه الأنواع، ولقد آثر الباحث أن يستعمل ذات المصطلح الذي درج الفقه على استعماله في هذا المضمار.

**د- بطاقات ضمان الشيكات** Cheque Guarantee Card:

يقتصر عمل هذه البطاقة على ضمان وفاء الشيكات، حيث يقوم التاجر بتدوين بياناتها الرئيسية على ظهر الشيك، بعد التأكد من تاريخ الصلاحية، وأن الشيك والبطاقة يحملان نفس اسم المصرف، ونفس رقم الحساب، ونفس التوقيع. ويقتصر الضمان الذي تقدمه هذه البطاقة للتاجر على حدود معينة يجب عليه عدم تجاوزها، وإلا سقط الضمان عن كامل المبلغ.

و بعد أن ذكرنا أنواع بطاقات الائتمان والمزايا التي تقدمها، لابد لنا من الإشارة إلى أنه يمكن استخدام بطاقات الائتمان للحصول على السلع والخدمات عن طريق الإنترنت؛ فحامل البطاقة يمكن أن يدخل إلى الموقع الإلكتروني للمتجر المرغوب فيه، ثم يقوم باختيار السلع المراد شراؤها، وعند ذلك يظهر على الشاشة نموذج يتضمن خانات فارغة متعلقة ببيانات بطاقة الائتمان، حيث يقوم المشتري بملء هذه الخانات بالبيانات المتعلقة ببطاقته وعنوانه، ثم يتم استيفاء قيمة السلع من بطاقة الائتمان، وإرسال هذه السلع إلى عنوان المشتري.

وغني عن البيان مدى الخطورة التي يمكن أن يتعرض لها حامل البطاقة عند إرساله لبيانات بطاقته عبر الإنترنت، وخاصة رقمها السري ، وما يترتب على ذلك من إمكانية الاستيلاء على هذه البيانات، الأمر الذي قد يؤدي إلى خسارة مادية جسيمة لأصحاب البطاقات والمصارف والتجارة الإلكترونية جميعاً.

## ثالثاً- أساليب الاستيلاء على بيانات بطاقات الائتمان:

هناك العديد من أساليب الاستيلاء على البيانات والأرقام السرية لبطاقات الائتمان لاستخدامها في الاحتيال. ومن أبرز هذه الأساليب:

**أ- <u>أسلوب انتحال الصفة:</u>**

يتم هذا الأسلوب عن طريق إنشاء مواقع مزيفة على شبكة الإنترنت، على غرار مواقع الشركات والمؤسسات التجارية الأصلية الموجودة على هذه الشبكة، بحيث يبدو هذا الموقع المزيف وكأنه الموقع الأصلي المقدّم لتلك الخدمة. ويقوم الجناة عادة بالحصول على البيانات الخاصة بالموقع الأصلي وعنوانه ورقمه عن طريق الإنترنت، ثم يستخدمون هذه البيانات لإنشاء الموقع المزيف، بحيث يبدو للعيان شبيهاً بالموقع الأصلي، وبعد ذلك يقومون بتعديل البيانات السابقة على الموقع الأصلي، بحيث لا يكون على الإنترنت إلا موقع واحد بنفس العنوان.

وبعد إنشاء الموقع المزيف، يستقبل عليه الجناة جميع المعاملات المالية والتجارية التي يقدمها عادة الموقع الأصلي لعملائه عبر شبكة الإنترنت، فيتم استقبال الرسائل الإلكترونية الخاصة بالموقع الأصلي والاطلاع عليها، ومن ثم يتم الاستيلاء على البيانات الخاصة ببطاقات الائتمان أو بطاقات الدفع الإلكتروني[1].

وفي إحدى القضايا، تم القبض في مصر على عصابة مكونة من ثلاثة أشخاص، لقيامهم بتصميم مواقع تشبه مواقع بعض المصارف، ثم قيامهم بإرسال رسائل عشوائية عن طريق البريد الإلكتروني إلى عملاء حقيقين، فينخدعون ويقومون بكتابة بياناتهم ويتبعون الخطوات التي يحددها لهم المتهمون. وبعد التعرف على البيانات السرية للعملاء، خاصة كلمات المرور السرية، يتم الاستيلاء على أرصدة هؤلاء الضحايا [2].

---

(1) د. جميل عبد الباقي الصغير: الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة ، المرجع السابق، ص37.

(2) د. محمد الشناوي: المرجع السابق، ص133.

**ب- أسلوب التجسس:**

يقوم الجناة وفقاً لهذا الأسلوب باستخدام برامج لاختراق الأنظمة المعلوماتية للشركات والمؤسسات التجارية العاملة على شبكة الإنترنت، ومن ثم يستطيع هؤلاء الجناة الاطلاع على البيانات والمعلومات التجارية الخاصة بهذه الشركات، ومنها المعلومات المتعلقة ببطاقات الائتمان أو الدفع الإلكترونية المستخدمة في التجارة الإلكترونية عبر الشبكة. وبذلك يتمكن الجاني من الاستيلاء على بيانات البطاقات الصحيحة، واستخدامها عبر شبكة الإنترنت على حساب الحامل الشرعي للبطاقة[1].

ومن أمثلة هذا الاختراق، ما حدث في عام 1996، حيث تم اختراق حاسوب محمول يحتوي على 000.314 رقماً لبطاقة ائتمان تخص أحد المكاتب التابعة لمؤسسة Visa Card INT في كاليفورنيا.

وفي عام1997، قام شخص يدعى "كارلوس سادالغو" Carlos Sadalgo، بالاستيلاء على أرقام 000.100 بطاقة ائتمان وبيانات أخرى، من خلال اختراقه لمجموعة من مزودي خدمات الإنترنت، وقام بوضع هذه الأرقام على أسطوانة مضغوطة، ثم قام بتشفيرها وعرضها للبيع بمبلغ مائتين وخمسين ألف دولار. ولقد اكتشف عملاء المباحث الفيدرالية هذه الجريمة، وحوكم "سادالغو" وعوقب بالسجن ثلاثين شهراً[2].

**جـ- أسلوب الشفط Skimming[3]:**

---

(1) د. جميل عبد الباقي الصغير: الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة ،المرجع السابق، ص38.

(2) د. عمر بن يونس: المرجع السابق، ص421.

(3) Robin Bryant, op- cit, p. 141-142.

"Skimming" هو طباعة التفاصيل المخزنة على الشريط الممغنط لبطاقة الائتمان، عن طريق تمرير البطاقة على قارئ إلكتروني، وبمجرد الحصول على تفاصيل البطاقة، مثل رقم التعريف بهوية الحامل (PAN)، وتاريخ انتهاء صلاحية البطاقة، يستطيع المحتال إنشاء بطاقة مطابقة للبطاقة الأصلية، لاستعمالها في الصفقات التي تعقد على الإنترنت.

وأجهزة الـ "Skimmer" توضع مثلاً على فتحة الصراف الآلي، حيث يتم مسح تفاصيل بطاقة الزبون ضوئياً، وتخزينها في جهاز خاص قبل أو بعد دخول البطاقة إلى قارئ البطاقات في الصراف، وقد يرفق بالماسحة الضوئية كاميرا تسجل رقم PIN المُدخل من قبل الضحية.

وخطورة هذا النوع من الاستيلاء على بيانات البطاقات هو أن حامل البطاقة لا يعلم بأن بطاقته تم اختراقها، لذا لا يبلغ أحداً لإلغائها، وبذلك يستطيع المحتال استخدام البطاقة المزورة خلال فترة طويلة، وهذا بعكس الأسلوب التقليدي المتبع في الاستيلاء على بيانات البطاقة وهو سرقة البطاقة، لأنه في حال سرقة البطاقة يكون الاحتيال بها قصير الأمد، إذ إن الضحية ستلاحظ ذلك، وتقوم بتبليغ مصدر البطاقة لإلغائها.

ففي عام 2005، تمّ الحكم في إنكلترا على أربعة من أعضاء عصابة لمسح البطاقات وسحب الأموال، بالسجن لمدة أربع سنوات لارتكابهم الاحتيال الذي قدرت خسارته بـ 200،000 جنيه استرليني.

كما تم التحذير من أسلوب Skimming، حيث وضعت تحذيرات على أجهزة السحب الآلي في معظم الدول، تتضمن الطلب من الزبائن عدم استخدامها إذا بدت غير طبيعية، وإذا كان هناك شك بوجود آلة Skimmer على جهاز سحب النقود، فإن الشرطة تنصح بعدم الإبلاغ فوراً لأن هذه الأجهزة غالية الثمن، وقد يتدخل المجرم تدخلاً عنيفاً في هذه الحالة. ولكن

يمكن اعتقال هذا المجرم عندما يتم ترصده، لأنه سوف يعود لاسترجاع الجهاز.

ومن أكثر الحالات التي يمكن أن يستخدم بها جهاز Skimmer هي عند دفع الفواتير في المطاعم، حيث يقوم الزبون بإعطاء البطاقة إلى محاسب المطعم الذي يقوم بتمريرها على جهاز Skimmer ثم يقوم بإعادتها إلى صاحبها، وبذلك تتم عملية نسخ لبيانات البطاقة.

ومن الجدير بالذكر أن هناك أسلوباً ميكانيكياً للاستيلاء على بيانات بطاقات الائتمان، حيث يتم تحويل التفاصيل المنقوشة على البطاقة البلاستيكية ميكانيكاً من بطاقة إلى أخرى. وقد عرفت هذه التقنية بما يسمى Shave And Paste. و هذه الطريقة أسهل من أسلوب سرقة البطاقة برمتها أثناء نقلها ما بين البنك والزبون.

**د- <u>تخليق أرقام البطاقات Card Math:</u>**

ويقوم هذا الأسلوب على تخليق أرقام بطاقات ائتمانية اعتماداً على إجراء معادلات رياضية وإحصائية ، بهدف الحصول على أرقام بطاقات ائتمانية مملوكة للغير، وهي كل ما يلزم للشراء عبر شبكة الإنترنت.

فهذا الأسلوب يعتمد على أسس رياضية في تبديل وتوفيق أرقام حسابية، تؤدي في النهاية إلى ناتج معين ، وهو الرقم السري لبطاقة ائتمان متداولة، ثم يتم استخدامها استخداماً غير مشروع عبر شبكة الإنترنت[1].

## رابعاً- الاستخدام غير المشروع لبطاقات الائتمان:

قد يتم استخدام بطاقات الائتمان بصورة غير مشروعة، **إما عن طريق أطراف العلاقة** وهم: الجهة المصدرة (المصرف)، والعميل أو الحامل، والتاجر، **وإما عن طريق الغير**. وهذا ما سنبحثه على التتالي:

### أ- صور الاستخدام غير المشروع لبطاقات الائتمان من الجهة المصدرة:[2]

يقصد بالجهة المصدرة موظفو المصرف، وغالباً ما تتخذ جرائمهم الصور التالية:

1- التلاعب في رصيد البطاقة عن طريق حركات الإيداع والسحب لمصلحة الموظف، مستغلاً عدم دراية العميل الكافية.

2- تواطؤ موظف البنك مع حامل البطاقة على ارتكاب أفعال غير مشروعة، مثل استخراج بطاقة سليمة بناء على بيانات مزورة، أو السماح للعميل بتجاوز حد البطاقة في السحب، أو السماح للعميل بالصرف بموجب بطاقة منتهية الصلاحية أو ملغاة.

---

(1) د. عبد الفتاح بيومي حجازي، المرجع السابق، ص134.

(2) د. جميل عبد الباقي الصغير: الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة، المرجع السابق، ص24. د.محمد الشناوي: المرجع السابق، ص120.

3- تواطؤ موظف البنك مع التاجر على ارتكاب عدة أفعال غير مشروعة، مثل تجاوز حد السحب في صرف قيمة إشعارات البيع، أو قبول إشعارات وهمية أو مزورة.

4- تواطؤ موظف البنك مع العصابات الإجرامية، وتزويدهم ببيانات بطاقات ائتمان صحيحة ومتداولة، وذلك لاستخدامها في تزوير البطاقات.

وغني عن البيان بأن جميع أساليب التلاعب المذكورة التي يقوم بها موظف البنك، تشكل جرائم احتيال، إضافةً إلى جرائم أخرى تختلف بحسب الحال، مثل جريمة إفشاء الأسرار، وجريمة التزوير، وجريمة إساءة استعمال الوظيفة إذا كان المصرف عائداً للدولة.

**ب- صور الاستخدام غير المشروع من حامل البطاقة (العميل):**

قد يرتكب حامل البطاقة عدة أفعال غير مشروعة ، يمكن تلخيصها بما يلي:

**1- إساءة استخدام البطاقة من قبل الحامل عن طريق سحب النقود أو الوفاء بما يتجاوز رصيده أثناء فترة صلاحيتها:**

تضاربت أحكام القضاء الفرنسي في هذا الشأن، فمنها من اعتبر هذا الفعل مكوناً لجريمة السرقة، ومنها من اعتبره جريمة احتيال. إلا أن محكمة النقض الفرنسية حسمت هذا الخلاف في حكم لها عام 1983، حيث إنها لم تضف أي طابع إجرامي على هذا الفعل، معتبرةً إياه مجرد إخلال بالتزام تعاقدي، لا ينطوي على أية جريمة جزائية في ظل النصوص الجزائية القائمة. وقد جاء هذا الحكم تأييداً لحكم محكمة استئناف "Angers"، الذي انتهى إلى أن استيلاء حامل البطاقة على مبالغ تتجاوز رصيده، عن طريق السحب من أجهزة التوزيع الآلي، لا يشكل أي جريمة جزائية.

ولقد جاء في حيثيات حكم محكمة النقض المشار إليه (نظراً لأن محكمة الاستئناف، ومن أجل الحكم ببراءة المتهم، أثبتت أنه لكي يتمكن المتهم من

إجراء السحوبات غير المشروعة فقد استخدم – طبقاً للقواعد الفنية لاستعمال الجهاز – البطاقة بوصفه صاحبها، وحيث إنه بالنظر إلى ذلك، فقد بررت محكمة الاستئناف حكمها، إلا أنه في الواقع، فإن الوقائع المنسوبة للمتهم تنطوي على عدم ملاحظة التزام تعاقدي، ولا تندرج تحت أي نص جزائي)[1].

و**يرى الباحث** أن محكمة النقض الفرنسية كانت على حق في هذا الحكم، فخطأ العميل هنا تعاقدي، لأنه قام بمخالفة بنود العقد المبرم مع المصرف حول حد السحب المسموح به؛ لذلك فإن هذه الواقعة لا تشكل جرماً جزائياً، فلا يكون أمام المصرف في مواجهة العميل سوى مطالبته بالقدر الزائد من المال الذي حصل عليه بدون وجه حق.

وكذلك إذا استخدم العميل بطاقته خلال فترة الصلاحية بما يجاوز الحد المسموح به في الوفاء لدى التجار، فإن الرأي الراجح في الفقه يرى بأن العميل هنا أيضاً لا يرتكب جرم الاحتيال في مواجهة التاجر، لأن التاجر يعلم تماماً بموجب العقد الذي بينه وبين الجهة المصدرة للبطاقة (المصرف) بالحد الأقصى الذي يلتزم به المصرف ويضمن سداده إليه؛ فالتاجر يعد هنا متصرفاً في هذه الحالة على مسؤوليته[2].

---

(1) Cass. Crime. 24 Nov. 1983, Bull. crim. N 315 .

مشار إليه عند: المحامي محمد أمين الشوابكة: المرجع السابق، ص195.

J. Ferchaud: Gaz pal 20 Nov, 1984 , note B.SOUSI-ROUBI.

C.A. Angers, 4 Fevrier 1982, Parquet, C.P. N45.

وهذان الحكمان أيضاً يرفضان تطبيق أية عقوبة جزائية على الفعل المشار إليه . مشار إليهما عند د.أحمد حسام طه تمام: الجرائم الناشئة عن استخدام الحاسب الآلي، رسالة دكتوراه مقدمة إلى جامعة طنطا بمصر، عام 2000، المرجع السابق، ص529. د.محمد الشناوي: المرجع السابق، ص128. عفيفي كامل عفيفي: جرائم الكمبيوتر، منشورات الحلبي الحقوقية، بيروت، عام 2003، ص175.

(2) د.جميل عبد الباقي الصغير: الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة ، المرجع السابق، ص73.

**2- قيام الحامل باستخدام البطاقة بالرغم من إلغائها:**

قد يقوم المصرف مصدر البطاقة بإلغائها أثناء فترة صلاحيتها، وذلك كجزاء لسوء استخدام البطاقة من قِبَل حاملها خلال فترة صلاحيتها، كتجاوزه الحد المسموح به في السحب مثلاً. فإذا تم إلغاء البطاقة من جانب المصرف وتمّ إخطار العميل بذلك، فإنه يتعين على هذا الأخير إعادة البطاقة لمصدرها، فإذا امتنع العميل عن ردها إلى المصرف، فإن هذا الامتناع يعد تبديداً لشيء تم تسليمه على سبيل عارية الاستعمال، وهو ما يشكل اختلاساً تقوم به جريمة خيانة الأمانة[1].

وإذا استخدم العميل البطاقة الملغاة في الوفاء للتجار، فإن ذلك يشكل جريمة احتيال، لأن مجرد استعمال هذه البطاقة سيهدف إلى الإقناع بوجود ائتمان وهمي لا وجود له في الواقع، إذ إن إلغاء البطاقة يخلع عنها قيمتها كأداة ائتمان. ففي إحدى القضايا، تعسف الحامل الشرعي في استخدام بطاقته، الأمر الذي حمل المصرف على إلغاء هذه البطاقة ومطالبة العميل بردها . إلا أن العميل لم يقم بردها واستمر باستعمالها في الوفاء. فقام المصرف برفع الدعوى أمام محكمة جنح باريس، التي قضت بإدانة الحامل بجرم الاحتيال، على أساس أن قيامه بتقديم بطاقته الملغاة يهدف إلى الإقناع بوجود ائتمان وهمي[2].

---

(1) د.جميل عبد الباقي الصغير: الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة ، المرجع السابق، ص78.

(2) Trib. Corr. Paris,16 October 1974

مشار إليه عند : د.جميل عبد الباقي الصغير: الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة ، المرجع السابق، ص80.

المحامي محمد أمين الشوابكة: المرجع السابق، ص197. د.محمد الشناوي: المرجع السابق، ص129. عفيفي كامل عفيفي: المرجع السابق، ص176.

ويجب على المصرف أن يزود المتاجر بقائمة تتضمن البطاقات الملغاة، وحالياً فإن الآلة الإلكترونية في المتاجر تعطي بياناً عن البطاقة لكونها متصلة بالشبكة المصرفية اتصالاً مباشراً، حيث يظهر على الشاشة إذا كانت البطاقة ملغاة أو مفقودة أو مسروقة؛ كما أن أجهزة السحب الآلي مبرمجة إلكترونياً للاحتفاظ بالبطاقة في الحالات المذكورة، لذلك فسحب النقود من أجهزة السحب الآلي بواسطة بطاقة ملغاة أمر غير متصور، لأن هذه الأجهزة ترتبط مباشرة بحسابات العملاء في المصرف[1] .

**3- قيام الحامل باستخدام البطاقة بالرغم من انتهاء صلاحيتها:**

يرى الفقه – وهو محق- أن الحامل لا يرتكب جريمة احتيال إذا قام بالوفاء للتاجر بالبطاقة بعد انتهاء صلاحيتها، لأن الكذب هنا ينصب على الصلاحية لا على الإقناع بوجود ائتمان وهمي. فتقديم البطاقة لا يكفي لتحقيق الخداع، لأن إبراز هذه البطاقة يعد تجسيداً للكذب. بل إن المسؤولية هنا تقع على التاجر فيتحمل الضرر وحده، لأنه أخل بأحد التزاماته التعاقدية، وهو فحص تاريخ صلاحية البطاقة، فهو يستطيع اكتشاف كذب الحامل بسهولة. ولذلك سيرفض المصرف الوفاء بقيمة الفاتورة بسبب إخلال التاجر بأحد التزاماته التعاقدية، وهو فحص تاريخ صلاحية البطاقة.

ويختلف الأمر إذا اتفق التاجر مع الحامل على قبول الوفاء ببطاقة منتهية الصلاحية، وذلك بأن يقوم التاجر بتزوير تاريخ الصلاحية على الفاتورة (إشعار البيع)، أو أن يقوم بتقديم تاريخ عملية البيع، ففي هذه الحالات يتحقق

---

(1) د.جميل عبد الباقي الصغير: الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة ، المرجع السابق، ص82. د. أحمد حسام طه تمام: المرجع السابق، ص527.

الخداع، ويسأل الحامل باعتباره فاعلاً لجريمة الاحتيال، ويسأل التاجر باعتباره شريكاً فيها[1].

## جـ – صور الاستخدام غير المشروع لبطاقات الائتمان من التاجر:

يقصد بالتاجر هنا الجهة التي تقبل البطاقات من حامليها كوسيلة دفع إلكترونية مقابل السلع والخدمات المقدمة منها لهؤلاء العملاء، وذلك بشرط توقيعهم للتاجر على إشعارات البيع. ولا يحق لأي جهة قبول البطاقات من العملاء كوسيلة دفع دون وجود تعاقد مع أحد المصارف العاملة في هذا المجال، الذي يقوم تبعاً لذلك بتزويد التاجر بالأجهزة اللازمة لهذا التعامل ( سواء أكانت الأجهزة يدوية أو إلكترونية)، ومستلزمات التشغيل الخاصة بها (إشعارات البيع)، على أن يقوم التاجر بتحصيل قيمة تلك الإشعارات من المصرف المتعاقد معه.

وتحرص المصارف على تزويد التجار المشاركين بأحدث الوسائل الإلكترونية للتعامل في بطاقات الائتمان، حتى تضمن اكتشاف البطاقات المزورة ، والحد من تلاعب التجار بهذه البطاقات.

ويقوم التاجر بدور هام في إتمام عمليات البيع أو تقديم الخدمة باستخدام بطاقات الائتمان، فهو يقوم بفحص البطاقة والتأكد من صلاحيتها والتحقق من شخصية الحامل، ومضاهاة توقيع العميل على الإشعار مع توقيعه الموجود على ظهر البطاقة، وهذا يعني أن التاجر يحل محل المصرف في تأدية الخدمة لحامل البطاقة، عن طريق استخدام الأدوات المصرفية المسلمة إليه لإتمام عمليات الشراء، لذلك فإن المجال يكون واسعاً أمام التاجر للتلاعب أثناء قيامه

---

(1) د.جميل عبد الباقي الصغير: الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة ، المرجع السابق، ص84–85. المحامي محمد أمين الشوابكة: المرجع السابق، ص198. د.محمد الشناوي: المرجع السابق، ص130.

بهذه العمليات[1]. ويمكن أن نرصد بعض صور التلاعب بالبطاقات الذي يقوم به التاجر[2]:

1- قيام بعض التجار باستخدام البطاقات التي ليست لها أرصدة كافية للصرف، وذلك عن طريق إجراء عمليات بيع عديدة بمبالغ صغيرة وصرفها من المصرف، ثم يتضح بعد ذلك عدم وجود أرصدة لأصحاب هذه البطاقات.

2- قبول بعض التجار البطاقات المزورة من العملاء، والتلاعب في البرامج الخاصة بالآلة الإلكترونية، بحيث يتم تعطيل العمل بها أثناء عملية قراءة البطاقة حتى لا يتم اكتشاف أنها مزورة، واستخدامها في صرف مبالغ من المصارف.

3- استخدام أرقام بطاقات ائتمان عائدة للغير دون وجه حق. ففي إحدى القضايا التي وقعت في مصر، قامت ثلاث موظفات يعملن بمحل ملابس في الملحق التجاري لأحد الفنادق بالقاهرة، بالاستيلاء على مبالغ كبيرة تمثل قيمة مبيعات المحل من الملابس الجاهزة، التي تم بيعها لرواد المحل نقداً. ولتسوية الحساب، قمن بتحميل تلك المبالغ على أرقام بطاقات ائتمان بعض السياح الأجانب، الذين سبق لهم أن اشتروا من المحل باستخدام بطاقات الائتمان. وفي سبيل ذلك استخدمن آلات البيع الإلكترونية المسلمة للمحل من المصرف، ثم قمن بتزوير تواقيع أصحاب البطاقات على الإشعارات المستخرجة من تلك الآلات، وأرسلن تلك الإشعارات المزورة إلى المصرف حتى يتم خصم قيمتها من حساب أصحاب البطاقات الأجانب، وإضافة تلك القيمة إلى حساب المحل الذي اختلست أمواله.

---

(1) د.جميل عبد الباقي الصغير: الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة ،المرجع السابق، ص25-26.

(2) د.محمد الشناوي: المرجع السابق، ص 122-124. د.عبد الفتاح بيومي حجازي: المرجع السابق، ص 127.

وفي قضية مشابهة فقد تم إجراء اتصالات دولية وتحميل القيمة على بطاقات الائتمان الخاصة بالغير[1].

4- مغافلة حامل البطاقة والتلاعب بالمبالغ المسحوبة بالزيادة أثناء عملية السحب، وخاصة للسياح الأجانب.

ففي سورية عُرضت مؤخراً على القضاء العديد من القضايا التي تضمنت قيام بعض التجار بالتلاعب بالمبالغ المسحوبة من بطاقات الائتمان العائدة للسياح الأجانب. فبعد أن يختار السائح السلع المطلوبة، يقوم بتسليم بطاقته الائتمانية للتاجر لإجراء عملية سداد قيمة المشتريات، حيث يقوم التاجر هنا بمغافلة الزبون وإضافة زيادة على المبالغ الأصلية المطلوبة عن طريق الآلة الإلكترونية.

وعندما يعود السائح إلى بلده، يفاجئ بكشف المصرف والمبالغ المستوفاة أثناء وجوده في سورية، فيقوم بتقديم شكوى إلى وزارة الداخلية في بلده حيث يتم تحويلها إلى وزارة الداخلية في سورية (عن طريق شعبة الاتصال)، ثم يتم التوصل إلى أصحاب المحلات المعنية والتحقيق معهم عن طريق أرقام الآلات الإلكترونية الموجودة في هذه المحلات.

وقد قامت النيابة العامة بتحريك الدعوى العامة بحق هؤلاء التجار المتلاعبين بجرم الاحتيال[2].

## د- الاحتيال باستخدام بطاقات الائتمان الصادرة من الغير:

---

(1) د. جميل عبد الباقي الصغير: الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة ، المرجع السابق، ص29 - 30.

(2) من خلال عملنا القضائي قمنا بالتحقيق بالعديد من هذه القضايا، ومعظم هذه القضايا ما تزال منظورة أمام محاكم الأساس, ولم تصل بعد إلى ديوان محكمة النقض لتقول كلمتها الأخيرة فيها. ومن قضايا احتيال بطاقات الائتمان المنظورة أمام القضاء, القضية رقم أساس 1503 لعام 2007 المنظورة أمام محكمة بداية الجزاء الثانية عشرة بدمشق.

يمكن أن نميز هنا بين ثلاث حالات هي:

**1- حالة فقد البطاقة أو سرقتها:**

قد يحدث أن تتم سرقة البطاقة أو تتعرض للضياع ومعها الرقم السري، وغالباً ما يقوم المصرف بإلزام عميله في حالة السرقة أو الضياع بأن يبلغ عن الحادثة فوراً لإيقاف العمل بالبطاقة.

ومما لا شك فيه، فإن مسؤولية الحامل الشرعي تنتفي من اللحظة التي يتم فيها الإبلاغ عن سرقة أو فقدان البيانات السرية لبطاقة الائتمان، فلا يُسأل عن استعمال البطاقة احتيالياً. ويجب على المصرف المصدر للبطاقة أن يوقف التعامل بها فوراً، وإلا كان مسؤولاً عن العمليات المالية التي تتم بواسطتها[1].

وحتى يتخلص المصرف من المشاكل المتعلقة بموعد الإبلاغ، فقد تم إنشاء نظام تأمين لتعويض سرقة البطاقات أو ضياعها إذا ما تم استعمالها في السحب أو الوفاء، ويحدد المبلغ القابل للتعويض في العقد المبرم بين المصرف والعميل. كما تمت برمجة أجهزة التوزيع الآلي للنقود على افتراض وجود محاولات يقوم بها الجاني لتجربة بعض الأرقام حتى يتوصل إلى الرقم السري، فبعد إجراء ثلاث محاولات مثلاً، يقوم الجهاز بسحب البطاقة ولا يعيدها له، فإذا كان هو حاملها الشرعي فلا يستطيع استردادها إلا عن طريق المصرف المصدر لها[2].

وقد ذهبت المحاكم الفرنسية وسايرها الفقه إلى أن سرقة الأرقام والبيانات السرية الخاصة ببطاقة الائتمان، واستخدامها بصورة غير مشروعة من قبل الغير في سحب النقود من الصراف الآلي، أو في الوفاء لدى التجار يشكل

---

(1) المحامي محمد أمين الشوابكة: المرجع السابق، ص199.

(2) د. أحمد حسام طه تمام: المرجع السابق، ص535.

جريمة احتيال، على اعتبار أن المتهم قد انتحل اسماً كاذباً، ومن ثم يكون قد استخدم وسيلة الخداع لإقناع المجني عليه بوجود ائتمان[1].

أما في حالة السرقة الصورية، وفيها يقوم الحامل الشرعي للبطاقة بإبلاغ المصرف أو الشرطة عن سرقة بطاقته أو فقدها، في حين أن البطاقة لا تزال في حوزته، ويستمر في استعمالها سواء في سحب النقود أو الوفاء. ففي هذه الحالة يرى الفقه – **والباحث يؤيده** – أن هذا الحامل قد فقد صفته كحامل شرعي للبطاقة، وأنه أصبح من الغير، وذلك ابتداءً من لحظة المعارضة[2]. وتطبيقاً لذلك قضت محكمة النقض الفرنسية بتوافر أركان جريمة الاحتيال في مواجهة الحامل، إذا استعمل البطاقة الخاصة به بعد قيامه بالإبلاغ الكاذب عن سرقتها أو فقدها[3].

**2– حالة استخدام بطاقة ائتمان مزورة:**

---

(1) C.A Rennes, 26 Janvier 1981, D. 1982, I.R.
مشار إليه عند د.جميل عبد الباقي الصغير: الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة ،المرجع السابق، ص91.
C.A Bordeaux, 25 Mar 1987, R.T.D. com. 1987.
مشار إليه عند: د. جميل عبد الباقي الصغير: الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة ،المرجع السابق، ص 98–99 . د. عبد الفتاح بيومي حجازي، المرجع السابق، ص144 . د. محمد الشناوي: المرجع السابق، ص130. المحامي :محمد أمين الشوابكة: المرجع السابق، ص 200.

(2) د.جميل عبد الباقي الصغير: الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة ، المرجع السابق، ص 96.

(3) Cass. Crim. 16 Juin 1986, Revue de droit des systems electroniques de payment, 1987, N 18.
مشار إليه عند: د.جميل عبد الباقي الصغير: الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة ، المرجع السابق، ص 97.

اختلف الفقهاء في التكييف القانوني لاستخدام بطاقة الائتمان المزورة . ويمكن التمييز هنا بين وصفين رئيسيين هما:

**الرأي الأول:** يرى أصحابه أن استخدام البطاقة المزورة في مجال سحب النقود، يشكل جريمة **سرقة باستعمال مفتاح مصطنع**[1]، لأن المال قد خرج من ذمة المصرف المجني عليه بغير رضائه، فالبطاقة المزورة والرقم السري تقوم مقام المفتاح المصطنع، إضافةً إلى أن قانون العقوبات لم يحدد ماهية المفتاح المصطنع.

إلا أن هذا الرأي مردود عند فقهاء آخرين لعدة أسباب منها: أن التسليم الإرادي في عملية السحب ينفي الأخذ، وهو العنصر الرئيسي في جريمة السرقة، ثم إنه من غير الممكن تشبيه بطاقات الائتمان بالمفتاح المصطنع، لأن ذلك يتعارض مع قاعدة حظر القياس في المسائل الجزائية، إذ إن القياس يؤدي إلى خرق مبدأ شرعية الجرائم والعقوبات[2].

**الرأي الثاني:** ويرى أصحابه – **والباحث يؤيده** – أن من يستعمل بطاقة مزورة في السحب أو الوفاء لدى أحد التجار، **يسأل عن جريمة الاحتيال**، حيث يشكل استعمال البطاقة وسيلة خداع تهدف إلى إقناع التاجر بوجود ائتمان وهمي، كما نكون بصدد استعمال اسم كاذب وصفة غير صحيحة[3].

---

(1) المفتاح المصطنع: هو أي مفتاح آخر غير المفتاح الحقيقي المستعمل فعلاً في الفتح. و يدخل حسب الفقه في هذا المفهوم، المفتاح المقلد، والنسخة الثانية، والمفتاح الأصلي إذا ضاع ولم يقم صاحبه باستبداله. د.علي القهوجي: المرجع السابق، ص 733–734.

(2) د. جميل عبد الباقي الصغير: الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة ، المرجع السابق، ص 139– 140.

(3) د. جميل عبد الباقي الصغير: الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة ،المرجع السابق، ص141–142. المحامي محمد أمين الشوابكة: المرجع السابق، ص202.

أما القضاء الفرنسي فقد سار مع الرأي الثاني من الفقه، إذ قضت محكمة (Rennes) بأن استخدام البطاقة المزورة هو من قبيل الطرق الاحتيالية التي تقوم بها جريمة الاحتيال.

كما قضت محكمة باريس أيضاً بالحكم على تاجر بالاشتراك في جريمة الاحتيال لقبوله بطاقة ائتمان مع علمه بأنها مقلدة[1].

وغني عن البيان بأن استعمال بطاقة الائتمان المزورة يشكّل حالة اجتماع جرائم معنوي، أي جريمة الاحتيال وجريمة استعمال المزور( وذلك في حال وجود نص يجرم تزوير المحررات الإلكترونية)، وفي هذه الحالة تقوم المحكمة بذكر جميع الأوصاف للحكم، ثم تحكم بالعقوبة الأشد (المادة 180 من قانون العقوبات).

**3- التواطؤ بين الحامل الشرعي والغير:**

ويتحقق ذلك بقيام الحامل الشرعي بإعطاء بطاقته للغير لاستخدامها بدلاً منه في السحب أو الوفاء، ثم يبادر بالاعتراض على هذه العمليات حتى لا يتحمل هذه المبالغ.

ففي إحدى القضايا، أعطى لبناني مقيم في أمريكا بطاقة الائتمان الخاصة به إلى لبناني آخر موجود في مصر، وقام هذا الأخير باستخدام هذه

---

(1) Rennes 26 Javu. 1981 D. 1982, IRSOO. Obs. Vasseurirev. Fud. Ovest. 1981.
C.A Paris 9 B. 17 Octobre 1991. Jouris. Data. N 24814.
مشار إليهما عند: د. أحمد حسام طه تمام: المرجع السابق، ص539. د. محمد الشناوي: المرجع السابق، ص130. عفيفي كامل عفيفي: المرجع السابق، ص178.

البطاقة فعلاً في سحب مبالغ كبيرة من أحد المصارف ، وبعد تحصيل المبالغ من المصرف المصدر للبطاقة، عاد هذا الأخير وطالب باستردادها، لأن الحامل الشرعي للبطاقة الموجود في أمريكا أثبت للمصرف المصدر بأنه لم يغادر البلاد، ولم يدخل إلى مصر، وأن البطاقة التي جرى السحب بموجبها كانت مزورة. وبذلك استطاع الحامل الشرعي التخلص من دفع المبلغ. وبعد إجراء التحريات تم كشف عملية الاحتيال هذه[1].

وأخيراً، ولتلافي جميع أساليب الاحتيال المذكورة، وخاصة الاحتيال في المجال التجاري الذي يتم عبر شبكة الإنترنت، فإن هناك العديد من **النصائح الوقائية**، ومنها مثلاً، استخدام بطاقة ائتمان مدفوعة الثمن سابقاً وبحد ائتماني صغير، وتخصيص استعمالها فقط للدفع عن طريق الإنترنت، بحيث إذا تعرضت للاستيلاء والاستخدام غير المشروع من قبل الغير كانت الخسائر محدودة[2]؛ كما ينصح بتجنب الشراء من أي موقع لا يعلن عن إجراءات الأمان التي يتبعها لحماية بيانات بطاقات الائتمان[3].

و**يرى الباحث** أنه لابد من التطوير المتسارع والدائم للأنظمة الأمنية التقنية المرافقة لاستخدام بطاقات الائتمان على مختلف أشكالها، وذلك للتخفيف قدر المستطاع من أساليب الاستيلاء على البيانات السرية لهذه البطاقات، إذ لم تسلم حتى هذه الأنظمة الأمنية من عبث العابثين.

---

(1) د. جميل عبد الباقي الصغير: الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة ، المرجع السابق، ص32.

(2) المحامي محمد أمين الشوابكة: المرجع السابق، ص202.

(3) د. محمد الشناوي: المرجع السابق، ص136.

## المبحث الثاني

## المواجهة التشريعية

مع التزايد المستمر لجريمة الاحتيال عبر الإنترنت، ذهبت أغلب الدول إلى تجريم هذه الجريمة المستحدثة ضمن إطار المواجهة التشريعية لمختلف جرائم الإنترنت. إلا أن هناك اتجاهاً حديثاً لمواجهة جريمة الاحتيال عبر

الإنترنت عن طريق إصدار تشريع مستقل يعالج هذه الجريمة، وهذا ما قام به المشرع البريطاني في عام 2006 عندما أصدر تشريعاً مستقلاً يكافح الاحتيال بصوره المستحدثة[1].

أما بقية الدول التي لم تتصدَ تشريعياً لجريمة الاحتيال عبر الإنترنت، فقد ذهب القضاء فيها إلى التوسع في تفسير النصوص الجزائية التقليدية؛ لتشمل هذا النوع من الإجرام، على الرغم من أن هذا التوسع لم يسلم من النقد الفقهي.

كما ظهرت اتفاقيات على المستوى الإقليمي لمواجهة جرائم الإنترنت، مثل الاتفاقية الأوربية حول الجريمة الافتراضية، والقانون العربي الاسترشادي لجرائم المعلوماتية على المستوى العربي.

وقد أشرنا سابقاً إلى أن التعرف على هذه التشريعات والاتفاقيات أمر في غاية الأهمية لمعرفة أسلوب صياغتها ومدى شمولها، لعلها تكون مرشداً للمشرع السوري عند سنّه مثل هذه التشريعات. واستناداً لذلك سنقسم هذا المبحث إلى المطلبين التاليين:

المطلب الأول: التشريعات على الصعيد الوطني.

المطلب الثاني: الاتفاقيات على الصعيد الإقليمي.

## المطلب الأول

## التشريعات على الصعيد الوطني

كانت الدول المتقدمة سباقة إلى مواجهة جرائم الإنترنت ، سواء عن طريق سن التشريعات الجزائية الخاصة بهذه الجرائم، أو من خلال تعديل النصوص القائمة لتشمل هذا الإجرام المستحدث.

---

(1) سنلقي الضوء على هذا التشريع في المطلب القادم.

كما أن المشرع العربي لم يقف مكتوف الأيدي أمام هذه الظاهرة، بل كانت هناك محاولات تشريعية في الدول العربية لاستيعاب هذا النوع من الإجرام. وبناءً على ذلك سوف نلقي الضوء على هذه المواقف التشريعية على صعيد الدول الأجنبية وعلى صعيد الدول العربية كما يلي:

## أولاً- التشريعات على صعيد الدول الأجنبية:

- قام المشرع في **كندا** بتعديل القانون الجزائي الاتحادي في عام 1983 ليشمل جرائم الحاسوب والإنترنت، حيث عاقبت المادة 342 من قانون العقوبات الكندي على الجرائم المتعلقة ببطاقات الائتمان، كتزويرها واستعمال البطاقات المزورة وغير ذلك. كما عاقبت المادة 1-342 على ارتكاب الجرائم من خلال الحاسوب ومنها جريمة الاحتيال[1].

---

(1) /342/ 1- Every Person who:
(*a*) steals a credit card,
(*b*) forges or falsifies a credit card,
(*c*) possesses, uses or traffics in a credit card or a forged or falsified credit card, knowing that it was obtained, made or altered
(i) by the commission in Canada of an offence, or
(ii) by an act or omission anywhere that, if it had occurred in Canada, would have constituted an offence, or
(*d*) uses a credit card knowing that it has been revoked or cancelled,
is guilty of
(*e*) an indictable offence and is liable to imprisonment for a term not exceeding ten years, or
(*f*) an offence punishable on summary conviction. ====

= = = 342.1 (1) Every one who, fraudulently and without colour of right,
(a) obtains, directly or indirectly, any computer service,
(b) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system,
(c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) or an offence under section 430 in relation to data or a computer system, or
(d) uses, possesses, traffics in or permits another person to have access to a computer password that would enable a person to commit an offence under paragraph (a), (b) or (c)
is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable on summary conviction.

– وفي **ألمانيا** فإن المادة (A/263) من قانون العقوبات الألماني تتضمن تجريماً للاحتيال المعلوماتي، حيث نصت على ما يلي: (كل من يقوم بنية الحصول لنفسه أو لشخص ثالث على منفعة مادية غير مشروعة، بالإضرار بممتلكات الغير، عن طريق التأثير في نتيجة المعالجة الآلية للبيانات، من خلال برمجة غير صحيحة، أو استعمال بيانات غير صحيحة أو غير مكتملة، أو عن طريق الاستعمال غير المصرح به للبيانات، أو عن طريق التدخل غير المصرح به في عملية المعالجة ذاتها. يعاقب بالسجن لمدة لا تزيد عن خمس سنوات أو بالغرامة.)[1].

كما حذا المشرع **اليوناني** حذو المشرع الألماني، حيث أضاف بعض المواد الخاصة بالجريمة المعلوماتية إلى قانون العقوبات اليوناني عام 1988، وقد سمحت المادة **386 (A)** من قانون العقوبات اليوناني بتجريم الاحتيال المعلوماتي، وهذه المادة تأثرت بالمادة المشار إليها في قانون العقوبات الألماني، فقد نصت هذه المادة على أنه: ( يعدّ مرتكباً لجريمة الاحتيال

---

430. (1) Every one commits mischief who willfully.
(*a*) destroys or damages property;
(*b*) renders property dangerous, useless, inoperative or ineffective;
(*c*) obstructs, interrupts or interferes with the lawful use, enjoyment or operation of property; or
(*d*) obstructs, interrupts or interferes with any person in the lawful use, enjoyment or operation of property.

متوفر على موقع القوانين الكندية: Laws. Justice.gc.ca

Eoghn Casey, op- cit, chapter- 2, p-2 .

Section 263a Computer Fraud (1)
(1) Whoever, with the intent of obtaining for himself or a third person an unlawful material benefit, damages the assets of another by influencing the result of a data processing operation through incorrect configuration of a program, use of incorrect or incomplete data, unauthorized use of data or other unauthorized influence on the order of events, shall be punished with imprisonment for not more than five years or a fine.
(2) Section 263 subsections (2) to (7), shall apply accordingly.===

=== قانون العقوبات الألماني له عدة تعديلات, كان أخرها عام 1994, وهو متوفر على موقع القانون الألماني www.iuscopm.org

المعلوماتي، كل من يقوم بالتأثير في المعلومات المبرمجة عن طريق برمجة غير سليمة، أو عن طريق التدخل أثناء تطبيق البرنامج، أو عن طريق استعمال بيانات غير سليمة أو غير مكتملة، أو بأية طريقة أخرى، مما يترتب عليه حدوث أضرار لممتلكات الغير، على أن يكون ذلك بنية إثراء نفسه أو غيره بربح غير مشروع).[1]

– أما **الدانمارك** فقد قامت في عام 1985 بسن تشريع خاص لمكافحة جرائم الحاسوب والإنترنت، شمل العديد من الجرائم، مثل الدخول غير المشروع إلى الحاسوب وتزوير البيانات وغيرها.[2]

– وأما **استراليا** ففي عام 1989 تم تعديل القانون الجزائي ليشمل جميع جرائم الحاسوب.[3]

– وفي **الفلبين** فقد تم إصدار تشريع يعاقب على القرصنة في عام 2000.

– وفي **بلجيكا** فقد صدر قانون حول الإجرام المعلوماتي في عام 2001.[4]

– وفي **سويسرا** فقد جرّم قانون العقوبات السويسري لعام 1995 الاحتيال المعلوماتي في المادة /147 / منه، والتي تنطبق على جميع حالات التلاعب

---

(1) قانون العقوبات اليوناني لعام 1950 له عدة تعديلات, وهو متوفر على الموقع www. jurist.law.edu وأيضاً: د. نائلة قورة: المرجع السابق، ص599 . د. سليمان فضل: المرجع السابق، ص205.

(2) المحاميان منير وممدوح الجنبيهي: المرجع السابق، ص188.

(3) Eoghn Casey, op- cit, chapter- 2, p-2 .

(4) محمد عبيد الكعبي: المرجع السابق، ص54.

بالمعلومات المبرمجة بقصد الاحتيال، بما في ذلك التحويل الإلكتروني غير المشروع للأموال.[1]

– كما قامت كلٌ من **هولندا وفلندا واليابان والمجر وبولندا** بسن تشريعات جزائية لمواجهة جرائم الحاسوب والإنترنت.[2]

– أما المواقف التشريعية في **الولايات المتحدة الأمريكية وبريطانيا وفرنسا** فسوف نتناولها بشيء من التفصيل.

## أ– الولايات المتحدة الأمريكية:

يعد قانون "فلوريدا" لجرائم الحاسوب الصادر في عام 1978 أول قانون في الولايات المتحدة الأمريكية يخاطب الاحتيال والتطفل على الحاسوب، حيث يَعتبر هذا القانون أن كل دخول غير مخول إلى الحاسوب هو بمثابة جريمة، حتى ولو لم يكن هناك نية عدائية من هذا الدخول.[3]

أما على الصعيد الفيدرالي، فقد صدر في عام 1984 قانون الاحتيال وسوء استخدام الكمبيوتر (CFAA)[4]، وتم تعديله في الأعوام 1986– 1988– 1989– 1990– 1994، ثم تم تعديله أخيراً عام 2001 بمقتضى القانون الوطني المؤرخ في 2001/10/26 "The patriot act"، حيث تم إدراجه في القسم 1030 من الباب /18/ من القانون الفيدرالي للولايات المتحدة الأمريكية.[5]

---

(1) د. نائلة قورة: المرجع السابق، ص604.

(2) المحاميان منير وممدوح الجنبيهي: المرجع السابق، ص189 وحتى 191.

(3) Eoghn Casey, op- cit, chapter- 2, p-1

(4) وهو اختصار لـ Computer Fraud And Abuse Act.

(5) The USA Patriot act هو القانون الوطني الأمريكي الصادر في 2001/10/26، وقد تناول تعديل حوالي خمسة عشر قانوناً، نذكر منها:

The ECPA of 1986, 18 USC Sec. 2701&Sec.
The CFAA of 1984, 18 USC Sec. 1030.

وقد عاقبت المادة (4/A/1030) من هذا القانون، كل من يقوم عمداً بالدخول إلى حاسوب مشمول بالحماية، دون أن يكون مصرحاً له بذلك، أو أن يكون متجاوزاً للتصريح الممنوح له، إذا كان الغرض والأثر المترتب على هذا الدخول هو الحصول على شيء ذي قيمة عن طريق الاحتيال، ويدخل وقت الحاسوب الذي يقدر بخمسة آلاف دولار أمريكي خلال سنة واحدة في عداد الأشياء ذات القيمة.[1]

وعليه فإن العناصر المطلوبة لتطبيق هذه المادة هي:

- المعرفة المسبقة ونية الغش.
- الدخول غير المخول إلى حاسوب محمي ، أو تجاوز الدخول المسموح به، وذلك بغرض الحصول على شيء ذي قيمة عن طريق الاحتيال.

ويقصد بالحاسوب المحمي، الحاسوب المستخدم في التجارة الداخلية أو التجارة الخارجية.[2]

أما **القوانين الأمريكية الفيدرالية الإجرائية**، فهي منصوص عليها في الأقسام، 2702 ، 2701 ، 2511 ، 2510 2703 ، 2705 2711، من الباب /18/ للقانون الفيدرالي، والقانون AA 2000 U.S.C. 42.

كما أن القسم /1029/ من الباب /18/ للقانون الفيدرالي يعاقب على الاستعمال غير المشروع لبطاقات الائتمان. ويتطلب هذا القسم أن يكون الجاني

---

The Federal Wiretap Act, 18 USC Sec. 2510&Sec.

Eoghn Casey, op- cit, Chapter- 2, p-18 . د.عمر بن يونس: الإجراءات الجنائية عبر الإنترنت في القانون الأميركي، الطبعة الأولى، بلا دار نشر، 2005، ص9.

(1) د.سليمان فضل: المرجع السابق، ص205 .

والقسم 18u.s.c.1030 متوفر على موقع القوانين الأميركية: www.lawsource.com

(2) Charles Doyle: Cyber Crime: An Overview Of The Fraud Computer, Fraud and Abuse Statute, 2008, p- 53.

(عالماً وبنية الاحتيال)، أي أن المسؤولية الجزائية تتطلب علم الجاني بأن فعله سوف يحرم شخصاً ما من أي شيء له قيمة.[1]

ومن الجدير بالذكر، أن هناك العديد من القوانين الجزائية الفيدرالية التي تجرم أشكالاً مختلفة من الاحتيال، ومعظمها يغطي التلاعب بالحواسيب كجزء من المخطط الاحتيالي ومنها قانون البيان الخاطئ (القسم 1001 من الباب18) وقانون التآمر للاحتيال على الولايات المتحدة (القسم 371 من الباب18).[2]

**ب- بريطانيا:**

قام المشرع في بريطانيا بإصدار قانون إساءة استخدام الكمبيوتر CAA لعام 1990 "Computer abuse act". وقد تضمن القسم الأول من هذا القانون تجريم الدخول غير المشروع إلى النظام المعلوماتي (القرصنة)، أما القسم الثاني فقد تضمن تجريم الدخول غير المشروع مع عنصر إضافي وهو النية لارتكاب أو تسهيل ارتكاب جرائم، أما القسم الثالث فقد تضمن تجريم أي تعديل لمحتوى الحاسوب.[3]

أما فيما يتعلق بالاحتيال، فقد قام القضاء البريطاني في بداية الأمر بتطبيق نصوص قانون السرقة على التلاعب في البيانات من أجل الحصول على منفعة مالية، فذهب إلى التوسع في تفسير المادة 15 من قانون السرقة الصادر عام 1968 والتي تنص على أنه :

( يعد مرتكباً لجريمة السرقة كل من حصل بطريق الغش وبصفة غير مشروعة على مال يخص الغير بقصد حرمانه منه بصفة دائمة) .

---

(1) Charles Doyle, op- cit, p- 58 .

(2) Charles Doyle, op- cit, p- 61 .

(3) Robin Bryant, op- cit, p- 37- 38. وأيضاً: القاضي الدكتور. غسان رباح: الوجيز في قضايا حماية الملكية الفكرية والفنية مع دراسة مقارنة حول جرائم المعلوماتية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، عام 2008، ص151.

وقد كانت الغاية من هذا التوسع اعتبار **خداع الآلة** بنية ارتكاب غش مالي، هو من قبيل الاحتيال المعاقب عليه جزائياً.[1]

وقد ثار جدل في الفقه حول هذا التوسع بالتفسير، لأن الخداع من وجهة نظر هذا الفقه يجب أن يقع على العقل البشري. إلا أن المشرع البريطاني حسم هذا الخلاف بإصداره **قانون الاحتيال لعام 2006**[2]. حيث سمح بموجبه بأن يكون الخداع موجهاً إلى نظام معلوماتي أو آلة، فلم يعد يُشترط أن يكون الخداع موجهاً إلى إنسان[3].

وقد نص قانون الاحتيال لعام 2006 على عقوبة قصوى للاحتيال، هي الحبس لمدة عشر سنوات، كما بيّن في المواد 2- 3- 4 ثلاث وسائل يمكن أن يرتكب بها الاحتيال.

حيث جعلت **المادة الثانية** منه عرض الكذب جريمة احتيال، إذا كان هذا العرض الكاذب بنية الحصول على شيء أو التسبب بخسارة. ويمكن لهذا التقديم أو العرض أن يتم من خلال الكلام أو الاتصالات أو الكتابة أو عبر موقع الوبّ، أو يمكن أن يحدث من خلال الاستخدام غير القانوني لبطاقة الائتمان، أو يمكن أن تتم الجريمة عن طريق انتحال الصفة "Phishing".

كما عدّت **المادة الثالثة** منه الغش في إعطاء معلومات من الواجب إعطائها لشخص ما، جريمة احتيال.

---

**15. Obtaining property by deception** (1)

(1) A person who by any deception dishonestly obtains property belonging to another, with the intention of permanently depriving the other of it, shall on conviction on indictment be liable to imprisonment for a term not exceeding ten years.

د. محمد الشناوي: المرجع السابق، ص101.

(2) Fraud Act 2006 دخل هذا القانون حيز التنفيذ في كانون الثاني لعام 2007 وهو متوفر على موقع القوانين البريطانية: www.britishlaw.org.uk

Robin Bryant, op- cit, p-42.

(3) الفقرة الخامسة من المادة الثانية من هذا القانون.

أما **المادة الرابعة**، فقد جعلت من إساءة استخدام منصب ما بطريقة غير شريفة، جريمة احتيال.

كما أن المشرع البريطاني عدل بعض القوانين لتشمل **خداع الآلة**، مثل قانون الضريبة المضافة Value Added Tax (VAT) حيث أصبح الخداع يشمل خداع الآلات. وكذلك قانون السير حيث أعيد صياغته، فأصبح من الممكن قانوناً خداع عداد مواقف السيارات.[1]

## ج- فرنسا:

قام المشرع الفرنسي بإصدار القانون رقم 19 لعام 1988، المتعلق بحماية نظم المعالجة الآلية للبيانات، ثم تم إدراج هذا القانون في قانون العقوبات الفرنسي لعام 1992 والذي طبق في 1994/3/1.

فقد نصت المواد من 1-323 حتى 7-323 من قانون العقوبات على تجريم الدخول بشكل احتيالي أو البقاء غير المشروع في نظام المعالجة الآلية للبيانات أو في جزء منه. وتشدد العقوبة لهذه الجريمة إذا أدى الدخول غير المشروع إلى محو أو تعديل البيانات. كما جرمت هذه المواد تعطيل أو التدخل في عمل نظام المعالجة الآلية للبيانات. إضافةً إلى تجريم إتلاف أو تعديل البيانات في نظام المعالجة الآلي. كما عاقبت المادة 7-323على الشروع في ارتكاب هذه الجرائم.[2]

---

(1) Robin Bryant, op- cit, p- 34, 44.

(2) محمد عبيد الكعبي: المرجع السابق، ص51. المحامي محمد أمين الشوابكة: المرجع السابق، ص23. د.أحمد حسام طه تمام: المرجع السابق، ص350. ويوجد نسخة من قانون العقوبات الفرنسي لعام 1992 باللغة الإنكليزية على موقع القوانين الفرنسية على الإنترنت www.Legifrance.gouv.fr.

أما المواد 1-441 حتى 9-441 فقد عاقبت على جريمة التزوير، بحيث شمل العقاب تزوير المستندات المعلوماتية.[1]

كما نصت المواد 16-626 إلى24-626، 31 على التلاعب بالبيانات الشخصية التي تكون موضوعاً للمعالجة الإلكترونية.[2]

أما **فيما يتعلق بالاحتيال عبر الإنترنت**، فإن المشرع الفرنسي لم يورد حتى تاريخ إعداد هذه الرسالة نصاً قانونياً خاصاً بالاحتيال عبر الإنترنت، بل اكتفى بتجريم الاحتيال بنص عام في المادة 1-313 من قانون العقوبات، حيث اعتبرت هذه المادة بأن الاحتيال: هو القيام باستعمال اسم كاذب أو صفة كاذبة أو بالتعسف بصفة حقيقية أو باستعمال مناورات احتيالية أو بخداع شخص طبيعي أو اعتباري، وبحثّه إضراراً به أو إضراراً بالغير، على إعطاء المبالغ أو القيم أو أي مال كان، أو على القيام بخدمة، أو القبول بعمل قانوني يؤدي إلى التزام أو إلى تنازل. ويعاقب على الاحتيال بالحبس لمدة خمس سنوات وبالغرامة 375،000 يورو.[3]

أما القضاء الفرنسي فقد طبق النص المتعلق بالاحتيال التقليدي، على الحالات التي يقوم بها الجاني بالتلاعب في البيانات داخل نظام الحاسوب، من أجل إجراء تحويل إلكتروني غير مشروع للأموال. فقد ذهبت محكمة استئناف باريس في حكم لها عام 1990، إلى أن قيام المتهم بإدخال بيانات لا جود لها إلى نظام الحاسوب، بحيث تسمح بإجراء عمليات تحويل إلكتروني للأموال

---

(1) العلامة رينيه غارو: موسوعة قانون العقوبات العام والخاص، عشرة مجلدات, منشورات الحلبي الحقوقية، بيروت، عام 2003، ترجمة المحامية لين صلاح مطر، المجلد العاشر، ص238. د. أحمد حسام طه تمام: المرجع السابق، ص407.

(2) د.علاء عبد الباسط خلاف: الحماية الجنائية لوسائل الاتصال الحديثة، دار النهضة العربية، القاهرة، عام 2002، ص138.

(3) العلامة رينه غارو: المرجع السابق، المجلد العاشر، ص105. د.محمد الشناوي: المرجع السابق, ص100.

لحساب شخص آخر دون وجه حق، يعدّ كافياً للقول بقيام جريمة الاحتيال[1]. كما يرى الفقه الفرنسي أن التسليم قد يكون محله المعلومات ذات القيمة المالية، ولعل عبارة "**أي مال كان**" الواردة في المادة 1-313 تدل على صحة هذا الرأي.[2]

أما فيما يتعلق بالاحتيال عن طريق بطاقات الائتمان، فقد أشرنا إلى الحالات التي اعتبرها القضاء الفرنسي من قبيل الاحتيال[3]. كما قام المشرع الفرنسي **بحماية بطاقات السحب والوفاء** من أفعال التزوير والتقليد من خلال القانون رقم 91- 1382 الصادر في 30 ديسمبر عام 1991. وقد عُرف هذا القانون، بقانون أمن الشيكات والبطاقات.[4]

## ثانياً- التشريعات على صعيد الدول العربية:

تعدّ محاولات المشرع العربي لمواجهة جرائم الحاسوب والإنترنت حديثة نسبياً. ويمكن التمييز في هذا الإطار بين اتجاهين في الدول العربية، هما:

1- الدول التي اكتفت بسن تشريع خاص بالمعاملات والتجارة الإلكترونية أو التوقيع الإلكتروني.

---

(1) C.A de Paris, 13 Fevrier 1990, Juris – Data N 022903.
مشار إليه وإلى العديد من الاجتهادات الأخرى عند د.نائلة قورة: المرجع السابق، ص 566. ولا بد من الإشارة هنا, بأن المادة المتعلقة بالاحتيال في قانون العقوبات الفرنسي القديم هي المادة 405 منه.

(2) د. محمد الشناوي: المرجع السابق، ص107.

(3) راجع المبحث المتعلق بالصور الخاصة بالاحتيال عن طريق بطاقات الائتمان.

(4) د. جميل عبد الباقي الصغير: الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة، المرجع السابق، ص130.

2- الدول التي سنّت تشريعاً خاصاً لجرائم المعلوماتية.

وسنتناول فيما يلي هذين الاتجاهين :

**الاتجاه الأول: الدول التي اكتفت بسن تشريع خاص بالمعاملات والتجارة الإلكترونية أو التوقيع الإلكتروني:**

قام بعض المشرعون العرب بإصدار قوانين أطلق عليها في أغلب الأحيان (قوانين المعاملات والتجارة الإلكترونية)، وهي قوانين متشابهة فيما بينها. ويعود سبب هذا التشابه **في رأي الباحث** إلى وحدة المصدر التي استقيت منه هذه القوانين، وهو القانون النموذجي الصادر عن لجنة الأمم المتحدة للقانون التجاري الدولي (اليونسترال)، الذي اتخذت الجمعية العامة للأمم المتحدة قراراً باعتماده تحت رقم 255 (د-21) تاريخ 16 كانون الأول عام 1996. وقد كان الهدف من اعتماده -حسب ما جاء في قرار الجمعية العامة المشار إليه- هو تشجيع التنسيق والتوحيد التدريجيين للقانون التجاري الدولي.[1]

ومن أمثلة هذه القوانين في الدول العربية:[2]

- القانون التونسي رقم /83/ الخاص بالمبادلات والتجارة الإلكترونية لعام 2000.
- قانون المعاملات الإلكترونية الأردني رقم /58/ لعام 2001.

---

(1) بشار محمود دودين: الإطار القانوني للعقد المبرم عبر شبكة الإنترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع- عمان، عام 2006، ص56. ومتوفر أيضاً على الإنترنت, قرار الجمعية العامة المشار إليه على الموقع doc. Abhatoo.net

(2) عبد الله عبد الكريم عبد الله: جرائم المعلوماتية والإنترنت، الطبعة الأولى، منشورات الحلبي الحقوقية- بيروت، عام 2007، الصفحات 63 و85. د. عبد الفتاح مراد: المرجع السابق، الصفحات 94، 111، 139، 167. وجميع هذه القوانين متوفرة على الإنترنت في عدة مواقع، ويمكن البحث عن القانون المطلوب عن طريق محرك البحث google.

- قانون التجارة الإلكترونية البحريني لعام 2002.
- قانون إمارة دبي الخاص بالمعاملات والتجارة الإلكترونية رقم /2/ لعام 2002.
- قانون التوقيع الإلكتروني في مصر رقم /15/ لعام 2004.
- نظام التعاملات الإلكترونية السعودي لعام 2007.
- قانون المعاملات الإلكترونية العُماني رقم 69 لعام 2008.

وقد تضمنت هذه القوانين أحكاماً قانونية تتعلق بالسجل الإلكتروني والعقد الإلكتروني والرسالة الإلكترونية والتوقيع الإلكتروني وتوثيقه وشروطه وغيرها من الأحكام. كما تضمنت **فصلاً خاصاً بالعقوبات**. حيث جرمت بعض الأفعال غير المشروعة التي يمكن أن ترافق استعمال التوقيع الإلكتروني المصادق عليه، ومن هذه الأفعال: استعمال توقيع إلكتروني عائد للغير، وتحريف أو تغيير أداة إنشاء التوقيع الإلكتروني، وقيام جهة التصديق على التوقيع الإلكتروني بإفشاء المعلومات التي عُهدت إليها، أو قيام هذه الجهة بالعمل دون ترخيص، وغير ذلك من الأفعال.

وفيما يتعلق **بجرائم المعلوماتية** ، فقد تضمن كلٌ من القانون الإماراتي (المادة 32) والقانون الأردني (المادة 38) للمعاملات الإلكترونية **نصاً عاماً** يجرم ارتكاب الجرائم التقليدية بالوسائل الإلكترونية، فعلى سبيل المثال، نصت المادة 38 من قانون المعاملات الإلكترونية الأردني رقم 58 لعام 2001 على ما يلي:

(يعاقب كل من يرتكب فعلاً يشكل جريمة بموجب التشريعات النافذة بواسطة استخدام الوسائل الإلكترونية، بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة، أو بغرامة لا تقل عن /3000/ ثلاثة آلاف دينار ولا تزيد على /10000/ عشرة آلاف دينار، أو بكلتا هاتين العقوبتين. ويعاقب بالعقوبة الأشد

إذا كانت العقوبات المقررة في تلك التشريعات تزيد على العقوبة المقررة في هذا القانون).

**ويرى الباحث** أن هذا النص قد يسعف القضاء في هذه الدول لمواجهة بعض الجرائم التقليدية التي ترتكب بوسيلة إلكترونية كالاحتيال، لكنه لا يبدو ملائماً لمواجهة جميع جرائم المعلوماتية. فلا يمكن تطبيق النص المتعلق بجريمة دخول مسكن الغير، على الدخول أو البقاء غير المشروع في نظم المعالجة الآلية للمعلومات. كما لا يمكن تطبيق النص المتعلق بجريمة إتلاف أموال الغير، على فعل إتلاف البرامج ونشر الفيروسات...

لذلك لا بد للمشرع العربي من التدخل لسن التشريعات الجزائية الكفيلة بمواجهة جميع جرائم المعلوماتية، كما فعل المشرع العُماني والسعودي والإماراتي والسوداني.

**<u>الاتجاه الثاني: الدول التي سنّت تشريعاً خاصاً لجرائم المعلوماتية</u>:**

– تعد دولة **سلطنة عُمان** أول دولة عربية تصدت لجرائم المعلوماتية، من خلال إصدارها المرسوم السلطاني رقم 2001/72، المتضمن تعديل بعض أحكام قانون الجزاء العُماني ليشمل جرائم الحاسوب. فقد جرم هذا القانون العديد من هذه الجرائم، ومنها الدخول غير المشروع إلى أنظمة الحاسوب، والالتقاط غير المشروع للمعلومات أو البيانات، وإتلاف أو محو البيانات والمعلومات، وغير ذلك من الجرائم المتعلقة بالبيانات. كما جرم هذا القانون تزوير بطاقات الائتمان واستعمالها، واستعمال البطاقة بعد انتهاء صلاحيتها أو إلغائها، أو استعمال البطاقة مع العلم بعدم وجود رصيد، واستعمال بطاقة الغير دون علمه، وغيرها من جرائم البطاقات.[1]

(1) د.عبد الفتاح مراد: المرجع السابق، ص109 . محمد عبيد الكعبي: المرجع السابق، ص55.

– أما **المملكة العربية السعودية**، فقد قامت في 31 آذار عام 2007 بإقرار نظام لمكافحة جرائم المعلوماتية، بما فيها الجرائم التي يمكن أن ترتكب عن طريق الهاتف الجوال. ويتكون هذا النظام من تسع عشرة مادة، وتتفاوت العقوبات المنصوص عليها فيه بين السجن من سنة إلى عشر سنوات، والغرامة بين خمسمئة ألف ريال إلى خمسة ملايين ريال، أو بإحدى هاتين العقوبتين.

وقد عاقب هذا النظام على العديد من الجرائم، ومنها على سبيل المثال:

- الدخول غير المشروع إلى منظومة معلوماتية لتهديد شخص أو ابتزازه.
- الاستيلاء على مال منقول أو سند أو توقيع على هذا السند أو انتحال صفة.
- الوصول دون وجه حق إلى بيانات بنكية أو ائتمانية أو أوراق مالية.
- إيقاف الشبكة المعلوماتية عن العمل أو تعطيلها أو إعاقة الوصول إلى الخدمة.
- إنتاج ما من شأنه المساس بالنظام العام أو الآداب العامة أو حرمة الحياة الخاصة.[1]

– أما **دولة الإمارات العربية المتحدة** فقد قامت بإصدار القانون الاتحادي رقم 2 لعام 2006 في شأن مكافحة جرائم تقنية المعلومات.[2]

– وفي **السودان**، فقد تم إصدار قانون جرائم المعلوماتية لعام 2007.[3]

والحقيقة أن كلا القانونين الإماراتي والسوداني قد تضمنا أحكاماً موضوعية تفصيلية لجرائم المعلوماتية، إلا أنهما لم يتضمنا الأحكام الإجرائية اللازمة لمكافحة هذه الجرائم.

---

(1) موقع جريدة الرياض على الإنترنت www.alriyadh.com.

(2) عبد الله عبد الكريم عبد الله: المرجع السابق، ص63. والقانون متوفر على الإنترنت www.aecert.ae/uaelaw-ar.html

(3) متوفر هذا القانون على الإنترنت www.uicuudan.gov.sd

كما برز بوضوح التشابه بين هذين القانونين لجهة التقسيم والصياغة، وذلك بسبب وحدة مصدرهما، وهو القانون العربي الاسترشادي النموذجي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها، الذي اعتمدته جامعة الدول العربية عبر الأمانة الفنية لمجلس وزراء العدل العرب، وذلك في الدورة التاسعة عشرة لهذا المجلس بالقرار رقم 495- د19- 2003/10/8، كما تم اعتماده من مجلس وزراء الداخلية العرب في دورته الحادية والعشرين بالقرار رقم 417، د2004/21.[1]

أما بالنسبة للأحكام القانونية التي جاء بها كلا القانونين الإماراتي والسوداني، فإننا وحرصاً على عدم التكرار، سوف نتناولهما في المطلب القادم، وذلك من خلال دراسة الأحكام القانونية التي تضمنها القانون العربي الاسترشادي المشار إليه، لأنه كما ذكرنا هو مصدر هذين القانونين.

**- الوضع التشريعي في سورية:**

صدر مؤخراً في سورية قانون التوقيع الإلكتروني وخدمات الشبكة رقم 4 تاريخ 2009/2/25[2]، وقد تضمن هذا القانون **فصلاً خاصاً** يتعلق بالجرائم المرتبطة بالتوقيع الإلكتروني، كتزويره، أو استعمال التوقيع المزور، أو تقديم معلومات غير صحيحة للحصول على شهادة المصادقة على التوقيع الإلكتروني، وغير ذلك من الجرائم.

---

(1) سنتناول هذا القانون النموذجي في المطلب القادم.

(2) كان الباحث ممثلاً لوزارة العدل في اللجنة التي أعدت هذا القانون. قرار السيد وزير الاتصالات والتقانة رقم 24/179 تاريخ 2008/1/16 حول تشكيل لجنة لإعداد مشروع قانون التوقيع الإلكتروني.

أما على صعيد **جرائم المعلوماتية**، فلا يوجد في سورية حتى تاريخ إعداد هذه الرسالة قانون يكافح جرائم المعلوماتية والإنترنت، إلاَّ أن هناك حزمة من القوانين الإلكترونية يتم إعداد مشاريعها من قبل الوزارات المعنية، وقد شُكّلت عدة لجان من مندوبي هذه الوزارات لوضع مشاريع هذه القوانين، وهذه المشاريع هي:

- مشروع قانون المعاملات والتجارة الإلكترونية.[1]
- مشروع قانون الصحافة الإلكترونية.[2]

وقد تضمنت هذه المشاريع نصوصاً تجّرم بعض الأفعال المخالفة لأحكامها والتي تدخل ضمن الجرائم المعلوماتية.

- **<u>مشروع قانون مكافحة الجريمة الإلكترونية</u>**[3]:

تمّ تشكيل لجنة من المختصين التقنيين والقانونيين لإعداد مشروع قانون مكافحة الجريمة الإلكترونية، وقد حاولت هذه اللجنة الاستفادة من القانون العربي الاسترشادي لمكافحة جرائم تقنية أنظمة المعلومات، ومن التجارب التشريعية الأجنبية والعربية، إضافةً إلى الاتفاقية الأوربية لمكافحة الجريمة الافتراضية لعام 2001.

---

(1) قرار السيد وزير الاقتصاد والتجارة رقم 16037 تاريخ 9/17 2007 وكتاب وزير الاقتصاد رقم (26/413/16960 ص.أ) تاريخ 2008/8/25، الموجه إلى وزارة العدل، وقرار السيد وزير العدل رقم 12436 تاريخ 2008/9/3 وذلك حول تشكيل لجنة مهمتها إعداد الصيغة النهائية لمشروع قانون المعاملات والتجارة الإلكترونية، وقد كان الباحث ممثلاً لوزارة العدل في هذه اللجنة.

(2) قرار السيد وزير الإعلام رقم (1/7/187) تاريخ 2007/7/23) وقرار السيد وزير العدل رقم 9830 تاريخ 2007/8/6 حول تشكيل لجنة لإعداد مشروع قانون الصحافة الإلكترونية، وقد كان الباحث ممثلاً لوزارة العدل في هذه اللجنة.

(3) كتاب السيد وزير الاتصالات والتقانة رقم (28/3000) تاريخ 2008/9/9 الموجه إلى وزارة العدل، وقرار السيد وزير العدل رقم 13113 تاريخ 2008/9/15 حول تشكيل لجنة لإعداد مشروع قانون مكافحة الجريمة الإلكترونية، وقد كان الباحث ممثلاً لوزارة العدل في هذه اللجنة.

وبعد أن انتهينا من دراسة التشريعات المتعلقة بجرائم المعلوماتية على الصعيد الوطني، سنشرع بدراسة الاتفاقيات الإقليمية المتعلقة بهذه الجرائم.

# المطلب الثاني
# الاتفاقيات على الصعيد الإقليمي

قبل الدخول في دراسة الاتفاقيات الدولية ذات الطابع الإقليمي، لا بد من الإشارة إلى أن هناك توصيات صادرة عن مؤتمرين شهيرين فيما يتعلق بجرائم المعلوماتية، هما:

**الأول: القرار الصادر عن مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة السجناء:**

عقد هذا المؤتمر في هافانا عام 1990، وقد خرج بالعديد من التوصيات، كتحديث القوانين بغرض مكافحة جرائم الحاسوب، وتحسين تدابير الأمن والوقاية المتعلقة بهذه الجرائم، وتدريب القضاة والمسؤولين على كيفية التحقيق والمحاكمة فيها، والتعاون مع المنظمات المهتمة بهذا الموضوع، وغير ذلك من التوصيات.[1]

**الثاني: المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات:**

عُقد هذا المؤتمر في البرازيل "ريو دي جانيرو" في الفترة الواقعة من 4 إلى 9 تشرين الأول عام 1994، وقد خرج بالعديد من التوصيات، منها ما يتعلق بوضع قائمة بالحد الأدنى للأفعال المتعين تجريمها واعتبارها من قبيل جرائم الحاسوب، ووجوب تحديد الجهات التي تقوم بإجراء التفتيش والضبط، وضرورة وضع القواعد المتعلقة بالإثبات الإلكتروني ومصداقية الأدلة، وغير ذلك من التوصيات.[2]

---

(1) د.عبد الله عبد الكريم عبد الله: المرجع السابق، ص107.

(2) د.عبد الله عبد الكريم عبد الله: المرجع السابق، ص111 . د.عبد الفتاح مراد: المرجع السابق، ص240.

أما على صعيد الاتفاقيات الإقليمية، فإننا سنتناول اتفاقيتين هما: الاتفاقية الأوربية حول الجريمة الافتراضية، والمعروفة باتفاقية "بودابست" لعام 2001. والاتفاقية العربية المتعلقة بالقانون العربي الاسترشادي (النموذجي) لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها لعام 2003.

## أولاً- الاتفاقية الأوربية حول الجريمة الافتراضية (اتفاقية بودابست لعام 2001) [1]:

بتاريخ 2001/11/23 في بودابست "المجر"، قامت ست وعشرون دولة أوربية بالتوقيع على أول اتفاقية تكافح جرائم الإنترنت، كما قامت أربع دول من غير الأعضاء في المجلس الأوربي بالمشاركة في إعداد هذه الاتفاقية والتوقيع عليها أيضاً، وهي كندا واليابان وجنوب أفريقيا والولايات المتحدة الأمريكية (المادة 36 من الاتفاقية).

وقد استغرقت المفاوضات بين الدول الموقعة على هذه الاتفاقية أربعة أعوام حتى تم التوصل إلى الصيغة النهائية المناسبة. ورغم أن هذه الاتفاقية هي في الأصل أوربية الميلاد، إلا أنها دولية الطابع، لأنها مفتوحة، أي تسمح بانضمام دول أخرى من غير المجموعة الأوربية (المادة 48). إلا أن هذه الدعوة للانضمام لا تسلخ عنها أنها اتفاقية تم إعدادها في إطار المجموعة الأوربية.[2]

---

(1) Europe Convention On Cyber-crime هذه الاتفاقية متوفرة على الموقع الإلكتروني conventions.co.int

(2) د. عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت, المرجع السابق، ص216. د. سليمان فضل، المرجع السابق، ص430 . راجع في المراحل التي مرت بها الاتفاقية Allen Hammond, Santa Clara University, The 2001 Council Of Europe Convention On Cyber- Crime An efficient Tool To Fight Crime On Cyber- space, p- 42.

وتتكون هذه الاتفاقية من 48 مادة موزعة على أربعة فصول، هي:

**الفصل الأول:** تضمن تعريفاً للمصطلحات الأساسية (المادة1).

**الفصل الثاني:** وجاء تحت عنوان الخطوات الواجب اتخاذها على الصعيد الوطني. وهو مؤلف من ثلاثة أقسام: الأول يضم المواد من 2 إلى 13 التي تعالج النصوص الموضوعية لجرائم الحاسوب. والثاني يضم المواد من 14 إلى 21 وتتعلق بالقواعد الإجرائية. والثالث يضم المادة 22 ويتعلق بالاختصاص.

**الفصل الثالث:** وجاء تحت عنوان التعاون الدولي، وهو من المادة 23 حتى 35.

**الفصل الرابع:** ويتضمن الأحكام الختامية من المادة 36 وحتى 48.

وبعد هذا التمهيد للاتفاقية الأوربية، سنلقي الضوء على أبرز الأحكام الموضوعية والأحكام الإجرائية التي جاءت بها الاتفاقية، بالإضافة إلى مسألة الاختصاص.

## أ- الأحكام الموضوعية:

فيما يتعلق بالأحكام الموضوعية، فقد تضمنت الاتفاقية أربع طوائف رئيسية لجرائم الحاسوب، وطائفة خامسة تتعلق بقواعد المساهمة بالجريمة والعقوبات المفروضة لهذه الطوائف الأربعة. وهذه الطوائف هي على النحو التالي: [1]

**الطائفة الأولى: الجرائم التي تستهدف عناصر أمن المعلومات،** وهي الجرائم ضد السرية والسلامة ووجود بيانات الحاسوب. وتشمل جريمة الدخول غير المشروع (المادة2)، وجريمة المراقبة أو الاعتراض غير المشروع (المادة3)، وجريمة التداخل أو التشويش على البيانات (المادة4)، وجريمة

(1) راجع الاتفاقية الأوربية المواد من 2 حتى 13. د. عبد الله عبد الكريم عبد الله: المرجع السابق، ص130-131.

إتلاف أو تعديل نظام الحاسوب (المادة 5)، وجريمة إساءة استخدام الأجهزة (المادة6).

**الطائفة الثانية: الجرائم المرتبطة بالحاسوب**، وتشمل التزوير المرتبط بالحاسوب (المادة7)، والاحتيال المرتبط بالحاسوب (المادة8).

**الطائفة الثالثة: الجرائم المرتبطة بالمحتوى**، وتشمل جريمة واحدة، وهي جريمة دعارة الأطفال (المادة9).

**الطائفة الرابعة: الجرائم المرتبطة بحق المؤلف والحقوق المجاورة**، وتشمل الجرائم التي تعد اعتداءً على المصنفات المحمية بحق المؤلف والحقوق المجاورة (المادة10).

**الطائفة الخامسة: المساهمة الجرمية والعقوبة**، ويعالج هذا الفصل الشروع والمساعدة والتحريض (المادة11)، ومسؤولية الأشخاص المعنوية (المادة12)، ومعايير العقاب (المادة 13).

واستناداً إلى المواد المشار إليها (من 2 وحتى 13) فإن الاتفاقية تلزم الدول الموقعة عليها بأن تتخذ التدابير التشريعية اللازمة لتجريم تسع جرائم في إطار جرائم المعلوماتية، وهي الجرائم التي أشرنا إليها ضمن هذه الطوائف.

أما **بالنسبة لجريمة الاحتيال** فقد نصت عليها المادة /8/ من الاتفاقية الأوربية تحت عنوان "الاحتيال المرتبط بالحاسوب"، حيث اعتبرت هذه المادة أن جريمة الاحتيال تقع (عندما يقوم شخص عن قصد، وبدون وجه حق، وعلى نحو يسبب خسارة في ممتلكات الغير بما يلي:

أ- أي إدخال أو تعديل أو حذف أو كتم لبيانات الحاسوب.

ب- أي تدخل في وظائف نظام الحاسوب.

وبنية احتيالية أو غير شريفة بغرض الحصول دون حق على منفعة اقتصادية لنفسه أو لغيره).

وحسب ما جاء في المذكرة التفسيرية لهذه الاتفاقية، فإن هذا النص يغطي جميع أشكال الاحتيال المرتبط بالحاسوب، ويشترط لتطبيق هذا النص أن يرتكب الجاني أحد الأفعال المذكورة في الفقرتين /أ و ب/ دون وجه حق، وأن تلحق خسارة اقتصادية في ملكية الغير (المجني عليه)، وأن يحصل الجاني لنفسه أو لغيره على منفعة اقتصادية نتيجة ارتكابه لهذه الجريمة. كما ترى هذه المذكرة أيضاً أنه يجب توافر القصد العام والقصد الخاص لدى الجاني لكي تتحقق هذه الجريمة، فالقصد العام يتجه إلى التلاعب بالحاسوب على نحو يسبب خسارة للغير، والقصد خاص المتمثل بنيّة الجاني غير الشريفة في الحصول على مكسب اقتصادي له أو لغيره.[1]

كما ألزمت الفقرة الثانية من المادة /11/ من الاتفاقية الدول الموقعة على ضرورة تجريم الشروع بالاحتيال والعقاب عليه.

و**يرى الباحث** أن نص المادة الثامنة وإن لم يأتِ على ذكر شبكة الإنترنت صراحةً، إلا أنه يشمل الاحتيال عبر الإنترنت ضمناً ، لأن النفاذ إلى الإنترنت لا يكون إلا بواسطة الحاسوب .

## ب- الأحكام الإجرائية:

نصت المواد من (14 حتى 21) من الاتفاقية الأوربية على الأحكام الإجرائية لجرائم الحاسوب. وقد تضمنت هذه المواد إلزام كل طرف في هذه الاتفاقية بتهيئة تشريعه الداخلي لتقرير السلطات والإجراءات اللازمة في مجال التحقيق بالجرائم المنصوص عليها في الاتفاقية.[2]

---

(1) د.عمر بن يونس: الاتفاقية الأوربية حول الجريمة الافتراضية (المذكرة التفسيرية)، الطبعة الثانية، مؤسسة آدم للنشر والتوزيع- مالطا، عام 2008، ص89-90.

(2) د.عمر بن يونس: الاتفاقية الأوربية حول الجريمة الافتراضية, المرجع السابق، ص113.

كما ألزمت هذه الاتفاقية الدول الأطراف –عند سن تشريعاتها الداخلية المتعلقة بجرائم الحاسوب والإنترنت– أن تراعي الاتفاقيات الدولية لحقوق الإنسان، مثل: الاتفاقية الأوربية لحماية حقوق الإنسان والحريات الأساسية لعام 1950، والميثاق الدولي حول الحقوق المدنية والسياسية لعام 1966 (المادة 15من الاتفاقية).[1]

أما فيما يتعلق **بتفتيش وضبط البيانات** المخزنة في الحاسوب، فقد أشارت المادة 19 من الاتفاقية، على ضرورة أن يكون هناك نصوص تشريعية داخلية لدى الدول الأطراف تسمح بما يلي:

- تفتيش نظام الحاسوب أو جزء منه والبيانات المخزنة فيه.
- تفتيش معالج تخزين البيانات في الحاسوب الذي يحوي على بيانات معينة.

ويدخل ضمن مفهوم معالج تخزين البيانات حسب المذكرة التفسيرية للاتفاقية الأقراص الليزرية والأقراص المرنة.[2]

كما تسمح الفقرة /2/ من المادة /19/ بمد التفتيش إلى نظام حاسوب آخر أو جزء منه، إذا كان هناك أساس يدعو إلى الاعتقاد بأن البيانات المطلوبة قد تم تخزينها في نظام الحاسوب الآخر، ويشترط أن يكون هذا الحاسوب ضمن النطاق الإقليمي.[3]

---

(1) د.عمر بن يونس: الاتفاقية الأوربية حول الجريمة الافتراضية, المرجع السابق، ص120.

(2) د.عمر بن يونس: الاتفاقية الأوربية حول الجريمة الافتراضية , المرجع السابق، ص151–152.

(3) د.عمر بن يونس: الاتفاقية الأوربية حول الجريمة الافتراضية, المرجع السابق، ص154.

أما بالنسبة إلى **ضبط البيانات** فإن الفقرة /3/ من المادة /19/ تسمح بضبط القطع الصلبة للحاسوب ووسيط التخزين، مع اتخاذ الإجراءات اللازمة للمحافظة على سلامة هذه البيانات.[1]

كما أشارت المادة /20/ من الاتفاقية إلى ضرورة اتخاذ إجراءات تشريعية لإلزام مزودي الخدمة بمساعدة الجهات المختصة لمعرفة حركة البيانات وتجميعها [2]. أما المادة /21/ فقد أشارت إلى إمكانية مراقبة محتوى البيانات أثناء عملية التراسل، وذلك من أجل تجميع الدليل ذي الطبيعة الجنائية.[3]

## ج- في الاختصاص:

أشارت المادة /22/ من الاتفاقية إلى المعايير التي يجب على الدول الأطراف اعتمادها لتقرير الاختصاص القضائي حول الجرائم المقررة في هذه الاتفاقية والمنصوص عليها في المواد من (2 وحتى 11).

ومعايير الاختصاص التي أخذت بها هذه الاتفاقية هي[4]:

- مبدأ الإقليمية.
- مبدأ نسبية الاختصاص المكاني، أو ما يعرف بالإقليم الاعتباري، أي الجرائم المرتكبة على السفن التي ترفع علم الدولة أو الطائرات المسجلة وفقاً للقانون فيها.
- مبدأ الجنسية .
- أما الفقرة /4/ من المادة /22/ فهي تسمح للدول الأطراف بأن تتخذ معايير أخرى من أجل انعقاد الاختصاص القضائي.

---

(1) د.عمر بن يونس: الاتفاقية الأوربية حول الجريمة الافتراضية, المرجع السابق، ص156.

(2) د.عمر بن يونس: الاتفاقية الأوربية حول الجريمة الافتراضية, المرجع السابق،ص169.

(3) د.عمر بن يونس: الاتفاقية الأوربية حول الجريمة الافتراضية, المرجع السابق، ص178.

(4) د.عمر بن يونس: الاتفاقية الأوربية حول الجريمة الافتراضية, المرجع السابق،ص181-185.

أما فيما يتعلق بالتعاون الدولي بين أطراف الاتفاقية، فقد جاءت أحكامه في الفصل الثالث من الاتفاقية، كما تضمن الفصل الرابع الأحكام الختامية.

## ثانياً- القانون العربي الاسترشادي (النموذجي) لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها: [1]

اعتمدت جامعة الدول العربية عبر الأمانة الفنية لمجلس وزراء العدل العرب ما سمي بقانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها ، نسبة إلى مقدم هذا المقترح وهو دولة الإمارات العربية المتحدة. حيث تم اعتماده من قبل مجلس وزراء العدل العرب في دورته التاسعة عشرة بالقرار رقم (495- د19- 2003/10/8)، كما اعتمده مجلس وزراء الداخلية العرب في دورته الحادية والعشرين بالقرار رقم (417، د2004/21).

ويتكون هذا القانون من 27 مادة، وهي على النحو التالي:[2]

المادة (1) تناولت تعريف عدة مفاهيم، وهي البيانات والبرنامج المعلوماتي والنظام المعلوماتي والشبكة المعلوماتية والموقع والالتقاط.

المادة (2) أشارت إلى عدم الإخلال بالعقوبة الأشد في حال وجود نص عقابي آخر يعاقب على الأفعال المجرمة في هذا القانون.

**أما الجرائم التي تضمنها هذا القانون، فقد جاءت في المواد من (3) إلى (22) وهي:**

---

(1) هذا القانون متوفر على موقع جامعة الدول العربية www.arableagueonline.org

(2) د. عبد الله عبد الكريم عبد الله: المرجع السابق، ص140 وما بعدها . د. سليمان فضل: المرجع السابق, ص437 وما بعدها.

- جريمة الدخول بغير حق إلى موقع أو نظام معلوماتي، مع تشديد العقوبة إذا كان الدخول بقصد إلغاء أو إتلاف أو إعادة نشر بيانات أو معلومات شخصية (المادة 3).
- جريمة تزوير المستندات المعالجة في نظام معلوماتي، أو استعمال السند المعالج المزور (المادة 4).
- ارتكاب الجاني للجرائم المنصوص عليها في المادة (3) إذا ارتكبت أثناء أو بسبب الوظيفة، أو سهّل الجاني ذلك للغير (المادة 5).
- جريمة إدخال ما من شأنه إيقاف الشبكة المعلوماتية عن العمل أو تعطيلها أو تدميرها أو إتلاف البرامج أو البيانات فيها (المادة 6).
- جريمة إعاقة الوصول إلى الخدمة أو الدخول إلى الأجهزة أو البرامج أو مصادر البيانات أو المعلومات (المادة 7).
- جريمة التنصت دون وجه حق على ما هو مرسل عن طريق الشبكة المعلوماتية (المادة 8).
- جريمة التهديد والابتزاز عن طريق الشبكة المعلوماتية (المادة 9).
- **جريمة الاحتيال** عن طريق الشبكة المعلوماتية أو الحاسوب .والتي نصت عليها المادة (10) بقولها:

(كل من توصل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها إلى الاستيلاء لنفسه أو لغيره على مال منقول أو على سند أو توقيع هذا السند، وذلك بالاستعانة بطريقة احتيالية أو باتخاذ اسم كاذب أو انتحال صفة غير صحيحة، متى كان ذلك من شأنه خداع المجني عليه، يعاقب بالحبس... والغرامة أو بإحدى هاتين العقوبتين).

- **جريمة الحصول بدون وجه حق على أرقام وبيانات بطاقات الائتمان.** وقد نصت عليها المادة (11) بقولها:

(كل من استخدم الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها، في الوصول بدون وجه حق إلى أرقام أو بيانات بطاقة ائتمانية وما في حكمها، بقصد استخدامها في الحصول على بيانات الغير أو أمواله أو ما تتيحه من خدمات، يعاقب بالحبس... والغرامة... أو بإحدى هاتين العقوبتين).

- جريمة الانتفاع بدون وجه حق بخدمات الاتصالات. والتي نصت عليها المادة (12) بقولها:

(كل من انتفع بدون وجه حق عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها بخدمات الاتصالات يعاقب بالحبس... والغرامة...).

- الجرائم المخلة بالآداب العامة والتي تتم عبر الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي(المادة 12).
- الجرائم المتعلقة بحماية حقوق الملكية الفكرية(المادة 14).
- الجرائم المتعلقة بالاعتداء على تصاميم المواقع(المادة 15).
- الجرائم المتعلقة بالاعتداء على المبادئ الدينية أو حرمة الحياة الخاصة(المادة 16).
- الجرائم المتعلقة بالاتجار بالجنس البشري(المادة 17).
- الجرائم المتعلقة بالاتجار وترويج وتعاطي المخدرات أو المؤثرات العقلية(المادة 18).

- الجرائم المتعلقة بغسل الأموال(المادة 19).
- الجـرائم المتعلقـة بتسـهيل وتـرويج البـرامج والأفكـار المخالفـة للنظـام العام(المادة 20).
- الجـرائم المتعلقـة بإنشـاء المواقـع العائـدة للجماعـات الإرهابيـة والتـرويج لأفكارها(المادة 21).
- الجرائم المتعلقة بالحصول على معلومات تمس الأمن الداخلي أو الخارجي أو الاقتصاد الوطني(المادة 22).

**أما الأحكام العامة فقد جاءت في المواد من (23) إلى (27) على النحو التالي:**

- المادة (23) تناولت جريمة التحريض أو المساعدة على ارتكاب الجرائم السابقة.
- المادة (24) قررت العقاب على الشروع بارتكاب الجرائم السابقة.
- المادة (25) جاءت بعقوبتين إضافيتين هما المصادرة وإغلاق المحل، بالإضافة إلى العقوبة الأصلية المنصوص عليها في المواد السابقة.
- المادة (26) وتتعلق بالاختصاص، حيث يختص القضاء الوطني بالنظر بالجرائم المذكورة ، ولو ارتكبت الجريمة كلياً أو جزئياً خارج إقليم الدولة، متى أضرت بأحد مصالحها.
- المادة (27) تتضمن وجوب إبعاد الأجنبي المحكوم عليه وفقاً للمواد (16 وحتى 22).

أما فيما يتعلق **بالاحتيال**، فقد ذكرنا نص المادة العاشرة من هذا القانون، التي تناولت جريمة الاحتيال عن طريق الشبكة المعلوماتية أو الحاسب الآلي. والحقيقة أن هناك **أربع ملاحظات** على النص المشار إليه، هي:

- لم يشر النص إلى أن الاستيلاء على المعلومات بطريقة احتيالية يعادل الاستيلاء على المال المنقول.
- لم يشر النص إلى أن خداع الحاسوب أو الآلة الخاضعة لسيطرة المجني عليه، يقوم مقام خداع المجني عليه ذاته.
- عدم حصر الوسائل الاحتيالية، بل كان من الأفضل عدم تحديدها، خاصة وأن هذه الوسائل مرتبطة بالتقدم التقني الذي لا يعرف حدود.
- لم يلحظ النص ضرورة تشديد العقاب عند تعدد المجني عليهم، أو إذا تجاوز مبلغ الاحتيال مليون ليرة سورية.

لذلك **يقترح الباحث** على المشرع السوري عند تجريمه للاحتيال عبر الإنترنت أن يكون النص على الشكل التالي:

( 1- كل من استولى لنفسه عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسوب، على مال منقول أو غير منقول أو معلومات أو برامج أو على سندٍ يتضمن تعهداً أو إبراءً أو أي امتياز مالي آخر، وذلك عن طريق خداع المجني عليه، أو خداع الحاسوب أو الآلة الخاضعة لسيطرة المجني عليه، بأية وسيلة كانت، يعاقب بالحبس من سنة إلى ثلاث سنوات، وبالغرامة ثلاثمائة ألف ليرة سورية.

2- إضافةً إلى الغرامة المذكورة في الفقرة الأولى، تكون العقوبة الأشغال الشاقة المؤقتة إذا وقعت الجريمة على ثلاثة أشخاص فأكثر، أو إذا تجاوز مبلغ الاحتيال مليون ليرة سورية.).

أما فيما يتعلق بالمادة (11) المتعلقة **بالحصول دون وجه حق على بيانات أو أرقام بطاقات الائتمان** بقصد الحصول على أموال الغير. **فالباحث يرى** بأن يكون النص أكثر شمولاً، بحيث يتضمن تجريم تزوير بطاقات الائتمان، واستعمال بطاقة الائتمان المزورة أو المسروقة أو المفقودة في سحب النقود أو الوفاء. كما يجب أن تشمل الحماية الجزائية البطاقات الإلكترونية أياً كان نوعها.

ولذلك **نقترح** أن يكون النص على الشكل التالي:

( يعاقب بالحبس من سنة إلى ثلاث سنوات، وبالغرامة ثلاثمائة ألف ليرة سورية على ما يلي:

1-كل من استخدم الشبكة المعلوماتية أو أحد أجهزة الحاسوب، للوصول دون وجه حق إلى بيانات أو أرقام بطاقة ائتمانية أو إلكترونية، وذلك بقصد الحصول على أموال الغير أو ما تتيحه من خدمات.

2-كل من قام بتزوير بطاقة ائتمانية أو إلكترونية بقصد الحصول على أموال الغير أو ما تتيحه من خدمات، أو كل من استعمل بطاقة ائتمانية أو إلكترونية مزورة في سحب النقود أو الوفاء.

3-كل من استعمل بطاقة ائتمانية أو إلكترونية مسروقة أو مفقودة في سحب النقود أو الوفاء.).

**وأخيراً** لا بد من الإشارة إلى أن القانون العربي الاسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها، كان موفقاً إلى حد ما في أحكامه الموضوعية، حيث شملت -كما بينا- معظم الجرائم التي يمكن أن ترتكب عن طريق الحاسوب أو عبر الإنترنت. إلا أنه يؤخذ على هذا القانون الاسترشادي عدم تعرضه للأحكام الإجرائية الضرورية لملاحقة هذه الجرائم، فلم يتعرض

لمسألة الاختصاص القضائي بشكل واضح، ولم يتضمن ما يشير إلى مدى إمكانية إخضاع البيانات أو المعلومات لإجراءات التفتيش والضبط، كما لم يتعرض إلى مفهوم الدليل الرقمي وشروطه وحجيته. وهذا ما سنعالجه في الباب الثاني من هذه الرسالة.

# الفصل الثاني
# مدى انسجام الاحتيال عبر الإنترنت
# مع مفهومه التقليدي

لمُ يعرف المشرع السوري الاحتيال في قانون العقوبات، وإنما اكتفى بذكر وسائله على سبيل الحصر في المادة /641/ من قانون العقوبات. أما الفقه فقد عرّف الاحتيال بأنه: "الاستيلاء بطريق الحيلة أو الخداع على مال مملوك للغير بنية تملّكه"[1]. فالاحتيال يتمثل في قيام الجاني بخداع المجني عليه بإحدى الوسائل التي حددها المشرع، فيقع هذا الأخير في الغلط ويسلّم ماله إلى الجاني.

وقد سبقت الإشارة إلى أن جريمة الاحتيال عبر الإنترنت تنتمي إلى طائفة الجرائم التقليدية التي تُرتكب بواسطة الإنترنت. ولمعرفة مدى انسجام الاحتيال عبر الإنترنت مع مفهومه التقليدي، لا بدّ لنا من دراسة أركان جريمة الاحتيال، أي دراسة الركن المادي والركن المعنوي.

لذلك سوف نقسم هذا الفصل إلى المبحثين التاليين:

المبحث الأول: الركن المادي.

المبحث الثاني: الركن المعنوي.

---

(1) د.علي عبد القادر القهوجي: المرجع السابق، ص759. وراجع أيضاً د.أسامة عبد الله قايد: شرح قانون العقوبات – القسم الخاص (جرائم الأموال)، دار النهضة العربية، القاهرة، 1989، ص 135. د.رؤوف عبيد: جرائم الاعتداء على الأشخاص والأموال، الطبعة الثامنة، دار الفكر العربي، القاهرة، 1985، ص 443.

# المبحث الأول

# الركن المادي

يتكون الركن المادي في جريمة الاحتيال من ثلاثة عناصر: النشاط الجرمي، والنتيجة، وعلاقة السببية.

**فالنشاط الجرمي** للاحتيال يتمثل في فعل الخداع، أي الكذب المقترن بإحدى الوسائل الاحتيالية المنصوص عليها على سبيل الحصر في المادة /641/ من قانون العقوبات. أما **النتيجة** فتتمثل بتسليم المجني عليه ماله إلى المحتال تحت وطأة الخداع. و**علاقة السببية** التي تقتضي أن يكون تسليم المال بسبب الخداع.

والواقع أن البحث في عناصر الركن المادي للاحتيال لمعرفة مدى انسجامه مع الاحتيال عبر الإنترنت، يثير العديد من الإشكاليات القانونية، منها ما يتعلق بموضوع الاحتيال، أي مدى انطباق وصف المال على المعلومات أو البرامج عندما تكون هي محل التسليم. ومنها ما يتعلق بالنشاط الجرمي، أي إمكانية وقوع فعل الخداع على الآلة أو الحاسوب، ثم مدى استيعاب الوسائل الاحتيالية لمختلف أساليب ارتكاب جريمة الاحتيال عبر الإنترنت. ومن المشكلات أيضاً ما يتعلق بالنتيجة الجرمية، كمسألة مدى اعتبار النقود الكتابية بمثابة تسليم للمال.

استناداً لذلك سنقسم هذا المبحث إلى أربعة مطالب كما يلي:

المطلب الأول: موضوع الاحتيال.

المطلب الثاني: النشاط الجرمي.

المطلب الثالث: النتيجة الجرمية.

المطلب الرابع: الصلة السببية.

# المطلب الأول
# موضوع الاحتيال

يقصد بموضوع الاحتيال "ذلك الشيء الذي يرد عليه التسليم الصادر من المجني عليه إلى المحتال نتيجة الغلط الذي أوقعه فيه"[1].

وقد حدّد المشرع السوري موضوع الاحتيال بالمادة /641/ من قانون العقوبات عندما نص بالفقرة الأولى على ما يلي: (كل من حمل الغير على تسليمه مالاً منقولاً أو غير منقول أو أسناداً تتضمن تعهداً أو إبراء فاستولى عليها احتيالاً...).

ومن ثم فإن الشروط المطلوب توافرها في موضوع الاحتيال هي: أن يكون موضوع الاحتيال مالاً مادياً، سواء أكان هذا المال منقولاً أم عقاراً، وأن يكون هذا المال مملوكاً للغير. وهذا ما سنبحثه على التتالي:

## أولاً- أن يكون موضوع الاحتيال مالاً مادياً:

إن علّة هذا الشرط هو أن الاحتيال جريمة تتضمن الاعتداء على حق الملكية، ولا يصلح محلاً للملكية إلاّ الشيء الذي له صفة المال.

ويقصد بالمال، كل شيء يصلح محلاً لحق عيني، وعلى وجه التحديد حق الملكية، والأصل أن كل شيء نافع للإنسان يصلح لأن يكون هدفاً للاستئثار وإنشاء الحقوق عليه، ولا يخرج عن هذا الأصل إلاّ الأشياء التي لا تقبل بطبيعتها أن تكون محلاً لحق عيني كالإنسان، فالإنسان لا يمكن أن يكون موضوعاً لجريمة الاحتيال، فمن يخدع فتاة ويحملها على تسليم جسدها لا

---

(1) د.محمود نجيب حسني: جرائم الاعتداء على الأموال في قانون العقوبات اللبناني، المرجع السابق، ص 382.

يرتكب هذه الجريمة. ولا يرتكبها أيضاً من يسلب حرية إنسان بالخداع أو الحيلة، فمحل هذه الجرائم ليس مالاً، وفي مثل هذه الحالات قد تتوفر جريمة الاغتصاب أو الخطف أو الحرمان من الحرية. كما يخرج عن مفهوم المال الأشياء التي لا يستطيع أحد أن يستأثر بحيازتها، كالمياه في البحار، والهواء في الجو، ولكن إذا تحددت هذه الأشياء أو احتجزت اعتبرت أموالاً. وإذا كان الشيء يصلح بطبيعته محلاً لحق عيني فهو مال، ولو كان القانون المدني يحظر التعامل فيه، كالمخدرات أو الأسلحة الممنوعة، فمن يحتال على آخر ليحصل على كمية من مخدرات يعتبر أنه ارتكب جريمة الاحتيال[1].

ويُشترط في المال أن يكون ذا طبيعة مادية، أي قابلاً للحيازة والتسليم والتملك. والشيء المادي هو "كل ماله كيان ذاتي مستقل في العالم الخارجي، أو هو كل ماله طول وعرض وسمك، بصرف النظر عن حجمه أو وزنه أو هيئته"[2].

ويستوي بعد ذلك في المال المادي أن يكون صلباً أو سائلاً أو غازيّاً. ويخرج عن مفهوم المال، الأشياء المعنوية، أي غير المادية، كالأفكار والآراء والحقوق والشعر والمخترعات الفنية، لأنها أشياء لا تدرك بالحس وليس لها كيان مادي يمكن الاستيلاء عليه. لكن هذه الأشياء تتحول إلى مالٍ ماديٍ إذا أُفرغت في وعاء مادي، كالسند أو الكتاب أو النوتة الموسيقية، أو براءة الاختراع، فالاستيلاء على هذه الأشياء بالخداع يتحقق فيه جرم الاحتيال[3].

---

(1) د.محمود نجيب حسني: جرائم الاعتداء على الأموال في قانون العقوبات اللبناني، المرجع السابق، ص34 و 384. د.علي القهوجي: المرجع السابق، ص802.

(2) د.علي القهوجي: المرجع السابق، ص664.

(3) د.علي القهوجي: المرجع السابق، ص 665.

ومتى اكتسب الشيء صفة المال؛ فإنه يصلح موضوعاً للاحتيال، سواء أكانت قيمته كبيرة أم ضئيلة، وسواء أكانت قيمته مادية أم معنوية. وتطبيقاً لذلك فإن الرسالة من شخص عزيز، أو التذكار العائلي ، يصلح أن يكون موضوعاً للاحتيال كونه ذا قيمة معنوية[1].

وبناءً على ما تقدم، فإن موضوع جريمة الاحتيال عبر الإنترنت لا يخرج عن هذا الأصل عندما يكون محل التسليم شيئاً له صفة المال المادي، كالنقود، أو المنقولات، أو العقارات، أو الأسناد التي تتضمّن تعهداً أو إبراءً. والمثال على ذلك، من يقوم بإنشاء موقع لشركة وهمية على الإنترنت، ويعرض من خلاله البضائع والسلع للبيع، ثم يستلم ثمنها عن طريق الدفع عبر الإنترنت من خلال بطاقات الائتمان، ولا يقوم بإرسال الشيء المبيع إلى المشتري. أو كمن يرسل رسالة إلكترونية تتضمن فوز المرسل إليه بجائزة، ويطلب من هذا الأخير إرسال بعض النقود من أجل تغطية كلفة شحن هذه الجائزة، وبعد أن يقوم المجني عليه بإرسال النقود المطلوبة يتبيّن بأن الجائزة وهمية. ففي مثل هذه الحالات لا يثير موضوع الاحتيال عبر الإنترنت أية مشكلة، ولكن إذا كان موضوعه المعلومات أو البرامج، فالسؤال الذي يطرح نفسه هنا: **هل ينطبق وصف المال المادي على المعلومات أو البرامج؟ بمعنى آخر، إذا قام الجاني بالدخول إلى إحدى المواقع التي تبيع البرامج عبر الإنترنت، واستخدم بطاقة**

---

(1) د.محمود نجيب حسني: جرائم الاعتداء على الأموال في قانون العقوبات اللبناني، المرجع السابق، ص385. د.علي عبد القادر القهوجي: المرجع السابق، ص803. وهناك رأي في الفقه يذهب إلى ضرورة أن يكون للمال موضوع الاحتيال قيمة مادية فقط , ويستبعد المال ذا القيمة المعنوية. راجع في هذا الرأي: د. محمود محمود مصطفى: شرح قانون العقوبات – القسم الخاص، الطبعة الثامنة، دار النهضة العربية، مطبعة جامعة القاهرة، 1984، ص 562. د.جاك الحكيم ود.رياض الخاني: شرح قانون العقوبات– القسم الخاص، مطبعة الداودي، دمشق، عام 1982، ص279.

**ائتمان مزورة في عملية الدفع الإلكتروني، واستلم البرنامج المعلوماتي عن طريق تحميله مباشرة عبر الإنترنت ، فهل يعدّ ذلك احتيالاً؟**

انقسم الفقه في إجابته على هذا التساؤل إلى اتجاهين:

**الاتجاه الأول:** يرفض أصحابه إعطاء المعلومة صفة المال، مستندين إلى أن المعلومات ليست لها صفة مادية، وأنها لا تقبل التملك والاستئثار في حالتها المجردة، وأن تداولها والانتفاع بها من حق الكافة دون تمييز، ومن ثم لا يمكن أن تكون محلاً للملكية الفكرية[1].

وهناك جانب من أنصار هذا الرأي يفرق بين المعلومات والبيانات التي تمّت معالجتها آلياً، فيرى بأن المعلومات إذا لم تعالج آلياً عن طريق الحاسوب فهي لا تعتبر من قبيل الأموال الخاضعة للحماية الجزائية. أما البيانات التي تمّت معالجتها فيصبح لها كيان مادي، يتمثل في إشارات إلكترونية يمكن تخزينها على وسائط معينة ونقلها وحجبها وبثها وإعادة إنتاجها، إضافةً إلى إمكانية قياسها لأنه أصبح لها كيان محسوس، وفي هذه الحالة تتمتع بالحماية الجزائية لأنها أصبحت أموالاً مادية. ويطلق أصحاب هذا الرأي عبارة البيانات على المعلومات المعالجة آلياً[2].

أما **الاتجاه الثاني:** فيمثله الفقه الحديث، ويرى أصحابه بأن التطور الذي حدث في مجال تكنولوجيا المعلومات، يدفع إلى البحث عن معيار جديد غير

---

(1) Goutal (Jean-Louis) , "informatique et droit prie", in bensoussan (Alain), Linant de Bellefonds, Maisl (Herbert), Emergence du droit de l,informatique ,1983,p.92

مشار إليه عند د.نائلة قورة: المرجع السابق، ص116.

(2) د.هشام محمد فريد, قانون العقوبات ومخاطر تقنية المعلومات,مكتبة الآلات الحديثة,أسيوط,2000, ص 249. مشار إليه عند د.سليمان فضل: المرجع السابق، ص76. عفيفي كامل عفيفي: المرجع السابق، ص133.

معيار مادية الشيء، يمكن من خلاله إسباغ صفة المال على الشيء المعنوي. لذلك لجأ أصحاب هذا الرأي إلى معيار **القيمة الاقتصادية للشيء**، حيث يعتبر الشيء مالاً بالنظر إلى قيمته الاقتصادية لا بالنظر إلى ما له من كيان مادي. كما يرى أصحاب هذا الاتجاه بأن القانون يعدّ منفصلاً عن الواقع إذا لم يسبغ صفة المال على الأشياء ذات القيمة الاقتصادية، ومن ثم يمكن إعطاء صفة المال لبرامج وبيانات ومعلومات الحاسوب، على أساس ما لها من قيمة اقتصادية، لذلك لا بدّ من شمولها بالحماية الجزائية[1].

ويرى أنصار هذا الاتجاه ، أن المادة هي كل ما يشغل حيزاً مادياً في فراغ معين، بحيث يمكن قياس هذا الحيز والتحكم فيه، فالبرامج أو المعلومات تشغل حيزاً مادياً في ذاكرة الحاسوب، ويمكن قياسه بمقياس معين هو البايت (BYTE)، فحجم أو سعة ذاكرة الحاسوب تقاس بعدد الحروف التي يمكن تخزينها فيها، إضافة إلى أن البيانات تكون على شكل إشارات إلكترونية ممثلة بالرقمين ( 0 أو 1)، وهي في ذلك تشبه التيار الكهربائي الذي اعتبرته بعض التشريعات من الأشياء المنقولة[2].

---

(1) Catala (Pierre) Informatique et droit penal, Travaux de l,institute de sciences criminelles de poitiers, edition cujas, 1983, p.267. مشار إليه عند د.نائلة قورة: المرجع السابق، ص119-120. وراجع أيضاً :عفيفي كامل عفيفي: المرجع السابق، ص130.

(2) علي حسن محمد الطوالبة: التفتيش الجنائي على نظم الحاسوب والإنترنت (دراسة مقارنة)، رسالة دكتوراه مقدمة إلى جامعة عمان العربية، كلية الدراسات القانونية العليا، 2003، ص30. د.علي محمود علي حمودة: الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، المنعقد في دبي من 26-28 نيسان 2003، ص 23. متوفر على الموقع www.arablawifo.com .

و**يرى الباحث** أن الاتجاه الأول الذي لا يسبغ على المعلومات المجردة صفة المال إلاّ إذا كانت مخزنة على دعامة أو وسيط[1](أي عندما يصبح لها كيان مادي) فيه شيء من التناقض، لأن المعلومات لا يمكن أن توجد مجردة عن وسائط التخزين في حال من الأحوال، فمن يقوم بالاستيلاء بطريقة احتيالية على برامج مخزنة على اسطوانة ممغنطة، لا يكون القصد الجرمي لديه متجهاً إلى الاستيلاء على الأسطوانة نفسها، بل على المعلومات المخزنة على هذه الأسطوانة. ومن ثم فمن غير المنطقي النظر إلى أن الاحتيال وقع على الأسطوانة فقط.

أما الاتجاه الثاني القائل بصلاحية البرامج أو المعلومات لأن تكون محلاً لجريمة الاحتيال، **فإن الباحث يؤيده للسببين التاليين:**

**السبب الأول:** إن المعلومات أو البرامج لها قيمة تصل إلى حد الثروات الطائلة، وكل شيء له قيمة يكتسب صفة المال، فالمعلومات والبرامج (وهي في جوهرها معلومات معالجة آلياً) التي تكون نتاج الإبداع الفكري، تصلح لأن تكون محلاً للملكية، وهي تُباع وتُشترى وتُقوّم بالمال.

وتماشياً مع هذا الاتجاه ، قام المشرع السوري بحماية المعلومات أو البرامج في قانون حماية المؤلف رقم /12/ لعام 2001، حيث نصت المادة الثالثة من هذا القانون، على حماية مصنفات البرمجيات الحاسوبية، بما في ذلك وثائق تصميمها ومجموعات البيانات.

---

(1) يقصد بالدعامة أو الوسيط، الوسيط المادي الذي يُستخدم لحفظ وتخزين ونقل البيانات أو المعلومات, مثل الأقراص المدمجة أو الأقراص الممغنطة أو الذواكر الإلكترونية أو أي وسيط آخر مشابه. (مادة 1 من قانون التوقيع الالكتروني السوري رقم 4 لعام 2009).

كما أن معظم التشريعات المقارنة أعطت المعلومات صفة المال، فالقوانين الفيدرالية الأميركية، أضفت على المال مفهوماً واسعاً بحيث يشمل كل شيء ينطوي على قيمة، ويندرج تحت هذا التعريف الأموال المعنوية والبيانات المعالجة. وتعاقب هذه القوانين على الاستخدام غير المسموح به للحاسوب، بغرض ارتكاب أفعال الغش أو الاستيلاء على الأموال[1].

و**السبب الثاني:** إن التشريع السوري من التشريعات التي أنزلت القوى المحرزة منزلة الأشياء المنقولة، وهذا ما نصت عليه الفقرة الثانية من المادة /621/ من قانون العقوبات بقولها: (إن القوى المحرزة تنزل منزلة الأشياء المنقولة في تطبيق القوانين الجزائية).

فالمعلومات أو البرامج يمكن أن تدخل في نطاق تطبيق هذه الفقرة، خاصة أن المعلومات بطبيعتها هي عبارة عن إشارات إلكترونية، تشبه إلى حد بعيد الإشارات الكهربائية التي أنزلها المشرع منزلة الأشياء المنقولة في تطبيق القوانين الجزائية. ومن ثم يمكننا أن نعدّ المعلومات مفهوماً يندرج تحت مصطلح القوى المحرزة التي يحميها القانون الجزائي.

## ثانياً- أن يكون موضوع الاحتيال مملوكاً للغير:

لا يتصور الاعتداء على حق الملكية إلاّ إذا كان المال موضوع الاعتداء غير مملوك للمحتال، فإذا كان مملوكاً له أو غير مملوك لأحد، كالمال المباح، فلا يمكن تصور الاعتداء على الملكية الذي تتطلبه جريمة الاحتيال، ويعدّ الشيء مملوكاً للغير حتى ولو كانت ملكيته على الشيوع بين المحتال والمجني عليه.

---

(1) المحامي محمد أمين الشوابكة: المرجع السابق، ص 188.
Micheal Kunz and Patrick Wilson: op-cit, p12.

وعلى ذلك إذا سعى شخص لأن يسترد المال الذي يملكه ممن يحوزه بناءً على سبب غير مشروع، بل وحتى على سبب مشروع، فإنه لا يرتكب جرم الاحتيال، فمن يستعمل الخداع لاسترداد ماله من يد سارقه لا يرتكب جريمة الاحتيال. ولا تقوم هذه الجريمة أيضاً إذا سعى المالك إلى استرداد ماله بالخداع ممن يحوزه بناءً على سبب مشروع، فالمؤجر أو المودع أو المعير أو الراهن الذي يسترد ماله بالخداع من المستأجر أو الوديع أو المستعير أو المرتهن لا يرتكب احتيالاً. ويختلف الأمر في حالة الدائن، إذ لا يعتبر الدائن مالكاً لشيء من أموال مدينه، فكل ما يملكه المدين يعتبر بالنسبة للدائن مملوكاً للغير، فإذا استولى بالخداع على مال مدينه فيعتبر محتالاً[1].

وبناءً على ما تقدم، فإن هذا الشرط يتوفر فيمن يقوم بالاستيلاء على مال الغير عن طريق الاحتيال عبر الإنترنت، ويتحقق ذلك مثلاً عند قيام المجني عليه المخدوع بتحويل ماله إلى المحتال عن طريق البريد أو المصارف، أو عن طريق الدفع من خلال بطاقات الائتمان عبر الإنترنت.

أما بالنسبة إلى البرامج أو المعلومات، فإن الاستيلاء بطريق الخداع على دعامة أو وسيط مخزن عليه معلومات أو برامج يصلح لأن يكون محلاً للاحتيال، لأن الغرض من هذا الاستيلاء هو الاستحواذ على هذه المعلومات التي لا يمكن فصلها عن الدعامة أو الوسيط، وبالتالي ينتقل الشيء المعلوماتي من حيازة مالكه إلى حيازة الجاني، وكذلك الحال عند الاستيلاء على هذه المعلومات عن طريق النسخ المكرر من النسخة الأصلية. فالاستيلاء على دعامة منسوخة يقصد منه حيازة ما تحتويه من معلومات مملوكة للغير[2].

---

(1) د.محمود نجيب حسني: جرائم الاعتداء على الأموال في قانون العقوبات اللبناني، المرجع السابق، ص386. د.علي القهوجي: المرجع السابق، ص804.

(2) د.أحمد حسام طه تمام: المرجع السابق، ص483.

ومما لا شك فيه، فإن المعلومات أو البرامج تصلح لأن تكون محلاً للملكية، إذ إن قاعدة "الحيازة في المنقول سند الحائز" تنطبق على المعلومات والبرامج، ناهيك عن أن البرنامج هو ملك لمن ابتكره، وفقاً لقانون حماية الملكية الفكرية[1]، لذلك فالمعلومات أو البرامج تصلح لأن تكون محلاً لملكية الغير التي يمكن أن تقع عليها جريمة الاحتيال.

## ثالثاً- أن يكون موضوع الاحتيال منقولاً أو عقاراً:

يستوي في جريمة الاحتيال أن يكون موضوعها منقولاً أو عقاراً، وهذا هو الفرق الأساسي بين جريمة الاحتيال وجريمتي السرقة وإساءة الائتمان، إذ إن السرقة وإساءة الائتمان لا تقعان إلاّ على المنقولات.

وقد حدّد القانون المدني السوري في المادة /84/ منه الفارق بين العقار والمنقول، حيث عرف العقار بأنه: (كل شيء مستقر بحيزه ثابت فيه لا يمكن نقله منه دون تلف، وكل ما عدا ذلك من شيء فهو منقول).

فالعقار في إطار القانون المدني، هو كل شيء مستقر بحيزه، ثابت فيه، لا يمكن نقله منه دون تلف، ويدخل في هذا المفهوم، **العقار بطبيعته** كالأرض أو البناء والمناجم والمقالع، **والعقار بالاتصال**، وهو المنقولات المتصلة بالعقار اتصال قرار، وتكون متممة له، كالأبواب والنوافذ والأدوات الصحية المثبتة بأماكنها. **والعقار بالتخصيص**، وهو المنقول الذي يضعه صاحبه في عقار يملكه رصداً على خدمة هذا العقار أو استغلاله، كتخصيص صاحب الأرض جراراً من أجل الزراعة[2].

---

(1) د.هدى حامد قشقوش: جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، بلا عام، ص58.

(2) د.وحيد الدين سوار: الحقوق العينية الأصلية، منشورات جامعة دمشق، 1993، ص30 وما بعدها.

ويختلف معنى المنقول في المفهوم الجزائي عن معناه في المفهوم المدني، فالمنقول في المفهوم الجزائي هو كل مال يمكن تغييره من موضعه، أي أن يقبل الشيء النقل والحركة من مكانه، سواء أصابه تلف أم لم يصبه، وسواء كان جزءاً من العقار أم لم يكن.

فبالإضافة للمنقول بطبيعته كالملابس والأثاث والسيارات والسندات وغيرها، يعدّ منقولاً صالحاً لجريمة الاحتيال، العقار بالتخصيص كالآلات الزراعية وآلات المصانع وغيرها، والعقار بالاتصال وهو المنقول الذي انفصل عن العقار الذي كان متصلاً به ، مثل النوافذ والأبواب[1].

وعلى الرغم من دخول الأسناد في مفهوم المال المنقول، إلاّ أنّ المشرع ذكرها صراحةً (الأسناد التي تتضمن تعهداً أو إبراءً ).

ويُقصد بالأسناد، الصكوك أو المحررات ذات القيمة المالية، أي كل ورقة تحمل تعهداً أو إبراءً. والمراد بالتعهدات، الموجبات على اختلاف موضوعاتها، ومثالها سند الدين. أما الإبراء، فيراد به كل إنهاء لموجب أياً كان سببه، ومثاله سند المخالصة[2].

ولا يقتصر تعبير الأسناد على الأسناد ذات الطبيعة المادية، بل يمتد إلى التعهد أو الإبراء في حد ذاته، ويتمثل ذلك بالحصول بطريق الخداع على التعهد أو الإبراء في سند موجود في حيازة المجني عليه، دون أن يحصل المحتال على السند ذاته، كأن يستطيع المحتال أن يحمل المجني عليه بالخداع على أن يثبت في دفتره اسمه على أنه يستحق مالاً في ذمته، أو على أن يحذف من دفتره مبلغاً كان ثابتاً في ذمة المحتال[3].

---

(1) دعلي القهوجي :المرجع السابق, ص668.

(2) د.علي القهوجي: المرجع السابق، ص 805.

(3) د.محمود نجيب حسني: جرائم الاعتداء على الأموال في قانون العقوبات اللبناني، المرجع السابق، ص 389.

وتطبيقاً لما تقدم، فإذا استطاع المحتال أن يخدع مالك العقار من خلال الإنترنت بأن يوهمه أنه رجل أعمال معروف، وأن لديه رصيداً مرتفعاً في بطاقة ائتمانه التي سيدفع ثمن العقار من خلالها بعد التسجيل، وحمل بذلك المالك على تسجيل عقاره على اسمه، فإن عمله يشكّل جرم الاحتيال الواقع على عقار إذا تبيّن بأن المحتال لا يملك ثمن هذا العقار وأن بطاقة ائتمانه كانت مزورة.

أما بالنسبة إلى طبيعة البرامج والمعلومات، فهي من المنقولات، لأنه عند تشغيل الحاسوب تنتقل هذه المعلومات من ذاكرة الحاسوب إلى الشاشة، ثم إلى ذهن المتلقي، وهي عبارة عن إشارات إلكترونية تشبه التيار الكهربائي القابل للانتقال، على الرغم من عدم حيازته المادية[1].

(1) د.هدى حامد قشقوش: المرجع السابق، ص56.

## المطلب الثاني
## النشاط الجرمي (فعل الخداع)

يقصد بفعل الخداع ، "تغيير الحقيقة في واقعة ما، تغييراً من شأنه وقوع المجني عليه في غلط يدفعه إلى تسليم ماله إلى الجاني"[1].

فجوهر الخداع هو الكذب الذي يتخذه الجاني حيال المجني عليه، ولكن لا يكفي الكذب المجرد لتحقيق النشاط الجرمي، بل يلزم أن يقترن بإحدى الوسائل الاحتيالية الخمسة المنصوص عليها على سبيل الحصر في المادة /641/ من قانون العقوبات، حيث نصت هذه المادة على ما يلي:

(1-كل من حمل الغير على تسليمه مالاً منقولاً أو غير منقول أو أسناداً تتضمن تعهداً أو إبراءً فاستولى عليها احتيالاً:

إما باستعمال الدسائس.

أو بتلفيق أكذوبة أيّدها شخص ثالث ولو عن حسن نية.

أو بظرف مهّد له المجرم أو ظرف استفاد منه.

أو بتصرفه بأموال منقولة أو غير منقولة وهو يعلم أن ليس له صفة للتصرف بها.

أو باستعماله اسماً أو صفة كاذبة.

عوقب بالحبس من ثلاثة أشهر إلى سنتين، وبالغرامة من مائة إلى خمسمائة ليرة.

2- يطبق العقاب نفسه في محاولة ارتكاب هذا الجرم.).

وفيما يتعلق **بعدد الوسائل الاحتيالية**، فهناك جانب من الفقه يرى أن عدد الوسائل المذكورة في المادة 641 من قانون العقوبات هي ثلاث وسائل

---

(1) د.علي القهوجي: المرجع السابق، ص762.

فقط ، لأنه ليس هناك اختلاف من حيث العناصر والطبيعة القانونية بين الوسيلة الأولى (استعمال الدسائس)، وبين الوسيلتين الثانية والثالثة، إذ إن الأخريين ليستا مستقلتين عن الأولى، بل هما مجرد تفصيل وتوضيح لهما[1].

وهناك جانب آخر من الفقه يرى بأن الوسائل الاحتيالية هي خمسة، لأن الوسيلة الأولى هي عبارة عن نموذج عام، والوسيلتين الثانية والثالثة عبارة عن نموذج خاص يتضمن جميع عناصر النموذج العام ويضيف إليه عناصر مخصصة[2].

و**الباحث** يؤيد هذا الرأي الأخير، لأن المشرع في المادة /641/ من قانون العقوبات حدّد الوسائل الاحتيالية بخمس، ولا يمكن أن نعتبر الوسيلتين الثانية والثالثة من قبيل التأكيد والتوضيح، فالأصل أن المشرع لا يلغو عند سنّه للتشريع.

وبناءً على ذلك فإنه يتطلب لقيام فعل الخداع، أن يتوفر الكذب أولاً، وأن يتم هذا الكذب بإحدى الوسائل الاحتيالية الخمسة، المحددة بنص المادة /641/ من قانون العقوبات .

## أولاً- الكذب:

الكذب هو تغيير للحقيقة ينصب على واقعة، ويترتب عليه خلق الاضطراب في عقيدة شخص وتفكيره بجعله يعتقد غير الحقيقة، وهو ما يعني وقوعه في غلط[3].

---

(1) د.محمود نجيب حسني: جرائم الاعتداء على الأموال في قانون العقوبات اللبناني- دراسة مقارنة، دار النهضة العربية، بيروت، 1984، ص224- 225.

(2) د.عبد الفتاح الصيفي: قانون العقوبات اللبناني- جرائم الاعتداء على أمن الدولة وعلى الأموال، دار النهضة العربية، بيروت، 1972، ص369-370.

(3) د.محمود نجيب حسني: جرائم الاعتداء على الأموال في قانون العقوبات اللبناني، الطبعة الثالثة، عام 1998، المرجع السابق، ص301.

ويستوي أن يكون الكذب شفوياً أو مكتوباً، بل يمكن أن يكون بالإشارة متى كان لها دلالة معروفة عند المجني عليه فتوقعه بالغلط. كما يستوي أن يكون الكذب كلياً أو جزئياً، فمن يدعي بأن لديه شركة تحقق أرباحاً طائلة، يعتبر قوله كذباً على الرغم من وجود هذه الشركة وتحقيقها للأرباح، إذا كانت هذه الأرباح غير طائلة في الحقيقة.

والعبرة في الاعتداد بالكذب هو الوقت الذي صدر فيه، دون أي وقت آخر، سابق أو لاحق، فمن ذكر أن شركة تحقق أرباحاً طائلة، يعدّ كاذباً إذا لم تكن تحقق مثل تلك الأرباح في الوقت الذي تكلم فيه، حتى ولو كانت تحقق هذه الأرباح في الماضي[1].

والكذب المجرد لا يكفي لقيام جريمة الاحتيال، فإذا صدر عن شخص كذب مجرد، فاقتنع به المجني عليه ووقع في الغلط وسلّم إليه ماله، فلا تقوم هنا جريمة الاحتيال، وعلة هذه القاعدة أن الأصل في الناس ألاّ يستسلموا لمجرد المزاعم دون أن يكون هناك ما يؤيدها، فإذا أفرط شخص في الثقة وكان مقصراً فلا يلومنَّ إلاّ نفسه. ومن ثم لا مبرر لأن يتدخل المشرع بالعقاب إزاء من يقوم بالكذب، فالأقوال الكاذبة ولو اقترنت بالأيمان المغلظة أو الإلحاح المتكرر حتى أثرت بالمجني عليه ودفعته إلى تسليم ماله إلى المدعى عليه، فلا تتكون هنا جريمة الاحتيال. وإذا كان الكذب المجرد لا تقوم به جريمة الاحتيال، فمن باب أولى أن الكتمان لا يكفي لتجسيد الخداع، لأنه موقف سلبي محض[2].

---

(1) د.علي القهوجي: المرجع السابق، ص763.

(2) د.محمود نجيب حسني: جرائم الاعتداء على الأموال في قانون العقوبات اللبناني، الطبعة الثالثة، عام 1998،المرجع السابق، ص320. د.علي القهوجي: المرجع السابق، ص767. العلامة رينيه غارو: موسوعة قانون العقوبات العام والخاص، عشرة مجلدات, منشورات الحلبي الحقوقية، بيروت، عام 2003، ترجمة المحامية لين صلاح مطر، المجلد الثامن، ص247.

وقد استقر القضاء على ذلك مقرراً أن (الكذب العادي لا يشكّل جرم الاحتيال الذي يجب أن يُبنى على الغش والخداع)[1]. فالكذب يترتب عليه نشوء عقيدة وهمية لدى المجني عليه، و العقيدة الوهمية تعني الاقتناع بصحة الكذب، أو بتعبير آخر وقوع المجني عليه في الغلط.

**ثانياً– الوسائل الاحتيالية:**

لا يكفي الكذب لتكوين فعل الخداع، بل يجب أن يترافق هذا الكذب مع إحدى وسائل الاحتيال التي حددها المشرع في المادة /641/ من قانون العقوبات، ذلك لأن هذه الجريمة من الجرائم ذات القالب المحدد التي تتطلب أن يتم النشاط الجرمي فيها بوسائل محددة، فالكذب الذي لا يقترن بإحدى الوسائل الاحتيالية لا تقوم به جريمة الاحتيال[2].

وقبل الدخول في شرح هذه الوسائل لا بدّ لنا من ذكر بعض الملاحظات المتعلقة بالنشاط الجرمي لجريمة الاحتيال عبر الإنترنت وهي:

- لزوم مباشرة نشاط تقني لارتكاب جريمة الاحتيال عبر الإنترنت، لأن النشاط الجرمي يبدأ من الحاسوب الذي يوفر النفاذ إلى هذه الشبكة، ومن ثم يجب أن يتمتع الجاني بالقدر الكافي من المعرفة التقنية لارتكاب هذه الجريمة. ويترتب على ذلك أنه لا يمكن إدانة شخص بهذه الجريمة لمجرد اعترافه، إذا لم يكن يعلم عن الحاسوب والإنترنت شيئاً[3].

---

(1) نقض سوري رقم /1332/ أساس /981/ تاريخ 1994/5/2، مجموعة أحكام النقض في قانون العقوبات والقوانين المتممة من عام 1988 حتى 2001، إعداد عبد القادر جار الله: الطبعة الأولى، المكتبة القانونية، دمشق، عام 2001، ص21.

(2) د.علي القهوجي: المرجع السابق، ص764.

(3) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت، المرجع السابق، ص256.

- إن الدخول غير المصرح به إلى نظام معلوماتي يخص الغير، يعدّ أحد العناصر الضرورية لبعض أساليب جريمة الاحتيال عبر الإنترنت، كمن يخترق النظام المعلوماتي لأحد المصارف عبر الإنترنت، ليقوم بإجراء تحويلات مالية لمصلحته. وفي أغلب التشريعات قد يشكّل الدخول غير المصرّح به جريمة في حد ذاته، إضافةً إلى كونه الوسيلة إلى ارتكاب جرائم أخرى مثل الاحتيال(1).
- تقدم تقنية الإنترنت للمحتالين القدرة على الاتصال الإلكتروني بملايين الضحايا حول العالم، وذلك بكلفة أقل بكثير من وسائل الاتصال التقليدية كالهاتف.
- يستطيع المحتالون من خلال الإنترنت أن يخفوا هوياتهم الحقيقة، الأمر الذي يجعل من الصعب ملاحقتهم ومحاكمتهم(2).

وبعد أن انتهينا من هذه الملاحظات، سنشرع بدراسة الوسائل الاحتيالية الواردة في المادة /641/ من قانون العقوبات.

**أ- استعمال الدسائس:**

يقصد باستعمال الدسائس القيام بعمل ظاهري يجعل للخداع وجوداً حسياً، فيعطي الوقائع الكاذبة التي يدعيها الفاعل مظهر الحقيقة والواقع(3).

ووفقاً لهذا المفهوم، فإن معظم جرائم الاحتيال من الممكن أن تلاحق بوصف استعمال الدسائس، لأنه ذو مفهوم واسع يشمل مختلف وسائل الاحتيال. فالأعمال أو المظاهر الخارجية التي تعطي للكذب وجوداً حسياً يصعب حصرها، لأنها متطورة ومتجددة تبعاً لتطور جوانب الحياة، وخاصة

---

(1) Micheal Kunz and Patrick Wilson: op- cit, P 17 .

(2) Richard Hillman: securities fraud, The internet poses challenges to Regulateres and Investors, United States General Accounting Office, 1999, P4.

(3) د.جاك الحكيم ود.رياض الخاني: المرجع السابق، ص367.

الاختراعات التي يكشف عنها العلم. ولا يشترط في هذه الأعمال أو المظاهر الخارجية سوى أن يكون لها كيان مستقل عن الكذب، أي أن لا تكون مجرد ترديد له، وإنما هي ذلك الجديد الذي يُضاف إلى الكذب ليدعمه ويحمل على الاعتقاد بصحته وصدقه[1].

والمظاهر الخارجية التي تدعم الكذب في استعمال الدسائس يجب أن لا تتمثل بتدخل شخص ثالث، لأن هذه الحالة تدخل ضمن الوسيلة الثانية من وسائل الاحتيال وهي تلفيق أكذوبة أيّدها شخص ثالث ولو عن حسن نيّة. كما يجب أن لا تتمثل تلك المظاهر بشيء يعتبر ظرفاً مهّد له المحتال أو استفاد منه، لأن هذه الحالة تدخل ضمن الوسيلة الثالثة من وسائل الاحتيال.

وبناء على ذلك يمكن لتوفر الدسائس أن تتمثّل المظاهر الخارجية بإحدى صورتين[2]:

**الصورة الأولى:** مظاهر خارجية متمثلة بشيء مادي أيّاً كانت ماهيته أو مادته. ومن أمثلة ذلك:

- عرض آنية نحاسية مطلية بالذهب على المجني عليه، وإيهامه بأنها أثرية ومن الذهب الخالص، فيدفع المجني عليه مبلغاً كبيراً ثمناً لها.

- إبراز المدين حافظة نقود محشوة بأوراق لا قيمة لها، لإيهام الدائن بأنه مستعد للوفاء بالتزامه، فيسلّمه الدائن سند الدين فيمزقه.

- إبراز أوراق مزوّرة تفيد بملاءة المحتال، فيحصل بناءً عليها على صفقة لم تكن لتتم لولاها.

---

(1) د.علي القهوجي: المرجع السابق، ص771.

(2) د.علي القهوجي: المرجع السابق، ص772-774.

**الصورة الثانية:** المظاهر الخارجية المتمثلة في شخص الفاعل نفسه دون سواه، بأن يخلق حول نفسه مظاهر خاصة في الحياة تدعم كذبه. ومن أمثلة ذلك:

- قيام المحتال بالتحدث مع الجن، وإشعال البخور، لإيهام المجني عليه بقدرته على شفائه من مرضه العضال عن طريق الاتصال بالجن، وحصوله على مبلغ من المال مقابل ذلك.
- اتخاذ المحتال مظهر الرجل الثري، من حيث الملبس والمسكن والتنقل بالسيارات الفاخرة، ليوهم المجني عليه بأنه من رجال الأعمال، ثم يحصل منه على الأموال للاستثمار التجاري.

وقد حاول جانب من الفقه رسم الوسائل الرئيسية للاحتيال المعلوماتي، رغم إيمان أصحابه بتنوع هذه الوسائل وتزايدها المستمر. وهذه الوسائل هي:

- التلاعب في مرحلة إدخال البيانات.
- التلاعب في مرحلة إخراج البيانات.
- التلاعب في البرامج.
- التلاعب في المكونات المادية للحاسوب.
- التلاعب في البيانات التي يتم تحويلها عن بعد.
- التلاعب في محيط الصرف الآلي.
- استعمال شفرة غير صحيحة للدخول إلى نظام مدفوع الأجر.

ويرى أصحاب هذا التصنيف بأن التلاعب في نظم البيانات، الذي يتم بطريقة التحويل عن بعد، هو من أكثر الوسائل التي يمكن أن يُرتكب بها الاحتيال عبر الإنترنت[1].

---

(1) د.نائلة قورة: المرجع السابق، ص436. د.سليمان فضل: المرجع السابق، ص202.

و**يرى الباحث** أن مفهوم استعمال الدسائس المشار إليه يشمل في معناه العام جميع هذه الوسائل، إضافةً إلى الطرق والوسائل – ولا حصر لها – التي تُرتكب بواسطتها جريمة الاحتيال عبر الإنترنت.

وفي مجال الاحتيال عبر الإنترنت يثور التساؤل التالي: **هل يمكن أن يقع الخداع على الحاسب الآلي بوصفه آلة؟** فمثلاً إذا قام الجاني عن طريق الإنترنت بالدخول إلى نظام معلوماتي عائد لأحد المصارف، وقام بخداع هذا النظام عن طريق التلاعب ببياناته بغية تحويل أموال عائدة للغير إلى حسابه، **فهل يتحقق هنا فعل الخداع؟** وفي مثال آخر، إذا قام الجاني باستعمال بطاقة ائتمان دولية مزوّرة من أجل سحب النقود من الصراف الآلي، **فهل يتحقق هنا فعل الخداع في مواجهة الآلة أو الحاسوب، علماً بأن النشاط الجرمي لم يمارس مباشرة في مواجهة المجني عليه؟**

للإجابة على هذا السؤال لا بدّ لنا من استعراض بعض المواقف الفقهية والتشريعية:

## 1- الموقف الفقهي:

هناك من يرى في الفقه الفرنسي[1] أن الاحتيال على الحواسيب لسلب المال، تتحقق به الطرق الاحتيالية باعتبارها أكاذيب تدعمها وقائع خارجية تتمثّل في المعلومات والبيانات التي يتم إدخالها إلى الحاسوب، وذلك على اعتبار أن هناك شخصاً طبيعياً يقف وراء الحاسوب، هو الذي خُدع بالطرق الاحتيالية. واستند أنصار هذا الرأي إلى بعض الأحكام التي صدرت عن القضاء الفرنسي، التي اعتبرت من قبيل الاحتيال التلاعب في عدادات المياه

---

(1) Pradel (Jean) & Feuillard (Christian) Les infraction commises au moyen de l,ordinateur , Revue de droit penal et de criminology, Juillet, 1985,p.311

مشار إليه عن د.نائلة قورة: المرجع السابق، ص560.

والكهرباء، وكذلك في الأجهزة الحاسبة في مواقف انتظار السيارات، حيث قضت محكمة النقض الفرنسية بتطبيق عقوبة الاحتيال على شخص دخل بسيارته إلى أماكن انتظار السيارات، وبدلاً من وضع النقود الأصلية في العداد، قام بوضع قطعة معدنية عديمة القيمة[1].كما قررت محكمة استئناف باريس في حكم لها عام 1990، بأن قيام المتهم بإدخال بيانات لا وجود لها إلى نظام الحاسب الآلي، بهدف إجراء عمليات تحويل إلكتروني للأموال لحساب شخص آخر دون وجه حق، يعدّ كافياً للقول بقيام جريمة الاحتيال[2].

أما الرأي الآخر في الفقه الفرنسي، فقد ذهب إلى القول بعدم تحقق الاحتيال على الحاسوب، واعتبر أن استخدام وسائل الغش والخداع في أنظمة الحاسوب لا تدخل ضمن نطاق الطرق الاحتيالية، لأن الطرق الاحتيالية يجب أن تربط بين شخصي الجاني والمجني عليه.[3]

وفي الفقه العربي، فهناك اتجاه يرى أن التلاعب في البرامج والبيانات والتغيير فيها، بما يترتب عليه إيهام المجني عليه بصحتها، ويجعله يسلم بها، يعدّ من أساليب الاحتيال، لأن الحاسوب وفقاً لهذا الاتجاه ليس سوى مجرد وسيط[4].

---

(1) Cass. Crime.10 December 1970, JCP. 1972 II, 17277 .
مشار إليه عند: د.علاء عبد الباسط خلاف: المرجع السابق، ص103. د.نائلة قورة: المرجع السابق، ص560. المحامي محمد أمين الشوابكة: المرجع السابق، ص185.

(2) C.A de Paris, 13 Fevrier 1990, Juris – Data N 022903.
مشار إليه وإلى العديد من الاجتهادات الأخرى عند د.نائلة قورة: المرجع السابق، ص 566.

(3) د.أحمد حسام طه تمام: المرجع السابق، ص543. المحامي محمد أمين الشوابكة: المرجع السابق، ص 186. لم يتضمن المرجعين المشار إليهما أسماء الفقهاء الفرنسيين, وإنما اكتفيا بذكر هذا الرأي فقط.

(4) د.هدى حامد قشقوش: المرجع السابق، ص132. د.سليمان أحمد فضل: المرجع السابق، ص90.

## 2- الموقف التشريعي:

فيما يتعلق بموقف التشريعات من مسألة مدى إمكانية تحقق جرم الاحتيال عند ممارسة الأفعال الاحتيالية على الحاسوب وإيقاعه في الغلط. فهناك اتجاهان رئيسيان هما:

### الاتجاه الأول:

تشترط تشريعات هذا الاتجاه لقيام جريمة الاحتيال، أن يكون المخدوع شخصاً طبيعياً، ومن ثم فلا يتصور خداع الحاسوب بوصفه آلة، وبالتالي لا يمكن أن تنطبق النصوص التقليدية لجريمة الاحتيال على خداع الحاسوب؛ لافتقاره إلى أحد العناصر الضرورية. ووفقاً لهذا الاتجاه، فإن نظام معالجة البيانات يفتقر إلى خاصية التفكير، وهو أمر ضروري في جريمة الاحتيال؛ لأن الخداع يقوم على فكرة أن تفوت على المجني عليه عملية التفكير في الأمور المغايرة للحقيقة. ومن التشريعات التي أخذت بهذا الاتجاه ألمانيا والدانمارك وإيطاليا واليونان والسويد واليابان ولوكسمبورغ[1].

### الاتجاه الثاني:

وفقاً لتشريعات هذا الاتجاه، يمكن تطبيق النصوص المتعلقة بجريمة الاحتيال على خداع الحاسوب أو الآلة. ومن هذه التشريعات الدول الأنجلوسكسونية مثل المملكة المتحدة وكندا وأستراليا والولايات المتحدة الأميركية[2].

---

(1) عفيفي كامل عفيفي: المرجع السابق، ص186. المحامي محمد أمين الشوابكة: المرجع السابق، ص187. محمد عبيد الكعبي: المرجع السابق، ص179.

(2) المحامي محمد أمين الشوابكة: المرجع السابق، ص187. محمد عبيد الكعبي: المرجع السابق، ص179.

وقد قام **القضاء الإنكليزي** بتطبيق نصوص قانون السرقة الصادر في عام 1978 على واقعة شهيرة، حيث أدانت المحكمة المتهم توسون (Thomson) بجرم الاحتيال، في قضية تتلخص بقيام "توسون" الذي كان يعمل كخبير للبرمجة في البنك التجاري الكويتي في الكويت، بفتح خمسة حسابات باسمه في الفروع الخمسة لهذا البنك، ثم قام بجمع معلومات حول بعض الأرصدة التي تتصف بأنها كبيرة الحجم وساكنة بنفس الوقت، أي لا يتعامل فيها أصحابها إلاّ نادراً، ثم قام بإدخال برنامج على الحاسب الآلي للبنك، ليقوم بسحب مبالغ كبيرة من هذه الأرصدة الساكنة وإيداعها في حساباته الخاصة، وبفضل خبرته، استطاع أن يبرمج عمليات السحب والإيداع بحيث لا تتم إلاّ في وقت لاحق على سفره إلى المملكة المتحدة. وبعد وصوله إلى المملكة المتحدة قام بفتح عدة حسابات في بنوك مختلفة، ثم أرسل كتاباً إلى مدير البنك في الكويت مطالباً إياه بتحويل المبالغ التي توجد في الأرصدة الخمسة الخاصة به إلى حساباته الجديدة في المملكة المتحدة، وبعد قيام مدير البنك الكويتي بتحويل المبالغ المطلوبة التي وصلت إلى /45/ ألف جنيه إسترليني، قام "توسون" بسحبها، وعندما كُشف أمره، تمت إدانته من قبل القضاء الإنكليزي بتهمة الاحتيال، وحُكم عليه بالسجن لمدة خمسة عشر شهراً[1].

وقد كان موقف القضاء الإنكليزي في هذه القضية محل **جدال** بين الفقهاء؛ فيرى البعض[2] أن إدانة المتهم بجرم الاحتيال من قبل القضاء الإنكليزي، كانت من قبيل التوسع في تفسير نصوص قانون السرقة الصادر في

---

(1) R.V Thompson, court of Appeal, 22 March 1984, 3 ALLER 565.
مشار إليه عند: د.نائلة قورة: المرجع السابق، ص 503-504.

(2) د محمد سامي الشوا, ثورة المعلومات وانعكاساتها على قانون العقوبات, دار النهضة العربية- القاهرة,1994,ص 126. مشار إليه عند المحامي محمد أمين الشوابكة: المرجع السابق، ص 187. عفيفي كامل عفيفي: المرجع السابق، ص170.

عام 1978، بحيث شمل التلاعب بالبيانات بغرض الحصول على منفعة مادية. أما البعض الآخر[1]–وهو على عكس الرأي السابق– يرى أن المحكمة أدانت المتهم بجرم الاحتيال ليس لأن هناك تلاعب ببيانات الحاسوب، بل لأن الطرق الاحتيالية تمت ممارستها في مواجهة موظفي البنك.

وعلى أي حال فقد **حسم المشرع في المملكة المتحدة** هذا الخلاف، حيث قام بتجريم كافة أنواع الخداع التي ترتكب على الحاسوب أو الآلة، وذلك من خلال **قانون الاحتيال لعام 2006** والذي أصبح نافذاً منذ تاريخ 15 كانون الثاني لعام 2007[2].

أما في **الولايات المتحدة الأميركية**، فقدُ طبقت القوانين المتعلقة بالغش في مجال الاتصالات والبريد والمصارف على الاحتيال المعلوماتي، بالإضافة إلى اندراج هذا النوع من الاحتيال تحت سلطان قانون الاحتيال وإساءة استخدام الكمبيوتر CFAA[3] الصادر عام 1984، والذي أُدرج فيما بعد ضمن القسم /1030/ من القانون الفيدرالي الذي يجرّم شتى أنواع الاحتيال المعلوماتي[4].

**ويؤيد الباحث** ما ذهب إليه الفقه العربي القائل بأن فعل الخداع يمكن أن يقع على النظم الحاسوبية ،لأن الحاسوب ليس سوى وسيط يعبّر عن إرادة المجني عليه، فهذا الأخير هو من يقوم ببرمجته وفقاً لمتطلباته، وبالتالي فخداع الحاسوب هو خداع للمجني عليه ولا يوجد هناك ما يمنع قانوناً من أن تمارس

---

(1) د.نائلة قورة: المرجع السابق، ص 559.

(2) Robin Bryant: Investigating Digital Crime, John Wile& Sons, ltd, 2008, P42.

(3) وهو اختصار لـ Computer Fraud And Abuse Act المحامي محمد أمين الشوابكة: المرجع السابق، ص189، عفيفي كامل عفيفي: المرجع السابق، ص171. محمد عبيد الكعبي: المرجع السابق، ص180.

(4) Charles Doyle: Cyber Crime: An Overview Of The Fraud Computer Fraud and Abuse Statute, 2008, P54.

الوسائل الاحتيالية على الحاسوب. وما يؤكد صحة هذا الاتجاه، ما ذهبت إليه بعض أحكام القضاء الفرنسي، بأن التلاعب بالبيانات الحاسوبية بقصد تحويل الأموال بطريقة غير مشروعة يعد من قبيل الاحتيال.

وفي مجال الاحتيال عن طريق التحويلات المصرفية، فقد استخدمت الإنترنت للولوج إلى أنظمة المصارف، والقيام بتحويلات مالية من حسابات العملاء إلى حسابات الهكرة. فقد استطاع الهكرة الروس ارتكاب خمسمائة عملية استيلاء على مصرف روسيا المركزي خلال الفترة مابين عام 1994 إلى 1996، وقاموا بتحويل مبالغ تصل إلى مائتين وخمسين مليون روبل إلى حساباتهم الخاصة. وكان المدعو "فلاديمير ليفين" وهو مبرمج حاسوب عمره 29 عاماً، أحد أقوى الهكرة الروس الذي اخترق شبكة حاسوب مصرف "ستي بنك" "Citibank" بولاية نيوجرسي الأميركية، واستولى على عدة ملايين باستخدام حاسوبه المحمول أثناء وجوده في روسيا، وبلغت قدرة هذا الهاكر أنه استطاع مراقبة التحويلات والصفقات المالية التي تتم بالمصارف، ثم قام بتحويلات مالية من حسابات عملائها إلى حسابات خاصة به سبق وأن فتحها في مصارف هولندا وفنلندا وألمانيا والولايات المتحدة، حيث وصلت قيمة التحويلات المالية المختلسة من قبله إلى اثني عشر مليون دولار أميركي. وقد أُلقي القبض عليه في إنكلترا وتمّ تسليمه إلى الولايات المتحدة الأميركية، حيث صدر بحقه حكم بالسجن مدة ثلاث سنوات في عام 1998[1].

وفي مثال آخر عن استعمال الدسائس، أنه في 27 كانون الأول عام 2000 حكم قاضِ فيدرالي في مقاطعة كاليفورنيا بالسجن لمدة سبعة وعشرين شهراً وبمبلغ مئة ألف دولار تعويضاً للضحايا، على مجموعة من الأفراد قاموا بالاحتيال التجاري عبر الإنترنت، حيث أرسلوا أكثر من /50/ مليون رسالة

(1) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت، المرجع السابق، ص409.

إلكترونية دعائية إلى الطلاب وكبار السن، طلبوا فيها الحصول على المال مقابل العمل في المنازل، وتضمنت هذه الرسائل الوعود بالعمل بالمنازل مقابل دفعات مالية، وقد أرسل معظم الضحايا المال إلى المتهمين. كما وضع المتهمون في رسائلهم عنوان بريد مزوّر لتضليل المجني عليهم، يظهر بأن الرسائل أرسلت من مزود خدمة الإنترنت Big Bear.net ، وبعد ذلك أرسل المجني عليهم الغاضبون إلى موقع مزود الخدمة المذكور أكثر من /100.000/ رسالة إلكترونية، لاعتقادهم الخاطئ بأنه هو المسؤول عن الاحتيال، الأمر الذي أدّى إلى تعطل مزود الخدمة نتيجة هذا العدد الكبير من الرسائل. وقد استعانت شركة Big Bear بثلاثة موظفين مؤقتين للرد على هذه الرسائل لمدة /6/ أشهر. كما شمل قرار المحكمة التعويض على الشركة المذكورة إضافةً إلى الضحايا [1].

## ب- تلفيق أكذوبة أيّدها شخص ثالث ولو عن حسن نية:

تختلف هذه الوسيلة عن الوسيلة الأولى وهي استعمال الدسائس، بأن هذه الأخيرة تشكّل النموذج العام للكذب المدعم بمظاهر خارجية، وهذه المظاهر يمكن أن تتمثّل بأشياء مادية أو بشخص الفاعل نفسه دون سواه. أما الوسيلة الثانية فتشكّل نموذجاً خاصاً للكذب المدعم بمظاهر خارجية، وهذه المظاهر لا تتمثّل إلاّ بتدخل شخص ثالث.

ولا شك بأن تدخل الشخص الثالث يضفي على أكاذيب المحتال حجة تجعلها مقنعة للمجني عليه، وخاصة إذا ظهر هذا الشخص الثالث بمظهر المحايد الذي لا مصلحة له من تدخله، أو كان يظهر بأنه يقصد الخير للمجني

---

(1) On line fraud and crime, op-cit, P 33 .

عليه من هذا التدخل. فالتدخل هنا عنصر مستقل عن الكذب ويشكّل الأعمال الخارجية التي تعطي للكذب مظهر الحقيقة.

ويشترط لتحقق هذه الوسيلة من وسائل الاحتيال شرطان[1]:

**الأول:** أن يكون تدخل الشخص الثالث قد تمّ بناء على سعي الجاني وتدبيره. فإذا لم يتحقق هذا الشرط فإن مسؤولية المدعى عليه لا تقوم، لأن ما صدر عنه من كذب مجرد، لا يرقى إلى مرتبة الوسائل الاحتيالية. ويستوي أن يكون المحتال متواطئاً مع المتدخل بعد أن كشف له مشروعه الإجرامي، أو أن يكون قد خدعه واستخدمه كأداة لخداع المجني عليه.

**الثاني:** أن يضيف تدخل الشخص الثالث جديداً إلى أكاذيب الجاني، فيزيد من ثقة المجني عليه. وبناء على ذلك ،لا يتوفر هذا الشرط إذا كان الشخص الثالث مجرد نائب أو رسول عن المحتال، واقتصر دوره على تبليغ أقواله كما ذكرها إلى المجني عليه.

وبعد تحقق هذين الشرطين تستوي صور التدخل ودوافعه، فقد يتخذ التدخل صورة القول الشفوي أو يتخذ صورة الكتابة، كأن يحضر الشخص الثالث أثناء حديث المحتال إلى المجني عليه، فيؤيد ما قاله، أو أن يبعث إلى المجني عليه برسالة يؤكد فيها ما ذكره المحتال.

وتطبيقاً لذلك في الاحتيال عبر الإنترنت، إذا استطاع الجاني الاستيلاء على رقم الحساب المصرفي العائد للغير والشفرة الخاصة بتحويل الأموال، وكانت شفرة التحويل حسب الاتفاق بين المصرف والعميل، هي رسالة إلكترونية تتضمن أمر التحويل، إضافةً إلى اتصال هاتفي من العميل تأكيداً للرسالة، فإذا

---

(1) د.علي القهوجي: المرجع السابق، ص778. د.محمود نجيب حسني: جرائم الاعتداء على الأموال في قانون العقوبات اللبناني، الطبعة الثالثة، عام 1998،المرجع السابق، ص324.

قام الجاني بإرسال رسالة إلكترونية تتضمن أمر التحويل، ثم أتبعها باتصال هاتفي للمصرف تأكيداً للرسالة، وزيادة في التأكيد استعان الجاني برسالة إلكترونية من عميل آخر للمصرف كان قد خدعه أيضاً وذلك لإثبات أنه هو صاحب الحساب الحقيقي، ففي هذه الحالة يتحقق أسلوب تدخل الشخص الثالث لتأكيد أكذوبة المحتال.

## جـ- ظرف مهّد له المجرم أو استفاد منه:

الظرف هو الواقعة أو الشيء الذي يربط به المحتال بينه وبين أكاذيبه لكي يدعمها.

والظرف الذي مهّد له المجرم أو استفاد منه، هو الظرف الذي أوجده غير المحتال، أي الظرف الذي من صنع غيره لا من صنعه هو[1]. وبهذا المفهوم للظرف، يظهر الفارق بين هذه الوسيلة و وسيلة استعمال الدسائس، ففي هذه الأخيرة، يقوم المحتال نفسه بصنع المظاهر الخارجية التي تدعم أكاذيبه. أما في وسيلة التمهيد لظرف أو الاستفادة منه، فلا يقوم المحتال بصنع الظرف، بل هو من صنع غيره.

والظرف الذي مهّد له الجاني، هو الظرف الذي ضمّ فيه الجاني نشاطه إليه حتى يتمكن من الاستعانة به لتدعيم أكاذيبه. ومثاله أن ينتهز المحتال فرصة مزاد أُقيم لبيع مخلفات شخصية تاريخية، فيدسّ بين المعروضات منقولاته الخاصة.

---

(1) د.علي القهوجي: المرجع السابق، ص 782. د.عبد الفتاح مصطفى الصيفي: المرجع السابق، ص 395 و 396. وعلى عكس هذا الرأي, يرى الدكتور محمود نجيب حسني – **والباحث لا يؤيده**– أن الظرف الذي مهّد له المجرم هو من صنعه, بينما الظرف الذي استفاد منه المجرم هو من صنع غيره. جرائم الاعتداء على الأموال في قانون العقوبات اللبناني، عام 1998، المرجع السابق، ص329.

أما الظرف الذي يستفيد منه الجاني، فهو الذي لا يتدخل فيه الجاني بأي نشاط وتتحقق استفادته منه بالحالة التي وُجد عليها. ومثاله أن يقدم الجاني إلى المجني عليه ورقة مالية ذات قيمة منخفضة، موهماً إياه أن قيمتها أكبر من حقيقتها، ومستغلاً في هذا تقدم المجني عليه في السن وضعف بصره وخفوت الضوء في الطريق[1].

ويدخل أيضاً في حكم الظرف الذي مهّد له المجرم أو استفاد منه، إساءة الجاني استعمال صفته الحقيقية والثقة المفروضة فيه. فقد يستفيد الجاني مثلاً من ممارسته عملاً ما فيقوم بالاحتيال. ففي فلوريدا في الولايات المتحدة الأميركية، تمكنت السلطات الأمنية من إلقاء القبض على متهمين كانا يعملان في أحد المصارف، وتمكنا من الاستيلاء على ما يقارب من مليون ومائة ألف دولار من أرصدة العملاء عن طريق إجراء ثلاثة تحويلات إلكترونية غير مشروعة، حيث استطاع أحد المتهمين وهو يعمل سكرتير لنائب مدير المصرف أن يحصل على الشفرات الخاصة بتلك التحويلات. وقد تمّ اكتشاف هذا التلاعب أثناء قيام موظفي المصرف بمراجعة بعض الأرصدة[2].

**د- تصرف المحتال بأموال منقولة أو غير منقولة وهو يعلم أن ليس له صفة للتصرف بها:**

تقوم هذه الوسيلة على عنصرين هما:

1) التصرف بأموال منقولة أو غير منقولة.

2) انتفاء الحق أو الصفة في التصرف بها.

---

(1) د.علي القهوجي: المرجع السابق، ص 783 و 784.

(2) د.نائلة قورة: المرجع السابق، ص506.

والمشرع يكتفي في هذه الوسيلة بالكذب، دون أن يكون إلى جانبه أي سلوك آخر، ولكن يشترط أن يتحقق في هذا الكذب العنصران المذكوران.

## 1- التصرف بأموال منقولة أو غير منقولة: [1]

يقصد بالتصرف كل عمل قانوني من شأنه إنشاء حق عيني أو نقله أو انقضاؤه.

والغالب في التصرف أن يكون من عقود المعاوضة كالبيع أو المقايضة، ومن الممكن أن يكون من عقود التبرع كالهبة. ويجوز أن يكون مصدر التصرف الإرادة المنفردة كالوصية إذا تعلقت بمال ليس للموصي سلطة التصرف به، وكان يفرض على الموصى له التزام بتسليم شيء.

وقد يكون التصرف متعلقاً بحق عيني أصلي كالملكية والانتفاع والارتفاق، أو متعلقاً بحق عيني تبعي كالرهن. ولكن يخرج عن نطاق التصرف كل عمل قانوني يتعلق بحق شخصي، لأن الحقوق الشخصية تقتصر على الموجبات، دون الحقوق العينية، فإذا أجّر شخص مالاً مملوكاً للغير وتقاضى بدل الإيجار، فلا تقوم جريمة الاحتيال بهذه الوسيلة، لأن الإيجار لا يعد تصرفاً بمال الغير.

ويستوي بعد ذلك أن يكون موضوع التصرف أموالاً منقولة أو غير منقولة، وإن كانت أهمية هذه الوسيلة تتضح في العقار أكثر من المنقول، فمن الممكن لغير المالك أن يحوز العقار غير المسجل ويمارس عليه مظاهر السيطرة. الأمر الذي يؤدي إلى خداع المجني عليه عند ادعاء الجاني بأنه مالك العقار.

## 2- انتفاء الحق أو الصفة في التصرف بالمال:

---

(1) د. محمود نجيب حسني: جرائم الاعتداء على الأموال في قانون العقوبات اللبناني، الطبعة الثالثة، عام 1998،المرجع السابق، ص340. د.علي القهوجي: المرجع السابق، ص787.

إن الحق في التصرف بالمال، مستمد من الحق الثابت عليه، فحق الملكية مثلاً يخول صاحبه سلطة التصرف.

أما الصفة في التصرف بالمال، فتفترض أن المتصرف ليس صاحب الحق على المال، ولكن له صفة تخوله ذلك، ومصدر هذه الصفة هو النيابة عن صاحب الحق. وقد تكون هذه النيابة قانونية كنيابة الولي، أو تكون قضائية كنيابة الوصي أو القيّم، أو اتفاقية كنيابة الوكيل.

وقد يكون هناك سبب قانوني يحرم المالك من سلطة التصرف بماله، فإذا تصرف هذا المالك بالمال، فهو يتصرف بمال ليس له صفة التصرف به، كالمدين المحجوز عليه حجزاً تنفيذياً، إذ يقيد هذا الحجز سلطة المالك كي يحقق الحجز غرضه القانوني في تمكين الدائن الحاجز من الحصول على حقه. ومن الحالات التي تتقيد بها سلطة المالك أيضاً حالة تقييد الملكية بشرط المنع من التصرف، عندما يكون هذا الشرط صحيحاً[1].

ومن الجدير بالذكر بأنه يوجد العديد من المواقع المتخصصة في بيع المنقولات والعقارات على شبكة الإنترنت، ومن أشهر هذه المواقع التجارية موقع e-bay الشهير، حيث يقوم الباعة بعرض ما يرغبون ببيعه عن طريق هذا الموقع. فمثلاً إذا قام شخص بعرض حاسوب للبيع عن طريق أحد هذه المواقع الإلكترونية، وتسلّم ثمنه من المشتري عن طريق الدفع من خلال بطاقات الائتمان، ولم يقم البائع بشحن هذا الحاسوب إلى المشتري، بل قام ببيعه مرة أخرى، فهنا تتحقق هذه الوسيلة من وسائل الاحتيال.

## هـ- استعمال المحتال اسماً مستعاراً أو صفة كاذبة:

(1) د. محمود نجيب حسني: جرائم الاعتداء على الأموال في قانون العقوبات اللبناني، الطبعة الثالثة، عام 1998،المرجع السابق، ص346. د.علي القهوجي: المرجع السابق، ص789.

تتحقق هذه الوسيلة عند صدور كذب من المحتال يتعلّق باسمه أو صفته، فينخدع المجني عليه بهذا الاسم أو الصفة الكاذبة، ويقع في الغلط، ويقدم على تصرف مالي تحت تأثير هذا الغلط. ويفترض أن الاسم أو الصفة الكاذبة يرتبطان بقدر من الثقة لا يتوفر للاسم أو الصفة الحقيقية، أو على الأقل يخفيان سوء الظن المرتبط بهما.

ومن الملاحظ أن المشرع في هذه الوسيلة قد اكتفى بالكذب المجرد، دون أن يقترن بالمظاهر الخارجية، أي أن الكذب بالاسم أو الصفة الذي يؤدي إلى حمل الغير على تسليم المال يعدّ كافياً لقيام هذه الوسيلة، دون اشتراط تدعيم هذا الكذب بمظاهر خارجية.

ويشترط في هذه الوسيلة أن يصدر عن الجاني نشاط إيجابي ينتحل به الاسم أو الصفة الكاذبة، أي أن ينسب هذا الاسم أو الصفة الكاذبة لنفسه لا لغيره. وأن يكون الاسم أو الصفة الكاذبة مما ينخدع الناس به ، أي ألاّ يكون الكذب مفضوحاً. ويكفي أن يتخذ الجاني لنفسه اسماً أو صفة غير صحيحة، فلا يشترط أن يتخذهما معاً. ويستوي بعد ذلك أن يعبر الجاني عن هذا الكذب شفاهة أو كتابة[1].

## 1- الاسم المستعار:

يقصد بالاسم المستعار كل اسم غير الاسم الحقيقي للمحتال، سواء كان هذا الاسم لشخص حقيقي آخر أم خيالي. ويستوي أن يكون الاسم المستعار مختلفاً عن الاسم الحقيقي كلياً أو جزئياً، كما لو غير المحتال أحد ألفاظ الاسم، أو أضاف إليه لفظاً، أو عدل من ترتيب ألفاظه.

---

(1) د.محمود نجيب حسني: جرائم الاعتداء على الأموال في قانون العقوبات اللبناني، الطبعة الثالثة، عام 1998،المرجع السابق، ص349. د.علي القهوجي، المرجع السابق، ص791.

وعليه فمن كان معروفاً باسم شهرة مختلف عن اسمه المثبت في بطاقة الهوية، فإنه لا يرتكب احتيالاً إذا تقدم به إلى المجني عليه، لأنه يعتبر اسماً حقيقاً له ولو كان المجني عليه يظن أنه لا يحمل اسماً آخر[1].

## 2- الصفة الكاذبة:

يقصد بالصفة تلك الخاصية التي تحدد معالم الشخصية. ومعالم الشخصية كثيرة ومتنوعة وغير قابلة للحصر، ويشترط في الصفة أن توفر قدراً من الثقة المالية بالشخصية التي ترتبط بها. كما يشترط فيها أن تكون من الصفات التي جرى عرف المعاملات على التسليم بالادعاء بها دون المطالبة بتقديم دليل يثبت صحة هذا الادعاء[2].

ومن الصفات التي اعتاد الناس عدم طلب ما يثبت صحتها والتي يقوم الاحتيال بالكذب بشأنها، الصفات المتعلقة بالمركز العائلي، كادعاء المحتال أنه على علاقة قرابة بشخص هو محل ثقة لدى المجني عليه، وأنه سيكفل وفاء التزام المحتال. ومن هذه الصفات أيضاً ما يتعلق بالمهنة، كما لو ادعى المحتال مهنة ليست له كالطبيب أو المهندس أو المحامي أو الصحفي..، وتوصل بذلك إلى الاستيلاء على مال المجني عليه، فإنه يرتكب جرم الاحتيال. ومن هذه الصفات أيضاً ما يتعلق بالمركز الاجتماعي مثل حمل رتبة أو وسام أو عضوية جمعية أو لجنة.. الخ.

ويخرج من مجال جريمة الاحتيال الصفات التي اعتاد الناس على مطالبة بعضهم البعض بتقديم الدليل على صحتها، ومن أمثلة هذه الصفات صفة

---

(1) د. محمود نجيب حسني: جرائم الاعتداء على الأموال في قانون العقوبات اللبناني، الطبعة الثالثة، عام 1998،المرجع السابق، ص352. د.علي القهوجي: المرجع السابق، ص793.

(2) د.محمود نجيب حسني: جرائم الاعتداء على الأموال في قانون العقوبات اللبناني، الطبعة الثالثة، عام 1998،المرجع السابق، ص353.

الدائن، والمالك، وبلوغ سن الرشد[1]. فمن يدعي كذباً أنه دائن ويطلب الوفاء بما يدعي من دين، لا يرتكب جرم الاحتيال إذا اعتقد الغير صحة ادعائه وسلّمه المال المطلوب، لأنه كان يجب على هذا الغير أن يطالبه بتقديم الدليل الذي يثبت حمله لصفة الدائن.

وتطبيقاً لذلك، فمن يقوم باستعمال بطاقة ائتمان مسروقة أو مفقودة لسحب النقود أو الوفاء لدى التجار، فإنه يرتكب جرم الاحتيال بوسيلة انتحال صفة كاذبة وهي صفة الحامل الشرعي، كما إنه يتخذ اسماً كاذباً وهو اسم الحامل الشرعي، وهذا ما اتفق الفقه على تكييفه[2].

ففي عام 2005 ، تمّ الحكم في إنكلترا على أربعة أشخاص بالسجن لمدة أربع سنوات، لارتكابهم الاحتيال عن طريق سحب النقود من الصراف الآلي بواسطة البطاقات المزورة، حيث قدرت المبالغ التي تم الاستيلاء عليها بـ200.000 جنيه إسترليني[3].

وبعد أن أنهينا شرح الوسائل الاحتيالية، فإن **الباحث** يرى بأن وسيلة استعمال الدسائس، ذات مفهوم واسع يشمل مختلف الوسائل التقنية التي سبقت الإشارة إليها، والتي يمكن أن ترتكب بها جريمة الاحتيال عبر الإنترنت. ومع هذا **فالباحث يقترح** على المشرع عند تجريمه للاحتيال عبر الإنترنت أن يبتعد عن تحديد الوسائل الاحتيالية، تماشياً مع سرعة تطور الوسائل التقنية التي يصعب تتبعها تشريعياً والتي يمكن أن تستخدم في ارتكاب هذه الجريمة ، وحرصاً على ألا يفلت الجناة من سوط العقاب.

---

(1) د.محمود نجيب حسني: جرائم الاعتداء على الأموال في قانون العقوبات اللبناني، الطبعة الثالثة، عام 1998،المرجع السابق، ص358. د.علي القهوجي: المرجع السابق، ص796.

(2) د. نائلة قورة: المرجع السابق، ص541.

(3) Robin Bryant, op-cit, p.142.

## المطلب الثالث
## النتيجة الجرمية (تسليم المـال)

حدّد المشرع النتيجـة الجرميـة للاحتيـال فـي المـادة 641 عقوبـات بأنهـا: (تسليم المجنـي عليـه لمـال منقول أو غيـر منقول أو أسناداً تتضـمن تعهداً أو إبراء فاستولى عليها احتيالاً).

وعلـى ذلك فإن النتيجـة الجرميـة هـي التسليم الصـادر عن المجنـي عليـه للمحتال تحت تأثير الغلط الذي أوقعه به. ولا يجوز النظر إلى التسليم هنا على أنه واقعة مادية تتمثل في مناولة مادية، ترد على شيء ينقله المجنـي عليه من حيازته إلى حيازة الجاني، بل يجب النظر إلى التسليم على أنه عمل قانوني، جوهره قيام إرادة المجني عليه المعيبة بتمكين المحتال من السيطرة على المال، سواء تحققت هذه السيطرة على الفور أم بعد وقت قصير. وهذه الإرادة تلتقي بها إرادة المحتال، فإذا تحقق هذا الالتقاء الإرادي توفرت عناصر التسليم، حتى ولو لم تكن ثمة مناولة مادية فورية، بل حتى ولو كانت هذه المناولة غير محققة في المستقبل. فالتسليم هو تصرف مالي قد تكون المناولة المادية إحدى صوره المتنوعة[1].

وصـور التسليم متعددة، فقد تتمثل بالمناولـة يداً بيد، أو بتسليم مفتـاح المخزن الذي توجد فيه البضائع، أو بوضع المال تحت تصرف الجاني بحيث يتمكن من الاستيلاء عليه بغير عائق.

ومن تطبيقات التسليم غير المصحوب بمناولة مادية، حمل المجنـي عليه بالخداع على تسجيل اسم المحتال في دفتر لديه على أنه من الدائنين، فالتسجيل في حد ذاته تصرف مالي تتحقق به جميع عناصر التسليم، ولا

---

(1) د. محمود نجيب حسني: جرائم الاعتداء على الأموال في قانون العقوبات اللبناني، الطبعة الثالثة، عام 1998،المرجع السابق، ص367.

يختلف الأمر إذا استطاع المحتال خداع المجني عليه وحمله على حذف الدين الثابت في ذمته من دفاتره، فشأنه هنا شأن من حصل بالخداع على سند يبرئ ذمته[1].

وقد يتم التسليم إلى الجاني أو إلى شخص آخر يحدده الجاني للمجني عليه مثل زوجته أو ابنه أو أي شخص آخر. وقد يقع التسليم من المجني عليه نفسه أو من غيره، فقد يقوم المجني عليه بتسليم المال إلى الجاني بنفسه، أو عن طريق نائبه أو وكيله بناءً على أمره[2]. ويرى جانب من الفقه – **والباحث يؤيده**– أنه يمكن اعتبار جهاز التوزيع الآلي للنقود، بمثابة الطرف الثالث الذي يعمل لحساب المجني عليه، لان خداع الجهاز هو خداع لصاحبه[3].

ويستوي أن تكون حيازة المجني عليه للمال موضوع الاحتيال حيازة مشروعة أو غير مشروعة، كما لو كان مالاً مسروقاً أو متحصلاً عليه من جريمة. ويستوي أيضاً في تسليم المال، أن يكون الغرض الذي يسعى إليه المجني عليه مشروعاً أو غير مشروع، فقد يسلم ماله للمحتال من أجل تقديمه كرشوة لموظف ما، أو لتهريب مواد يُمنع استيرادها، أو لإقامة علاقة جنسية غير مشروعة مع إحدى الفتيات[4].

ومتى حصل التسليم الذي اتجهت إليه الإرادة المعيبة، قامت جريمة الاحتيال، ولو لم يصب المجني عليه ضرر مالي منه، فالضرر في هذه الجريمة يتحقق بمجرد العدوان على الملكية والمساس بحرية الإرادة، حتى لو لم

---

(1) د. محمود نجيب حسني: جرائم الاعتداء على الأموال في قانون العقوبات اللبناني، الطبعة الثالثة، عام 1998،المرجع السابق، ص368.

(2) د. علي القهوجي: المرجع السابق، ص800.

(3) أحمد حسام طه تمام: المرجع السابق، ص544. د.نائلة قورة: المرجع السابق، ص 465.

(4) د.محمود نجيب حسني: جرائم الاعتداء على الأموال في قانون العقوبات اللبناني، الطبعة الثالثة، عام 1998،المرجع السابق، ص 365.

تنقص ثروة المجني عليه في مجموعها. فمن يخدع شخصاً ليحمله على تسليمه شيئاً، فإنه يرتكب جرم الاحتيال ولو ترك للمجني عليه ثمنه أو أكثر منه[1].

وفي مجال الاحتيال عبر الإنترنت، فالسؤال الذي يطرح نفسه هنا: **هل يتحقق التسليم إذا كان المحل هو النقود الكتابية[2]؟ بمعنى لو تلاعب الجاني بالبرامج أو المعلومات المصرفية بهدف تحويل الأموال من حسابات أصحابها إلى حسابه، فهل يتحقق التسليم هنا؟**

تختلف الإجابة عن هذا السؤال بحسب موقف المشرع المقارن من مسألة النقود الكتابية، ويمكن هنا التمييز بين اتجاهين[3]:

**الاتجاه الأول**: تمثله التشريعات التي تعدّ النقود الكتابية عبارة عن ديون، ومن ثم لا تصلح لأن تكون محلاً لجريمتي السرقة والاحتيال، لأنها ليست مالاً مادياً. ومن هذه الدول ألمانيا واليابان.

**الاتجاه الثاني**: وتمثله التشريعات التي تعدّ النقود الكتابية من قبيل الأموال التي تصلح لأن تكون محلاً لجريمتي السرقة والاحتيال. ومن هذه الدول كندا وهولندا وسويسرا وبريطانيا والولايات المتحدة الأمريكية.

ففي الولايات المتحدة الأمريكية ، سبقت الإشارة إلى أن القوانين الفيدرالية قد عرفت المال بأنه: "كل شيء يمثل قيمة، بحيث يشمل جميع الأموال الكتابية أو المصرفية".

---

(1) د.محمود نجيب حسني: جرائم الاعتداء على الأموال في قانون العقوبات اللبناني، الطبعة الثالثة، عام 1998،المرجع السابق، ص 363 و 364.

(2) يُقصد بالنقود الكتابية في هذا المجال، القيد الكتابي الذي يتم بطريقة الكترونية، بهدف تحويل الأموال بطريقة غير مشروعة إلى حساب المحتال.

(3) المحامي محمد أمين الشوابكة: المرجع السابق، ص192. د. سليمان فضل: المرجع السابق، ص89،: د.نائلة قورة: المرجع السابق، ص467. عفيفي كامل عفيفي: المرجع السابق، ص174.

ويلحق بهذه الدول فرنسا، حيث ابتدع القضاء الفرنسي نظرية "**التسليم المعادل**"، التي أقرتها محكمة النقض الفرنسية[1]، إذ اعتبرت بأن الدفع الذي يتم عن طريق القيد الكتابي يعادل تسليم النقود. وبناء على هذه النظرية فإن المادة 313 من قانون العقوبات الفرنسي لعام 1992 والمتعلقة بالاحتيال تنطبق على جميع أفعال التلاعب في عملية البرمجة أو في البيانات المدخلة إلى الحاسوب والمنقولة عبر الإنترنت. فجميع عمليات التحويل غير المشروع والتي تتم عن طريق الإنترنت، أي بالدخول إلى أنظمة المصارف والتلاعب بها، والتي يترتب عليها الاستيلاء على كل أو بعض الأرصدة العائدة للغير، يعد التسليم بها محققاً ومعادلاً لتسليم النقود. ويدعم اتجاه القضاء الفرنسي جانب من الفقه المصري الذي يرى أن التسليم في جريمة الاحتيال يتحقق بوضع الشيء تحت تصرف الجاني، بحيث يتمكن من حيازته بغير عائق[2].

**ويؤيد الباحث** ما ذهب إليه القضاء الفرنسي و الفقه المصري فيما يخص نظرية التسليم المعادل، لأن الاستيلاء على النقود الكتابية أو الإلكترونية يعادل الاستيلاء على الأموال العادية. فالتلاعب بالبيانات وإجراء تحويلات إلكترونية من حساب المجني عليه إلى حساب الجاني، يؤدي من حيث النتيجة إلى تحويل النقود العادية، مع الأخذ في الحسبان بأن التطور التقني قد سمح بأن تتم هذه التحويلات بشكل فوري، بعد إجراء عملية القيد الإلكتروني مباشرة.

---

(1) Cass. Crime. 25 Janvier 1967, Bull. crim. N 39 .
مشار إليه عند: د.نائلة قورة: المرجع السابق، ص 467.

(2) محمد عبيد الكعبي: المرجع السابق، ص183.

# المطلب الرابع
# الصلة السببية

لا يكفي لقيام الركن المادي للاحتيال أن يصدر عن الجاني نشاطٌ متمثلٌ بالخداع، ونتيجةٌ متمثلة بتسليم المجني عليه ماله للمحتال تحت تأثير الغلط، بل يجب أن تتوافر الصلة السببية بين الخداع والتسليم، بحيث يمكن القول أنه لولا الخداع لما تمّ التسليم.

فالصلة السببية بين الخداع والتسليم تستلزم تحقق الشروط الثلاثة التالية:

1) الصلة السببية بين الخداع والغلط.
2) الصلة السببية بين الغلط والتسليم.
3) ضرورة أن يسبق فعل الخداع تسليم المال.

فإذا توافرت هذه الشروط الثلاثة تحققت علاقة السببية، أما إذا انتفى أحدها فتنتفي هذه العلاقة. إلاّ أن انتفاء رابطة السببية وإن كان يحول دون قيام جريمة الاحتيال التامة، لكنه لا يمنع من تحقق الشروع في الاحتيال متى توفرت شرائطه.

## أولاً– الصلة السببية بين الخداع والغلط: [1]

يجب أن يكون من شأن الخداع إيقاع المجني عليه في الغلط، وأن يقع المجني عليه فعلاً في الغلط ذاته الذي أراده الجاني. أما إذا اكتشف المجني عليه خداع الجاني ولم يقع في الغلط، فإن الصلة السببية تنتفي، كما لو ادعى المحتال بأكاذيبه واستعان بأشخاص آخرين لتأييد ادعائه، إلا أن المجني عليه

---

(1) د.محمود نجيب حسني: جرائم الاعتداء على الأموال في قانون العقوبات اللبناني، الطبعة الثالثة، عام 1998،المرجع السابق، ص373. د.علي القهوجي: المرجع السابق، ص806.

اكتشف هذا الكذب ولم يقع في الغلط، ولكنه بالرغم من ذلك قام بتسليمه المال تحت تأثير الخوف من هؤلاء الأشخاص مثلاً.

ويقصد بوقوع المجني عليه في الغلط، اقتناعه بأكاذيب المحتال، أي أن تتكون لديه عقيدة مخالفة للحقيقة، ويفترض ذلك جهله بالحقيقة، سواء كان الجهل كلياً أو جزئياً. كما يفترض الغلط أيضاً جهل المجني عليه بطبيعة وآثار التصرف الذي يقدم عليه، أي أن يعتقد أنه يفعل ما فيه مصلحته أو مصلحة غيره، أو على الأقل ما ليس ضاراً به أو بغيره، في حين أن تصرفه على العكس من ذلك.

## ثانياً- الصلة السببية بين الغلط والتسليم:

يقصد بهذه الصلة أن يكون الغلط هو الدافع إلى التسليم، ولا يشترط أن يكون الغلط هو الدافع الوحيد إلى التسليم، بل يكفي أن يكون أحد الدوافع التي حملت المجني عليه على تسليم ماله. وهذه القاعدة مستمدة من نظرية تعادل الأسباب التي أخذ بها المشرع السوري في الفقرة الأولى من المادة /203/ من قانون العقوبات[1]. ويترتب على هذه القاعدة أيضاً، أن تقصير المجني عليه وإهماله في التحقق من أقوال المحتال لا يترتب عليه نفي الصلة السببية المطلوبة في الاحتيال، فسذاجة المجني عليه وقابليته للوقوع في الغلط بسهولة لا ينفيان هذه الصلة[2].

---

(1) تنص المادة /203/ من قانون العقوبات على ما يلي: (1-إن الصلة السببية بين الفعل وعدم الفعل من جهة، وبين النتيجة الجرمية من جهة ثانية، لا ينفيها اجتماع أسباب أخرى سابقة أو مقارنة أو لاحقة سواء جهلها الفاعل أو كانت مستقلة عن فعله. 2- ويختلف الأمر إذا كان السبب اللاحق مستقلاً وكافياً بذاته لإحداث النتيجة الجرمية. ولا يكون الفاعل في هذه الحالة عرضة إلاّ لعقوبة الفعل الذي ارتكبه).

(2) د.محمود نجيب حسني: جرائم الاعتداء على الأموال في قانون العقوبات اللبناني، الطبعة الثالثة، عام 1998،المرجع السابق، ص 375.

أما إذا ثبت أن الغلط لم يكن له تأثير على المجني عليه حين سلم ماله، بل كانت هناك دوافع أخرى حملته على هذا التسليم، فإن الصلة السببية تنتفي، فإذا تقدم شخص باسم مستعار إلى أحد الأثرياء، وادعى بأنه قريب لأحد الزعماء السياسيين، وطلب المال على سبيل التبرع، فأعطاه الثري ليس تحت تأثير الغلط بل رغبة منه في الإحسان، فإن الصلة السببية تنتفي[1].

كما تنتفي الصلة السببية بين الخداع والتسليم، إذا تمّ التسليم لا بسبب الغلط الذي أراده الجاني، وإنما بسبب غلط آخر وقع به المجني عليه دون أن يكون للمحتال يد فيه. ومثال ذلك، أن يتخذ الشخص اسماً مستعاراً، ويدعي أنه يقوم بتأسيس شركة، ويطلب من المجني عليه مالاً للمساهمة فيها، فيسلمه المال، ويثبت بعد ذلك أن الاسم المستعار لم يكن هو الدافع إلى التسليم، لأنه لم يكن محل اعتبار في نظر المجني عليه، وإنما ما دفعه إلى ذلك تلك الأقوال الكاذبة المجردة التي أبرزت أهمية هذه الشركة، والتي لا تكفي بذاتها لتكوين فعل الخداع[2].

وبناء على ما تقدم، فإذا قام شخص بإرسال رسالة عبر البريد الإلكتروني إلى شخص آخر، وادعى فيها بأنه الوارث الوحيد لرجل أعمال معروف، وطلب من المرسل إليه بعض المال لتغطية نفقات تصفية التركة، على أن يعطيه جزءاً من هذه التركة، فقام المجني عليه بإرسال المبلغ المطلوب لا لأنه وقع في الغلط، بل أرسله له على سبيل الإحسان والتبرع. ففي هذا الفرض لا تقوم جريمة الاحتيال عبر الإنترنت لانتفاء علاقة السببية بين الغلط والتسليم.

---

(1) قرار محكمة منوف الجزئية، تاريخ 14 تشرين الأول 1914، مشار إليه عند: د.محمود نجيب حسني: جرائم الاعتداء على الأموال في قانون العقوبات اللبناني، الطبعة الثالثة، عام 1998,المرجع السابق، ص 376.

(2) د.محمود نجيب حسني: جرائم الاعتداء على الأموال في قانون العقوبات اللبناني، الطبعة الثالثة، عام 1998،المرجع السابق، ص 376. د.علي القهوجي: المرجع السابق، ص 810.

## ثالثاً– ضرورة أن يسبق فعل الخداع تسليم المال:

وهذا الشرط يفرضه المنطق، لأنه لا يتصور تحقق علاقة السببية بين الخداع وتسليم المال، إذا كان الثاني يسبق الأول في الزمن. وبناء على ذلك يجب أن تتحقق علاقة السببية بين الخداع والغلط أولاً، ثم بين الغلط والتسليم ثانياً، أي يجب أن تكون هذه الخطوات مرتبة من حيث الزمن. فإذا سلّم المجني عليه ماله أولاً، ثم صدر عن الجاني بعد ذلك فعل الخداع لكي يفرّ بالمال أو يتخلص من الالتزام الذي نشأ في ذمته نتيجة لتسلمه هذا المال، ففي هذه الحالة تنتفي رابطة السببية، وتنتفي تبعاً لذلك جريمة الاحتيال[1].

## الشروع في الاحتيال:

عاقب المشرع السوري على الشروع بارتكاب جرم الاحتيال في الفقرة الثانية من المادة /641/ من قانون العقوبات حيث نصت على ما يلي: (2– يطبق العقاب نفسه في محاولة ارتكاب هذا الجرم).

والشروع –وفقاً للقواعد العامة– هو كل محاولة لارتكاب جناية أو جنحة (معاقب على الشروع فيها) بدأت بأفعال ترمي مباشرة إلى اقترافها، تعتبر كالجريمة نفسها إذا لم يحل دون إتمامها سوى ظروف خارجة عن إرادة الفاعل[2].

فالشروع هو جريمة بدأت فيها الأفعال التنفيذية إلا أن النتيجة الجرمية لم تتحقق لظروف خارجة عن إرادة الفاعل. والمعيار الذي أخذ به المشرع السوري للتمييز بين الأفعال التحضيرية والأفعال التنفيذية، هو المعيار الشخصي الذي ينظر إلى مقدار الخطورة التي وصل إليها الجاني من خلال أفعاله، وهو

---

(1) د.محمود نجيب حسني: جرائم الاعتداء على الأموال في قانون العقوبات اللبناني، الطبعة الثالثة، عام 1998, المرجع السابق، ص 377. د.علي القهوجي: المرجع السابق، ص811.

(2) راجع المواد 199– 200– 201– 202 عقوبات.

المعيار الذي يحقق للمجتمع حماية أكبر. أما المعيار المادي فهو ضيق؛ لأنه لا يعاقب الفاعل على أفعاله إلا إذا كانت داخلة ضمن الركن المادي للجريمة أو لظرف مشدد لها[1].

والأصل أنه إذا وقف نشاط الفاعل عند العمل التحضيري فلا عقاب عليه، إلا إذا كانت الأفعال التي قام بها تشكل جرائم بحد ذاتها.

**والشروع نوعان: شروع تام** ، وفيه يقوم الجاني بجميع الأفعال التنفيذية إلا أن النتيجة الجرمية لا تتحقق لظروف خارجة عن إرادته. ويطلق على هذا الشروع أيضاً اسم الجريمة الخائبة. أما النوع الثاني فهو **الشروع الناقص**، وفيه لا يكتمل النشاط الجرمي، وتتوقف الجريمة في مراحلها الأولى لظروف خارجة عن إرادة الفاعل. ويطلق على هذا الشروع اسم الجريمة الموقوفة.

والشروع بنوعيه يمكن تصوره في جريمة الاحتيال عبر الإنترنت، فمن يقوم باختراق نظام معلوماتي لأحد المصارف عن طريق الإنترنت، ويقوم بإدخال البيانات اللازمة لإجراء التحويلات المالية غير المشروعة، ثم لا تتحقق النتيجة الجرمية المتمثلة بتحويل النقود، نتيجة وجود خطأ في إدخال بعض البيانات، فإن نشاط الفاعل يشكل هنا شروعاً تاماً في الاحتيال.

وقد يقف نشاط الفاعل عند حد الشروع الناقص، كما لو تم إلقاء القبض على أحد الهكرة أثناء وجوده في أحد مقاهي الإنترنت، وهو يقوم باختراق لإحدى شبكات المصارف، بغية إجراء تحويلات غير مشروعة.

---

(1) د. عبود السراج: المرجع السابق, ص315.

# المبحث الثاني

# الركن المعنوي

الاحتيال جريمة مقصودة، فلا يعرف التشريع جريمة احتيال غير مقصودة، مهما كان خطأ الجاني جسيماً. إلا أن هناك اختلافاً بين الفقهاء حول ضرورة اشتراط القصد الجرمي الخاص المتمثل "بنية التملك" في جريمة الاحتيال، فبعض الفقهاء يكتفي بتوفر القصد الجرمي العام، والبعض الآخر يشترط توافر القصد الجرمي الخاص إلى جانب القصد العام.

أما الدافع فليس عنصراً من عناصر التجريم في جرم الاحتيال، فمتى تحقق الركن المادي والركن المعنوي، فلا عبرة بعد ذلك للدافع أو الباعث على قيام هذه الجريمة. إلا أن الدافع يبقى مؤثراً في مقدار العقوبة التي يفرضها القاضي. لهذا كان من الضروري التعرف على أصناف مجرمي الإنترنت ودوافعهم، لما في ذلك من فائدة عملية عند فرض العقاب من قبل القاضي الجزائي. لذلك سوف نقسم هذا المبحث إلى المطلبين التاليين:

المطلب الأول: القصد الجرمي المطلوب توافره في الاحتيال.

المطلب الثاني: تأثير الدافع على العقوبة .

## المطلب الأول
## القصد الجرمي المطلوب توفراه في الاحتيال

جريمة الاحتيال جريمة مقصودة، ومن ثم فالركن المعنوي يتخذ فيها صورة القصد الجرمي. والقصد الجرمي المطلوب للاحتيال هو القصد العام فقط[1].

ويذهب بعض الفقهاء إلى أن القصد الجرمي المطلوب توافره في جريمة الاحتيال، هو القصد الجرمي العام والقصد الجرمي الخاص، ووفقاً لهذا الرأي فإن مضمون القصد الخاص هو "نية التملك"[2].

و**يرى الباحث** أن القصد الخاص لا يلزم توافره إلى جانب القصد العام لتحقق الركن المعنوي في جريمة الاحتيال، لأن نيّة التملك تدخل في عناصر القصد العام، الذي تتجه الإرادة فيه إلى النشاط الجرمي والنتيجة. فالنتيجة الجرمية في جريمة الاحتيال تتمثّل في تسليم المال، ويُقصد بهذا التسليم تمكين المحتال من السيطرة على المال محل التسليم سيطرةً تسمح له بالاستيلاء عليه، أي أن يحوزه حيازة كاملة بعنصريها المادي والمعنوي، وهذه الحيازة هي التي تسمح للجاني أن يمارس على هذا المال مظاهر السيطرة التي ينطوي عليها حق الملكية. وبالتالي فلا حاجة لجعل نيّة التملك مستقلة ضمن القصد الخاص.

---

(1) من هذا الرأي د.علي القهوجي: المرجع السابق، ص814. د. جاك الحكيم ود.رياض الخاني: المرجع السابق، ص380. د. علاء عبد الباسط خلاف: المرجع السابق، ص107.

(2) ومن هذا الرأي د. محمود نجيب حسني: جرائم الاعتداء على الأموال في قانون العقوبات اللبناني، الطبعة الثالثة، عام 1998,المرجع السابق، ص392. د.أحمد حسام طه تمام: المرجع السابق، ص549. د. نائلة قورة: المرجع السابق، ص489.

والقصد العام يتكون من عنصرين هما: العلم والإرادة، أي العلم بجميع عناصر الركن المادي ، وإرادة تتجه إلى السلوك والنتيجة الجرمية.

فيجب أن يعلم الجاني بأنه يرتكب فعل الخداع، وأن هذا الفعل يؤدي إلى إيقاع المجني عليه في الغلط حيث يحمله على تسليم ماله، ويقتضي ذلك ضرورة علم الجاني بأن ما يصدر عنه هو أكاذيب، لأن الكذب هو جوهر الخداع. فإذا كان الخداع مثلاً عبارة عن انتحال صفة كاذبة، يجب أن يكون الجاني عالماً بها. أما إذا كان يعتقد أن من حقه اتخاذها فإن القصد لا يتوفر لديه. فمن كان مديراً لشركة أو وكيلاً عن شخص، لا يتوافر لديه القصد إذا كان قد فصل من عمله أو عزل من وكالته وقت إدلائه بأقواله، وكان لا يعلم بذلك[1].

ويجب أن يعلم الجاني أن من شأن ادعاءاته إيقاع المجني عليه في الغلط الذي يدفعه إلى تسليم ماله. أما إذا اعتاد شخص أن يدعي بأوصاف تخلع على صاحبها الاحترام في نظر المجتمع، وكان يريد من ذلك مجرد التفاخر والاستمتاع باحترام الناس، ووقع المجني عليه في غلط وسلمه شيئاً من ماله ، فلا يتوافر القصد الجرمي لدى هذا الشخص الذي لم يكن يعلم بوقوع المجني عليه بالغلط[2].

كما يجب أن يعلم الجاني بأن المال الذي تسلمه مملوكاً للغير، فإذا اعتقد أنه ماله فلا يتوفر القصد الجرمي.

---

(1) د. محمود نجيب حسني: جرائم الاعتداء على الأموال في قانون العقوبات اللبناني، الطبعة الثالثة، عام 1998,المرجع السابق، ص393.

(2) د. علي القهوجي: المرجع السابق، ص816.

ويتطلب القصد العام كذلك، ثبوت اتجاه إرادة الجاني إلى النشاط الجرمي وهو الخداع. وثبوت اتجاه إرادته أيضاً إلى تحقيق النتيجة الجرمية وهي استلام المال من المجني عليه، ثم الاستيلاء عليه والظهور بمظهر المالك "نية التملك"، ويكشف عن هذه النية عزم الجاني على عدم رد المال إلى المجني عليه وحرمانه منه، فإذا لم تنصرف نية الجاني إلى تملك المال فلا تقوم جريمة الاحتيال لانتفاء القصد الجرمي، فمن كان يريد تسلم الشيء لمجرد فحصه ثم رده ، فلا يتوافر لديه نية التملك، وبالتالي ينتفي لديه القصد الجرمي.

ومتى توفر عنصرا القصد العام ، فلا تأثير للبواعث والدوافع بعد ذلك، سواءً كان الدافع أو الباعث شريفاً أو شائناً، فيستوي أن يكون الدافع الطمع أو الانتقام من المجني عليه، أو تخصيص المال لمشروع خيري أو حتى إنفاقه في مصلحة المجني عليه كعلاجه أو تعليمه[1].

وتطبيقاً لذلك، فحتى يتوافر القصد الجرمي في جريمة الاحتيال عبر الإنترنت عن طريق التحويلات المالية غير المشروعة، يجب أن يعلم الجاني بأنه يخترق النظام المعلوماتي لأحد المصارف، وأن ما يقوم بإدخاله من بيانات من أجل إجراء تحويلات مالية غير مشروعة، سوف يؤدي إلى وقوع هذا النظام في الغلط، بحيث يجري التحويل المالي لمصلحة الجاني. كما يجب أن يعلم الجاني بأن المال المطلوب تحويله مملوك للغير ، وأن تتجه إرادة الجاني إلى تملك هذا المال.

وبناء على ذلك ينتفي القصد الجرمي لدى المخبر الذي يدخل إلى إحدى حلقات المحادثة عبر الإنترنت، ويتفق مع أحد الهكرة على إنشاء موقع

---

(1) د. محمود نجيب حسني: جرائم الاعتداء على الأموال في قانون العقوبات اللبناني، الطبعة الثالثة، عام 1998, المرجع السابق، ص396. د.علي القهوجي: المرجع السابق، ص817.

للاحتيال على الناس، ويستدرجه إلى أن يتم إنشاء هذا الموقع ثمُ يمكن السلطات من القبض عليه. ويُشترط لعدم معاقبة المخبر أن يقتصر دوره على كشف الجريمة، لا أن يخلقها من العدم.

وفي جرائم الإنترنت عموماً يمكن إثبات القصد الجرمي من خلال القرائن، فتفتيش حاسوب المشتبه به مثلاً، ومعرفة المواقع التي قام بتصفحها والأشخاص الذين اتصل بهم، قد يفيد في إثبات قصد الاحتيال عنده. ومن الوقائع الحقيقية التي تمّ فيها اكتشاف نية المدعى عليه في إحدى جرائم القتل، بأنه لدى تفتيش حاسوب المدعى عليه تبين بأنه كان يبحث عن مصطلحات مثل "قتل، خنق، وفيات، حادث" قبل قيامه بقتل زوجته، فبفضل عملية البحث هذه تم إثبات نية العمد لديه، ورفع مستوى الجريمة إلى القتل من الدرجة الأولى[1].

(1) Eoghan Casey, op-cit, chapter 1, p-4.

## المطلب الثاني
## تأثير الدافع على العقوبة

أشار المشرع السوري إلى الدافع في المادة 191 من قانون العقوبات والتي نصت على ما يلي:

(1- الدافع هو العلة التي تحمل الفاعل على الفعل أو الغاية القصوى التي يتوخاها.

2- ولا يكون الدافع عنصراً من عناصر التجريم إلا في الأحوال التي عينها القانون).

وبناء على ذلك فإن الدافع ليس عنصراً من عناصر التجريم في جريمة الاحتيال، ومن ثم فهو لا يؤثر على قيام المسؤولية الجزائية ولا على توافر الركن المعنوي. إلا أن دراسة دوافع مجرمي الإنترنت ومعرفة أصنافهم تتجلى فائدتها في تحديد مقدار العقوبة المفروضة، وخاصة في مجال تخفيف العقوبة، فالقاضي الجزائي له سلطة تقديرية بمنح الأسباب المخففة، واختيار العقوبة المناسبة لشخصية المجرم ضمن ما هو مقرر من وضع العقوبة بين حدين أدنى وأعلى. فالوقوف على شخصية المجرم ومعرفة دوافعه وظروفه وبيئته.. الخ، أمر في غاية الأهمية بالنسبة للقاضي، لفرض العقوبة والتدبير المناسبين على المجرم. وانطلاقاً من هذا المبدأ كان لابد لنا من التعرف على أصناف مجرمي الإنترنت وتسليط الضوء على دوافعهم الإجرامية.

وفي مجال تصنيف مجرمي الإنترنت يمكن التمييز بين خمسة أصناف، هم:

## أولاً– الهاكر الآمن Hacker:

يعود الفضل في وضع مصطلح الهكرة Hacking إلى كاتب الخيال العلمي الأمريكي "وليم جيبسون" في مؤلفه The Neu-Romancer الذي أصدره عام 1984، حيث أطلق على مجرم الإنترنت تسمية هاكر Hacker ، الذي يشير إلى جميع أشكال الاختراق عبر الإنترنت. وقد لقي هذا المؤلف نجاحاً كبيراً، وخاصة لاستخدامه هذا المصطلح[1].

و يقصد بالهاكر، من يستخدم الحاسوب وشبكة الإنترنت لاختراق نظم الأمن والشبكات، بغرض الدخول غير المصرح به. ورغم قدرة الهاكر الفائقة على الاختراق، إلا أنه غير مؤذٍ، فهو لا يقوم بالاختراق بغرض التخريب أو الإيذاء، وإنما نتيجة حبه للحرية وشعوره بأن الإنترنت أو العالم الافتراضي يؤمن له هذه الحرية، إذ إنه لا يقيم أهمية لحواجز الشفرات وكلمات المرور، بل يخترق أعتى الأماكن سرية وحصانة بغرض الاطلاع على التقنية، دون أن يتلف أو يخرب أي شيء. لذلك فإن ما يحكم هذا النوع من الهكرة هو الإيمان بالحرية المطلقة المتوفرة في العالم الافتراضي، إضافة إلى الفضول ودوافع التحدي وإثبات المقدرة. ومثال ذلك ما حدث في شهر تشرين الأول عام 2000 عندما تمّ اختراق نظام شركة مايكروسوفت الأمني من قبل مجموعة مجهولة لم يتم التوصل إليها. وقد حُفظت القضية لكون المجهولين لم يقوموا بعمليات تخريب، وإنما فقط قاموا بجولة هناك ثم تركوا المكان ولاذوا بالفرار[2].

والواقع بأن هناك من يدافع عن مجموعات الهكرة التي لا تمارس أية أفعال تستهدف إلحاق الضرر بالغير، بل تنحصر أهداف الاختراق لديهم بالكشف عن الثغرات الأمنية في النظام محل الاعتداء. وثمة من يؤكد من بين

---

(1) د. عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت، المرجع السابق ، ص235.

(2) د. عمر يونس: الجرائم الناشئة عن استخدام الإنترنت، المرجع السابق ، ص240.

الهكرة أن لديهم ضوابط وأخلاقيات خاصة بهم، بل إن العديد من مواقع الإنترنت التي تهتم بمسائلهم، والتي أنشأها بعضهم، تعرض لأفكار توضح حقيقتهم، وهم يحاولون سلخ أي صفة غير شرعية أو جرمية عن الأنشطة التي يقومون بها[1].

## ثانياً- الهاكر الخبيث أو الكراكر Cracker:

عُرف هذا المصطلح في عام 1985، وهو يعبر عن المخترق ذي النوايا الإجرامية، بحيث يقوم بما هو سيئ وشرير، وما يشكل جريمة كالإتلاف أو التخريب أو الإرهاب أو الابتزاز أو العدوان على الأموال بالاحتيال والسرقة وغيرها. فاعتداء هذا النوع يعكس ميولاً إجرامياً، وينبئ عن الرغبة في إحداث التخريب.

فعلى سبيل المثال، أثناء محادثات السلام في كامب ديفيد الثانية، بين الفلسطينيين والاحتلال الإسرائيلي، تحت رعاية الولايات المتحدة الأمريكية، حدث اختراق لنظام البريد الإلكتروني التابع لوزارة الخارجية الأمريكية، فقد أرسل القراصنة فيروساً جديداً غير معروف، إلى مجموعة من الموظفين، والصحفيين ترتب عليه عدم إمكانية تحميل صور الرؤساء المجتمعين، حيث كانت الرسائل المرسلة إلى عنوان وزارة الخارجية تحمل عنوان "الطرف الضاحكة" Funny jokes، وبمجرد فتح الرسالة، فإن فيروساً غير معروف يبدأ بتدمير القرص الصلب، ثم يرسل تلقائياً نسخة من البريد الإلكتروني الحامل للفيروس إلى كل عنوان بريدي موجود في الجهاز[2].

## ثالثا- المحترفون:

---

(1) المحامي يونس عرب: جرائم الكمبيوتر والإنترنت، بحث منشور على موقعه على الإنترنت www.arablaw.com، تمّ الاطلاع عليه بتاريخ 2006/7/5, ص28.

(2) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت، المرجع السابق ، ص241.

تتميز هذه الطائفة بسعة الخبرة والإدراك الواسع للمهارات التقنية، كما تتميز بالتنظيم والتخطيط للأنشطة التي ترتكب من قبل أفرادها، ولذلك فإن هذه الطائفة تعد الأخطر من بين مجرمي التقنية، حيث تهدف اعتداءاتهم إلى تحقيق الكسب المادي لهم، أو للجهات التي كلفتهم وسخرتهم لارتكاب جرائم الحاسوب، كما تهدف اعتداءات بعضهم إلى تحقيق أغراض سياسية، أو التعبير عن موقف فكري أو فلسفي. ويمكن تقسيم هذه الطائفة إلى مجموعات متعددة، تبعاً لتخصصهم بنوع معين من الجرائم، أو تبعاً للوسيلة المتبعة من قبلهم في ارتكاب الجرائم ، مثل طائفة محترفي التجسس الصناعي، أو طائفة مجرمي الاحتيال والتزوير [1].

**رابعاً– الحاقدون:**

يغلب على هذه الطائفة عدم وجود أهداف وأغراض إجرامية لدى أفرادها، فهم لا يسعون لإثبات مقدراتهم التقنية، ولا إلى تحقيق مكاسب مادية أو سياسية. إنما يحركهم الثأر والرغبة بالانتقام كأثر لتصرف صاحب العمل معهم، أو لتصرف منشأة ما سبق لهم التعامل معها. ولذلك فهم ينقسمون إلى مستخدمين للنظام بوصفهم موظفين، أو على علاقة ما بالنظام محل الجريمة، وإلى غرباء عن النظام .

وهؤلاء تتوفر لديهم أسباب الانتقام من المنشأة المستهدفة. ولا يتصف أعضاء هذه الطائفة بالضرورة بالمعرفة التقنية الاحترافية، كما تغلب على أنشطتهم من الناحية التقنية استخدام تقنية زرع الفيروسات والبرامج الضارة[2].

**خامساً– طائفة صغار السن:**

---

(1) المحامي يونس عرب: المرجع السابق، ص28.

(2) المحامي يونس عرب: المرجع السابق، ص29.

يطلق البعض على هذه الطائفة اسم (صغار نوابغ المعلوماتية) ، ويصفهم بأنهم الشباب البالغ المفتون بالمعلوماتية والحواسيب. والحقيقة أن من بين أفراد هذه الفئة من هم دون سن الأهلية، وهم مولعون بالحوسبة والاتصالات. وقد تعددت أوصافهم في الدراسات المسحية، وشاع في نطاق الدراسات التقنية وصفهم بمصطلح المتلعثمين. ويثير مجرمو الحوسبة من هذه الفئة جدلاً واسعاً. ويمكن تقسيم الاتجاهات التقديرية لطبيعة هذه الفئة ومدى خطورة أفرادها إلى ثلاثة اتجاهات، هي[1]:

**الاتجاه الأول:** وهو اتجاه لا يرى إسباغ أية صفة جرمية على هذه الفئة، ولا يرى ضرورة تصنيفهم ضمن الطوائف الإجرامية لمجرمي الحواسيب، استناداً إلى أن هؤلاء المتلعثمين لديهم ببساطة ميل للمغامرة والتحدي ورغبة في الاكتشاف، إضافةً إلى أنهم لا يدركون ولا يقدرون مطلقاً نتائج أفعالهم التي يقومون بها.

**الاتجاه الثاني:** يناصر هذا الاتجاه هذه الفئة ويعتبرها ممن تقدم خدمة لأمن المعلومات ووسائل الحماية، ويصف أفرادها بالأخيار وأحياناً بالأبطال الشعبيين. وينسب أصحاب هذا الاتجاه إلى هذه الفئة الفضل في كشف الثغرات الأمنية في تكنولوجيا المعلومات.

**الاتجاه الثالث:** يرى أصحابه أن مرتكبي جرائم الحاسوب من هذه الطائفة، يصنفون ضمن مجرمي الحاسوب كغيرهم دون تمييز، استناداً إلى أن الحد الفاصل بين العبث بالحواسيب وبين الجريمة أمر عسير.

ومن الأمثلة الشهيرة لجرائم هذه الفئة، العصابة الشهيرة التي أطلق عليها اسم (عصابة 414)، والتي نسب إليها ارتكاب ستين فعلاً عدائياً على نظم الحاسوب في الولايات المتحدة الأمريكية[2].

---

(1) المحامي يونس عرب: المرجع السابق، ص30.

(2) المحامي يونس عرب: المرجع السابق، ص30.

وهكذا وبعد أن بيّنا أنماط مجرمي الإنترنت ودوافعهم، يمكن الاستعانة بهذا التصنيف، لاختيار العقوبة والتدبير المناسبين، عندما تعرض على القاضي جريمة احتيال عبر الإنترنت.

**عقوبة الاحتيال:**

حدّد المشرع في المادة /641/ من قانون العقوبات، عقوبة الاحتيال البسيط، وهي الحبس من ثلاثة أشهر إلى سنتين، والغرامة من مائة إلى خمسمائة ليرة سورية. كما ضاعف هذه العقوبة في المادة /642/ إذا توفر ظرفان مشددان، حيث نصت هذه المادة على ما يلي:

(تضاعف العقوبة إذا ارتكب الجرم في إحدى الحالات التالية:

ي- بحجة تأمين وظيفة أو عمل في إدارة عمومية.

ك- بفعل شخص يلتمس من العامة مالاً لإصدار أسهم أو سندات أو غيرها من الوثائق لشركة أو لمشروع ما).

وعليه يترتب على توافر أحد هذين الظرفين مضاعفة عقوبة الحبس والغرامة، بحيث تصبح العقوبة، الحبس من ستة أشهر إلى أربع سنوات، والغرامة من مائتي ليرة إلى ألف ليرة سورية.

وتطبيقاً لذلك ، فإذا أنشاء شخص موقعاً على الإنترنت، وادعى فيه كذباً القدرة على تعيين الراغبين في وظيفة عامة أو في إحدى إدارات الدولة، وطلب مبلغاً من المال لقاء هذا التعيين ، وتسلمه فعلاً من المجني عليهم، ففي هذه الحالة يتحقق الظرف المشدد المنصوص عليه بالفقرة "أ" من المادة 642 من قانون العقوبات. أما الظرف المشدد الثاني المتعلق بالأسهم المالية، فقد سبق وأن بحثنا به بشيء من التفصيل في إطار الصور الرئيسية للاحتيال عبر الإنترنت.

وأخيراً وقبل ختام هذا الفصل، وبعد أن بحثنا في الركن المادي والركن المعنوي لجريمة الاحتيال، فإننا نرى من الضروري تلخيص رأي الباحث في مسألة مدى انسجام الاحتيال عبر الإنترنت مع مفهومه التقليدي.

## رأي الباحث في مسألة مدى انسجام الاحتيال عبر الإنترنت مع مفهومه التقليدي:

بعد أن استعراضنا بعض الآراء الفقهية والمواقف القضائية التي تناولت مختلف الصعوبات التي تواجه تطبيق النصوص التقليدية لجريمة الاحتيال على الاحتيال عبر الإنترنت. فإننا نرى إمكانية تطبيق هذه النصوص التقليدية للأسباب التالية:

1- يمكن معاملة البرامج والمعلومات على أنها من **الأموال المادية**، لأن الفقه الحديث- كما رأينا- يعترف للمعلومات بصفة المال، استناداً إلى **قيمتها الاقتصادية**، فهي تصلح لأن تكون محلاً للملكية الفكرية، وهي ملك لمن ابتكرها. إضافةً إلى أن المعلومات أو البرامج تشغل حيزاً مادياً في ذاكرة الحاسوب، يمكن قياسه بمقياس معين هو البايت (BYTE) ، فهذه المعلومات بطبيعتها عبارة عن إشارات إلكترونية، تشبه إلى حد بعيد الإشارات الكهربائية التي جعلها المشرع السوري من **القوى المحرزة** التي تنزل منزلة الأشياء المنقولة في تطبيق القوانين الجزائية (المادة 621 من قانون العقوبات). وبالتالي يمكننا أن نعدّ المعلومات مفهوماً يندرج تحت مصطلح القوى المحرزة التي يحميها القانون الجزائي.

2- إن **فعل الخداع** يمكن أن يقع على نظم الحاسوب، لأن هذا الحاسوب مجرد وسيط، وهو يعبر عن إرادة المجني عليه، فهذا الأخير هو من يقوم ببرمجته وفقاً لمتطلباته، ولا يوجد ما يمنع قانوناً من أن يمارس الخداع على

نظم الحاسوب، وقد رأينا أن جانباً من الفقه الفرنسي سار في هذا الاتجاه، وسانده جانبٌ من الفقه العربي.

3- وحول الوسائل الاحتيالية، فقد بينا بأن وسيلة **استعمال الدسائس** لها مفهوم واسع، بحيث تشمل جميع الوسائل التقنية- ولا حصر لها- التي يمكن أن ترتكب بها جريمة الاحتيال عبر الإنترنت. إضافة إلى أن بقية الوسائل الاحتيالية الواردة في المادة /641/ من قانون العقوبات،لا يوجد ما يمنع قانوناً من تطبيقها على الاحتيال عبر الإنترنت، كقيام شخص بتزوير بطاقة ائتمان دولية، واستعمالها في الوفاء لدى التجار مثلاً، فإن الجاني هنا يتخذ صفة كاذبة هي صفة الحامل الشرعي، كما يتخذ اسماً مستعاراً في آن واحد.

أما الاحتيال عن طريق الأوراق المالية، فقد أشرنا بأنه يندرج تحت نص المادة /642/ من قانون العقوبات، أو القوانين الخاصة المتعلقة بالشركات، أو هيئة سوق الأوراق المالية، على النحو الذي سبق تفصيله.

4- وفي مجال التسليم، فإن النقود الكتابية أو الإلكترونية يتحقق بها التسليم المطلوب في جريمة الاحتيال، لأنها تعادل تسليم الأموال العادية؛ وهذا ما يعرف **بنظرية التسليم المعادل** التي ابتدعها القضاء الفرنسي، وأيدها جانب من الفقه المصري.

**ولا بدَّ من الإشارة هنا**، بأننا حصلنا **مؤخراً** على بعض الدراسات القانونية الحديثة التي تدعم رأينا وما توصلنا إليه من نتائج في هذا الإطار؛ فهناك دراسة توصل فيها أحد الباحثين إلى إمكانية تطبيق النص التقليدي لجريمة الاحتيال في قانون العقوبات اليمني على الاحتيال عبر الإنترنت[1]. وفي دراسة

---

(1) شمسان ناجي صالح الخيلي,الجرائم المستخدمة بطرق غير مشروعة لشبكة الإنترنت(دراسة مقارنة),دار النهضة العربية,القاهرة,2009,ص201-202.

أخرى، توصل باحثٌ آخر إلى إمكانية تطبيق النصوص التقليدية المتعلقة بجريمة القذف والسب في قانون العقوبات العُماني على جرائم القذف والسب المرتكبة عبر الإنترنت[1].

**وغني عن البيان**، أن بعض النصوص المتعلقة بالجرائم التقليدية – كالاحتيال– قد تسعف القضاء في الوقت الراهن لمواجهة هذه الجرائم في حال ارتكابها عبر الإنترنت، مع الأخذ بالحسبان بأن هذه النتيجة لا يمكن تعميمها على جميع الجرائم التقليدية التي يمكن أن ترتكب عبر هذه الشبكة؛ فلا يمكن مثلاً تطبيق النص المتعلق بخرق حرمة المنزل على الدخول غير المشروع إلى موقع إلكتروني، ولا يمكن تطبيق النص المتعلق بالسرقة على الحصول على معلومات الغير بطريقة غير مشروعة، ولا يمكن أيضاً تطبيق النص المتعلق بتزوير المحرر على تزوير المعلومات أو البيانات[2].

وبناءً على ما تقدم، وعلى الرغم من **قناعة الباحث** بإمكانية تطبيق النصوص التقليدية لجريمة الاحتيال على الاحتيال عبر الإنترنت، إلا أننا نوصي المشرع السوري بأن يسرع في التدخل لتجريم مختلف جرائم الإنترنت التقليدية منها والمستحدثة. لأن الأمر سيبقى محل خلاف وجدال بين الفقهاء، ولن يُحسم إلا بنص صريح من لدنّ المشرع حتى يحكم فيما كانوا فيه يختلفون.

# الباب الثاني

# الاحتيال عبر الإنترنت رؤية إجرائية

---

(1) د. حسين بن سعيد الغافري,المرجع السابق,102وحتى104.

(2) للباحث بحثين محكمين في مجلة الاقتصاد والقانون: **الأول** بعنوان سرقة المعلومات في ظل التشريع السوري. **والثاني** بعنوان تزوير بطاقات الائتمان, وقد وصل الباحث فيهما إلى النتيجة المشار إليها.

إن الجوانب الإجرائية لجريمة الاحتيال عبر الإنترنت هي التي تنقل نص التجريم من حالة الركود إلى حالة الحركة. فعلى فرض أن المشرع استطاع أن يحيط بالقاعدة الموضوعية لجريمة الاحتيال عبر الإنترنت ومختلف جرائم الإنترنت الأخرى، فإن نجاحه سيبقى مرهوناً بمدى إمكانية تطبيق هذه النصوص على أرض الواقع، مع مراعاة ما يحتاجه هذا التطبيق من إمكانيات تقنية، تختلف بحسب مستوى التقدم التقني والتكنولوجي في كل دولة.

والمشرع السوري حتى تاريخ إعداد هذه الدراسة، لم يصدر قانوناً لمكافحة هذا الإجرام المستحدث، سواء من الناحية الموضوعية أومن الناحية الإجرائية، وإن كان يسعى لتحقيق ذلك. وهذا ما يدفعنا إلى تطبيق قواعد الأصول التقليدية.

فعند الانتقال إلى دائرة التطبيق العملي لجريمة الاحتيال عبر الإنترنت، تظهر التحديات التي تبدأ من مسألة الاختصاص عبر الإنترنت، مروراً بأعمال الاستدلال والتحقيق، وانتهاءً بقضية الإثبات؛ حيث اعتادت سلطات الاستدلال والتحقيق أن تكون أدلة الإثبات مادية ملموسة، وهذا ما لا يتحقق دوماً في جريمة الاحتيال عبر الإنترنت.

ونتيجة لهذا القصور التشريعي، فإن من الأهداف الأساسية لهذه الدراسة تقديم التصورات العملية الممكنة، ووضع الحلول المناسبة في هذا الإطار، مع ضرورة الإشارة إلى أن هذه التصورات والرؤى ليست حكراً على جريمة الاحتيال دون غيرها من جرائم الإنترنت، فما ينطبق على الاحتيال عبر الإنترنت في مجال الجوانب الإجرائية ينطبق على مختلف جرائم الإنترنت.

لذلك كان حقاً علينا في هذه الدراسة أن نسلط الضوء على أحدث الحلول التي توصل إليها المشرع والقضاء والفقه المقارن في هذا المضمار، ريثما تأزف ساعة صدور قانون الجريمة الإلكترونية السوري الذي سبقت الإشارة إليه، وهو

مشروع قانون ضم بين دفتيه الأحكام الموضوعية والأحكام الإجرائية للجرائم الإلكترونية.

وفي ضوء الاعتبارات السابقة، يبدو ملائماً تقسيم هذا الباب إلى الفصلين التاليين:

الفصل الأول: قواعد الاختصاص والتحقيق.

الفصل الثاني: قواعد الإثبات.

# الفصل الأول

# قواعد الاختصاص والتحقيق

إن طبيعة الجغرافيا على الإنترنت، والإمكانيات التقنية العالية التي تتيحها هذه الشبكة، يمكن أن يؤدي إلى اقتراف النشاط الجرمي في دولة، وتحقق النتيجة الجرمية في دولة أخرى، كما هو الحال في جريمة الاحتيال عبر الإنترنت. الأمر الذي يثير مشكلة تنازع القوانين الجزائية من حيث المكان، أو ما يعرف بالاختصاص الجزائي الدولي.

والواقع أن المشكلات الإجرائية لا تقف عند الحدود الإقليمية غير المعروفة في هذا العالم الافتراضي، بل تمتد إلى أعمال الاستدلال والتحقيق، كتحديات استقصاء هذه الجريمة وجمع أدلتها، وكيفية مراقبة المشتبه به وآلية القبض عليه، وغير ذلك من التحديات. الأمر الذي يتطلب وجود أجهزة ضبط قضائي مختصة في ملاحقة مرتكبي هذا النوع من الإجرام المستحدث.

وعليه فإن تسلسل الأفكار على هذا النحو يقتضي منا تقسيم هذا الفصل إلى المبحثين التاليين:

المبحث الأول: الاختصاص الجزائي الدولي.

المبحث الثاني: التحقيق.

# المبحث الأول
# الاختصاص الجزائي الدولي

يقصد بالاختصاص " السلطة التي يقررها المشرع للقضاء لأن ينظر في دعاوى معينة حددها القانون" [1]، فالاختصاص في المسائل الجزائية هو ولاية القاضي في نظر دعوى جزائية معينة[2].

والاختصاص على نوعين: دولي وداخلي، ويقصد بالاختصاص الدولي، الحالات التي يكون فيها القانون الجزائي في دولة ما مختصاً بنظر دعاوى معينة، أما الاختصاص الداخلي فيقصد به، توزيع الدعاوى الجزائية وفق معايير محددة داخل الدولة، بعد أن ينعقد لها الاختصاص الدولي، فبحث الاختصاص الدولي يسبق البحث في الاختصاص الداخلي.

وإذا كانت قواعد تنازع القوانين من حيث المكان في القانون المدني، تقرر مبدأً أساسياً هو عدم التلازم بين الاختصاص القضائي والاختصاص التشريعي ، فإن الأمر في إطار القانون الجزائي على العكس تماماً ، إذ إن هناك تلازماً بين نطاق تطبيق القانون الجزائي واختصاص المحاكم الجزائية. وهذا ما هو مطبق في تشريعنا السوري؛ فكل جريمة يسري عليها قانون العقوبات السوري تختص بها حكماً المحاكم الجزائية السورية دون غيرها.

ومسألة الاختصاص القضائي عبر العالم الافتراضي أو الإنترنت تعد من المشكلات المعاصرة التي واجهت الفقه الإجرائي؛ إذ إن المشكلة الأساسية

---

(1) د.محمود نجيب حسني: شرح قانون الإجراءات الجنائية، الطبعة الثانية، دار النهضة العربية، القاهرة، عام 1988، ص359.

(2) د. حسن الجوخدار: أصول المحاكمات الجزائية, من ثلاثة أجزاء، الطبعة الخامسة، منشورات جامعة دمشق، عام 1991، الجزء الثاني، ص81.

لجـرائم الإنترنـت تكمـن فـي أنهـا لا تعـرف حـدوداً جغرافيـة، ناهيـك عـن أن الإنترنت ليست ملكاً لأحد، ولا تخضع لسيطرة دولة معينة. لذلك تتعدد القوانين الجزائية التي يمكن أن تحكم جرائم هذه الشبكة بتعدد الدول المرتبطة بها.

والاتجاه الغالب في العالم اليوم، لحل مشكلة الاختصاص القضائي عبر الإنترنـت، هـو تطبيـق المبـادئ ذاتهـا المعمـول بهـا لحـل مشـكلة الاختصـاص الجزائي الدولي في الجرائم التقليدية، وعلى رأسها **مبدأ إقليمية القانون الجزائي**، أي تطبيق القانون الجزائي على جميع الجرائم التي ترتكب في إقليم الدولة أيّاً كانت جنسية مرتكب الجريمة. كما استعان هذا الاتجاه في كثير من الأحيان بالمبـادئ الأخرى التـي تـؤدي إلـى امتـداد القـانون الجزائـي خـارج إقلـيم الدولـة وتوسيع مساحة الاختصاص. وهذه المبادئ هي:

- **مبـدأ عينيـة الـنص الجزائـي أو الصـلاحية الذاتيـة**، أي تطبيـق الـنص الجزائي على الجرائم التي تمس المصالح الأساسية للدولة، ولو ارتكبت الجريمة خارج إقليم الدولة، وأيّاً كانت جنسية مرتكبها.
- **مبدأ شخصية النص الجزائي**، أي تطبيق النص الجزائي على كل جريمة يرتكبها من يحمل جنسية الدولة، ولو ارتكبت الجريمة خارج إقليمها.
- **مبـدأ عالميـة الـنص الجزائـي أو الصـلاحية الشـاملة**، أي تطبيـق الـنص الجزائي على كل جريمة مرتكبة خارج إقليم الدولة، إذا كان الجاني أجنبياً ومقيمـاً علـى إقليمهـا، ولـم يكـن قـد طُلـب تسـليمه إلـى إحـدى الـدول لمحاكمته أو قُبل.

وبناءً على ذلك سوف نقسم هذا المبحث إلى المطلبين التاليين:

المطلـب الأول: الموقـف القـانوني والقضـائي المقـارن مـن مسـألة الاختصاص.

المطلب الثاني: مسألة الاختصاص في ظل التشريع السوري.

# المطلب الأول

# الموقف القانوني والقضائي المقارن من مسألة الاختصاص

تعددت الطرائق والهدف واحد. فعلى الرغم من لجوء معظم الدول إلى مبدأ إقليمية النص الجزائي والمبادئ الأخرى المشار إليها لحل مشكلة الاختصاص القضائي على الإنترنت، إلا أن طريقة تبنّي هذا الحل اختلفت من دولة إلى أخرى. فبعض الدول تبّنت هذا الحل عن طريق الاتفاقيات الدولية، أو من خلال تشريعاتها المتعلقة بجرائم الإنترنت، وبعضها الآخر توسع قضاؤها في تفسير هذه المبادئ ليطبقها على جرائم الإنترنت، ودول أخرى ساير الاجتهاد الفقهي فيها هذا الاتجاه. لذلك لا بد لنا من دراسة أبرز الاتفاقيات والتشريعات التي تعرضت لمسألة الاختصاص، إضافةً إلى الموقف القضائي والفقهي في هذا المجال.

## أولاً- الاتفاقية الأوربية حول الجريمة الافتراضية لعام 2001:

أشارت المادة /22/ من هذه الاتفاقية إلى المبادئ التي يجب على الدول الأطراف اعتمادها، لتحديد الاختصاص القضائي فيما يتعلق بالجرائم المنصوص عليها في هذه الاتفاقية، وهذه المبادئ هي:

### أ-مبدأ الإقليمية:

نصت على هذا المبدأ الفقرة (1) البند (a) من المادة /22/، وقد طلب هذا البند من كل دولة طرف في هذه الاتفاقية أن تعاقب على الجرائم المنصوص عليها، إذا ارتكبت الجريمة ضمن النطاق الإقليمي للدولة.

وعلى سبيل المثال يعد هذا الاختصاص منعقداً، إذا كان نظام الحاسوب العائد للمعتدي ضمن الإطار الإقليمي، ولو كان المعتدي مقيماً خارج الدولة، أو إذا كان نظام الحاسوب العائد للضحية ضمن الإطار الإقليمي للدولة.

كما يعدّ الاختصاص الإقليمي متوفراً وفق هذا البند، إذا كان مصدر الإرسال أو جهة الوصول داخل إقليم الدولة.[1]

## ب-مبدأ نسبية الاختصاص المكاني (الإقليم الاعتباري):

نصت على هذا المبدأ الفقرة (1) البندين ( c و b ) من المادة /22/ ، وقد طلب هذان البندان من كل دولة طرف بالاتفاقية أن تكون مختصة جزائياً بالجرائم المرتكبة على السفن التي ترفع علم الدولة أو الطائرات المسجلة وفقاً للقانون فيها[2].

## ج- مبدأ الجنسية:

نصت على هذا المبدأ الفقرة (1) البند( D ) من المادة /22/، وقد طلب هذا البند من الدول الأطراف أن تكون مختصة جزائياً عندما يرتكب مواطنو أي من هذه الدول جريمة في الخارج، إذا كان هذا السلوك يشكّل جريمة وفق قانون الدولة التي ارتكبت على أرضها الجريمة[3].

## د- مبدأ التعاون الدولي في مكافحة الإجرام أو الصلاحية الشاملة أو العالمية:

نصت على هذا المبدأ الفقرة (3) من المادة /22/، والتي تقضي بأنه في حال رفض أي دولة طرف في هذه الاتفاقية تسليم مرتكب الجريمة المتواجد على

---

(1) د.عمر بن يونس: الاتفاقية الأوربية حول الجريمة الافتراضية ، المرجع السابق، ص181.

(2) د.عمر بن يونس: الاتفاقية الأوربية حول الجريمة الافتراضية ، المرجع السابق، ص182.

(3) د.عمر بن يونس: الاتفاقية الأوربية حول الجريمة الافتراضية ، المرجع السابق، ص183.

أرضها، على أساس مبدأ الجنسية، فيجب على الدولة الرافضة القيام بإجراءات التحقيق والمحاكمة، وفقاً لقانونها الوطني.

ولقد سمحت الفقرة (2) من المادة /22/ من هذه الاتفاقية للدول الأطراف بالتحفظ على هذه المعايير، ولكن لا يجوز التحفظ في نقطتين: الأولى مبدأ الإقليمية، والثانية عندما يكون هناك على الدولة التزام بالتسليم[1].

كما سمحت الفقرة (4) من المادة /22/، للدول الأطراف أن تتخذ أشكالاً أخرى من معايير الاختصاص على نحو يتناسب مع قانونها الوطني.

وإذا كانت جريمة الحاسوب تدخل في اختصاص أكثر من دولة من الدول الأطراف ( مثل جرائم العدوان الفيروسي أو الاحتيال وغيرها)، فإن على هذه الدول التشاور فيما بينها لتحديد المكان الملائم للمحاكمة، حتى يتم تجنب ازدواج الجهود المبذولة، والإزعاج غير الضروري للشهود، أو المنافسة بين السلطات الرسمية في الدول ذات العلاقة (الفقرة /5/ من المادة /22/)[2].

أما التعاون الدولي بين أطراف هذه الاتفاقية، فقد جاءت أحكامه في الفصل الثالث منها.

## ثانياً– القانون العربي الاسترشادي (النموذجي) لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها لعام 2004:

نصت المادة /26/ من هذا القانون (النموذجي)، تحت عنوان "**إطار تطبيق القانون**" على ما يلي:

---

(1) د.عمر بن يونس: الاتفاقية الأوربية حول الجريمة الافتراضية ، المرجع السابق، ص184.

(2) د.عمر بن يونس: الاتفاقية الأوربية حول الجريمة الافتراضية ، المرجع السابق، ص185.

( تسري أحكام هذا القانون على أي من الجرائم المنصوص عليها فيه، حتى ولو ارتكبت كلياً أو جزئياً خارج إقليم الدولة، متى أضرّت بأحد مصالحها، ويختص القضاء الوطني بنظر الدعاوى المترتبة عليها )[1].

ومن الملاحظ أن هذا القانون (النموذجي) عالج مسألة الاختصاص في جرائم الإنترنت على استحياء، إذ إن هذا النص الوحيد لم يأخذ بعين الاعتبار الجرائم التي تدخل ضمن نطاق مبدأ الجنسية ومبدأ العالمية.

## ثالثاً– الولايات المتحدة الأمريكية:

لجاء القضاء الأمريكي لحل مشكلة الاختصاص إلى مبدأ الاختصاص الشخصي "PERSONAL JURISDICTION " المقرر في الدستور الأمريكي، والذي يجعل المحاكم الأمريكية تختص بنظر جرائم الإنترنت في حالتين ، هما:

الأولى: وجود مرتكب الجريمة في الدولة.

الثانية: أن يكون لمرتكب الجريمة وجوداً كافياً في الدولة، أي أن يكون للجاني حد أدنى من الاتصال بالولايات المتحدة الأمريكية[2].

وقد طبق القضاء الأمريكي مبدأ الاختصاص الشخصي بطرق متعددة. ويمكن تلخيص هذه الطرق ضمن ثلاث نظريات ، هي:

### أ–نظرية الإطلاق أو امتداد النتيجة:

في عام 1997، أصدر النائب العام في ولاية "مينيسوتا" الأمريكية إعلاناً، يتضمن تحذيراً إلى مستخدمي ومزودي خدمة الإنترنت، حيث اعتبر الإعلان أن كل جريمة من جرائم الإنترنت، يمكن أن يصل بثها إلى ولاية "مينيسوتا" تكون

---

(1) د.عبد الله عبد الكريم عبد الله: المرجع السابق، ص147.

(2) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت، المرجع السابق، ص90.

قوانين الولاية مختصة بها، حتى ولو ارتكبت الجريمة خارج حدود الولاية، بحيث يبدو الأمر كما لو قام الجاني بإطلاق الرصاص من خارج حدود الولاية على شخص داخل الولاية، فتكون قوانين الولاية مختصة في هذه الحالة. وقد طبق قضاء ولاية "مينيسوتا" هذا المبدأ بشأن جريمة بث موقع لألعاب القمار عبر الإنترنت من "لاس فيغاس" بولاية "نيفادا"، والذي وصل بثه بطبيعة الحال إلى ولاية "مينيسوتا"[1].

## ب- نظرية الحد الأدنى للاتصال:

لخّصت المحكمة الاتحادية العليا في أمريكا المبادئ الأساسية للاختصاص القضائي، بأن من حق المحكمة ممارسة اختصاص قضائي شخصي على المتهم غير المقيم في الولاية، إذا كان هذا المتهم له صلات دنيا بالمجتمع، أو إذا كانت إقامة الدعوى عليه لا تؤذي فكرة المحاكمة العادلة[2].

ويعود التطبيق الأول للاختصاص القضائي على الإنترنت المتعلق بفكرة الحد الأدنى للاتصال إلى عام 1996، وذلك في قضية نُظرت في شمال أمريكا، وتتلخص وقائع هذه القضية بما يلي:

أن شركة INSET SYSTEM المحدودة ، وهي شركة مقرها في ولاية "كونيكيتكوت" Connecticut، قامت برفع قضية سرقة علامة تجارية ضد شركة INSTRUCTION SET التي مقرها في ولاية "ماساشوسيتش" Massachusetts، لأن هذه الأخيرة قامت بتقليد الموقع الإلكتروني للشركة الأولى وهو (Inset.com)، حيث كانت الشركة المنتهكة لهذه العلامة تقوم عبر

---

(1) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت، المرجع السابق، ص 886 و 909.

(2) Adam D Thierer, Clyed wayne crews, Who rules the net?, published by cat to institute, 2003, P- 92 .

هذا الموقع بعرض بضائعها وخدماتها عبر الإنترنت، الأمر الذي أثار حفيظة الشركة المالكة لهذه العلامة التجارية.

وقد تم رفع القضية في ولاية "كونيكتيكوت"، حيث طرحت المحكمة على نفسها السؤال التالي:

**هل يتوفر في هذه القضية الحد الأدنى للاتصال وفق معيار المحكمة الاتحادية العليا؟**

وقد قبلت المحكمة هذه القضية، وبررت قرارها بأن الشركة المعتدية وجّهت نشاطها الإعلاني بشكل مقصود إلى ولاية "كونكيتكوت"، لذلك من المنطقي أن يتم الادعاء عليها هناك[1].

كما استخدم القضاء الأمريكي في مسألة الاختصاص القضائي عبر الإنترنت معيار المواقع الإيجابية والمواقع السلبية، أو ما يُعرف **باختبار السلبية**. ويقصد **بالمواقع الإلكترونية السلبية** المواقع التي تقدم المعلومات فقط، أما **المواقع الإلكترونية الإيجابية** فهي التي تقوم بالتفاعل مع زبائنها، حيث يعتبر الاختصاص القضائي منعقداً إذا كان الموقع إيجابياً[2].

وتطبيقاً لذلك، فقد قامت شركة "بنسوسان" للمطاعم Bensusan Restaurant Corporation، والتي تملك نادي ليلي باسم Blue Note مقره في "نيويورك"، وتملك علامته التجارية، برفع دعوى انتهاك لهذه العلامة ضد شخص يدعى "ريتشارد كينغ" Richard King، لأن هذا الأخير كان يدير نادياً ليلياً في "ميسوري" ويحمل ذات الاسم Blue Note. وقد أنشأ المدير

---

(1) Adam D Thierer, op-cit, P-94.

(2) Adam D Thierer, op-cit, P-93.

المذكور موقعاً إلكترونياً بهذا الاسم، لتقديم معلومات عن النادي وعن مواعيد الحفلات.

وقد أُقيمت الدعوى أمام محكمة نيويورك الفيدرالية، حيث قررت المحكمة بأنها غير مختصة بنظر الدعوى في ولاية نيويورك، وعلّلت قرارها بأن الموقع الإلكتروني للنادي الذي يديره السيد "كينغ" هو موقع سلبي غير فعّال، لأن من يريد شراء التذاكر، كان عليه السفر إلى "ميسوري"، لأن مكتب النادي لا يقوم بإرسال التذاكر بالبريد[1].

## ج-نظرية الاستهداف:

اعتمدت معظم المحاكم في الولايات المتحدة الأمريكية مبدأ الاستهداف في الاختصاص القضائي على الإنترنت، والذي يتطلب أن يستهدف الموقع الإلكتروني سكان ولاية ما.

ففي عام 2001، رفعت شركة American Information Corp دعوى انتهاك علامة تجارية ضد شركة American Information المحدودة، وذلك أمام محكمة ولاية "ميرلاند"، التي قررت أنها غير مختصة قضائياً بنظر هذه الدعوى، لأن نشاطات البيع لم تستهدف سكان الولاية عبر موقعها الإلكتروني[2].

ومن الجدير بالذكر أن نقابة المحامين الأمريكية (ABA)[3]، قامت بإصدار دراسة عالمية حول الاختصاص القضائي للإنترنت، واقترحت بهذه

---

(1) Adam D Thierer, op-cit, P-95.

(2) Adam D Thierer, op-cit, P-106.

(3) وهو اختصار لـ American Bar Association

الدراسة اعتماد مبدأ الاستهداف لحل مشكلة الاختصاص القضائي على الإنترنت[1].

## رابعاً – بريطانيا:

بموجب قانون إساءة استعمال الكمبيوتر لعام 1990، فإن القضاء البريطاني يختص بالجرائم التي ينص عليها هذا القانون إذا اقترفت ضمن الاختصاص الإقليمي، أي إذا كان حاسوب الجاني أو حاسوب الضحية داخل إقليم الدولة[2].

كما تم إحداث اختصاصات قضائية حديثة بموجب قانون العدالة الجزائية البريطاني لعام 1993[3]، حيث تناولت هذه الاختصاصات معظم جرائم الاحتيال العابرة للحدود، وجرائم الابتزاز وغيرها[4].

وفي إحدى القضايا المعروضة على القضاء البريطاني، تمّت إدانة مواطن فرنسي مقيم في لندن، بجرم نشر المواد الفاحشة، حيث كان هذا الفرنسي يدير موقعاً على الإنترنت مخصصاً للمثليين جنسياً. وقد دفعت جهة الدفاع بعدم اختصاص القضاء البريطاني، لأن هذا الموقع كان مستضافاً على مُخدّم في الولايات المتحدة الأمريكية، إلاّ أن المحكمة الملكية أعلنت اختصاصها وأدانت المتهم، لأن هذه المواد الفاحشة تمّ نشرها في إنكلترا، كونها ظهرت على شاشة الحاسوب العائد لأحد الضباط المختصين في مكافحة هذه

---

(1) Adam D Thierer, op-cit, P-107.

(2) القاضي د. غسان رباح: المرجع السابق، ص167. د.عمر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، المرجع السابق، ص911.

(3) Criminal Justice Act 1993 متوفر على الإنترنت على الموقع www.britishlaw.org.uk

(4) Micheal Hirst, Jurisdiction and the Ambit of the criminal law, published by oxford university, 2003, P-111-113.

الجرائم في إنكلترا، ومن ثم فإن وصول البث إلى إنكلترا، يعدّ بمثابة ارتكاب الجريمة فيها[1].

## خامساً– فرنسا:

تضمن قانون العقوبات الفرنسي لعام 1992 القواعد المتعلقة بتنازع القوانين الجزائية من حيث المكان، والمنصوص عليها في المواد (1-113وحتى 7-113) منه[2]. وقد تضمنت هذه القواعد مبادئ الإقليمية والعينية والشخصية، التي قام القضاء الفرنسي بتطبيقها على جرائم الإنترنت. ففي إحدى القضايا التي عرضت على القضاء الفرنسي، تمّ إدانة مديري شركة "فرانس نت" France net و "ورد نت" World Net، لأنهما قاما بنشر صور دعارة أطفال آتية من الخارج[3]. وفي رأي الفقه، فإن وجود المخدم المضيف[4] في الخارج لا يؤثر على وقوع الجريمة، كما يعد فعل البث أحد العناصر المكونة للجريمة[5].

---

(1) Michael Hirst, op-cit, P-188.

(2) قانون العقوبات الفرنسي متوفر على موقع القوانين الفرنسية www.legifrance,gouv.fr

(3) القضية متوفرة على www.francenet.fr مشار إليها عند : د.جميل عبد الباقي الصغير: الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، 2002، ص 50.

(4) **المضيف** Host, هو حاسوب يتصل به عدد من الطرفيات والحواسيب الأخرى، ويقوم بعمليات المحاسبة والمعالجة، ويمكّن الحواسيب الأخرى من الوصول إلى الملفات المخزنة فيه. وعند فتح حساب انترنت لدى المضيف، يقوم بحجز مساحة من الذاكرة لخدمة هذا الحساب، ويؤمن له الوسائل البرمجية اللازمة للتعامل وإدارة الاتصال. د.عبد الحسن الحسيني: المرجع السابق، ص406.

(5) د.جميل عبد الباقي الصغير: الجوانب الإجرائية للجرائم المتعلقة بالإنترنت, المرجع السابق، ص46 وما بعدها. د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت، المرجع السابق، ص912.

**سادساً– إيطاليا:**

طبق القضاء الإيطالي مبدأ الإقليمية المنصوص عليه بقانون العقوبات الإيطالي على جريمة القذف عبر الإنترنت، حيث اعتبرت محكمة النقض الإيطالية أن القذف عبر الإنترنت لا يختلف فحواه عن ذلك المقرر في قانون العقوبات الإيطالي، لأن كل صورة أو قول أو معلومة يتم بثها عبر الإنترنت، ويمكن رؤيتها من قبل مجموعة غير محدودة من الناس في أي مكان حول الكرة الأرضية، فهناك جريمة تامة، ليس اعتباراً من الوقت الذي تمّ فيه بث الرسالة المجرّمة، وإنما من الوقت الذي أمكن فيه قراءة الرسالة من قبل الغير، وهذا ما يعرف **مبدأ الوجود في كل مكان**، إذ إن الجريمة تعد كما لو كانت قد وقعت في الأرض الإيطالية[1].

**سابعاً– الإمارات العربية المتحدة:**

طبق قضاء إمارة دبي مبدأ الإقليمية على واقعة قذف عبر الإنترنت، ارتكبتها إحدى الصحف الإلكترونية التي مقرها لندن، حيث كانت المجني عليها عند قراءة ألفاظ القدح موجودة في دبي. وقد اعتبرت المحكمة أنه طالما أن نتيجة الفعل تحققت في دبي، فإن الجريمة تعد قد وقعت في إقليم الدولة، وتخضع لأحكام قانون العقوبات الإماراتي[2].

**ثامناً– مصر:**

اجتهد الفقه المصري في حل مشكلة الاختصاص الجزائي عبر الإنترنت، حيث قام بتطبيق مبادئ الإقليمية والعينية والشخصية المقررة في قانون العقوبات المصري على جرائم الإنترنت؛ حيث اعتبر أن بثّ صور إباحية أو

---

(1) حكم محكمة النقض الايطالية متوفر على www.penale.it مشار إليه عند: د. عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت، المرجع السابق، ص903.

(2) استئناف دبي (1248، 2003/1252) مشار إليه عند محمد الكعبي، المرجع السابق، ص62.

رسالة مُجرمة عبر الإنترنت، يعقد الاختصاص لقانون العقوبات المصري بمجرد وصول البث إلى مصر، ولو كان الفعل غير معاقب عليه في البلد الذي تمّ منه البث، ومن ثم فإن وجود المخدّم المضيف خارج إقليم الدولة لا أثر له على وقوع الجريمة[1].

وبعد هذه الجولة على الموقف القانوني والقضائي المقارن في مسألة الاختصاص، نجد أن معظم الدول قامت بتطبيق مبدأ الإقليمية والمبادئ الأخرى المعمول بها في تحديد الاختصاص الجزائي الدولي على جرائم الإنترنت، حيث اعتبرت وصول البث إلى إقليم الدولة هو أحد العناصر المكونة للجريمة، ولو كان المخدّم المضيف خارج إقليم الدولة.

(1) د. جميل عبد الباقي الصغير: الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، المرجع السابق، ص47 وما بعدها. د.أحمد حسام طه تمام: المرجع السابق، ص145 وما بعدها. فهد سلطان محمد أحمد بن سليمان: مواجهة جرائم الإنترنت (دراسة مقارنة)، رسالة ماجستير مقدمة إلى كلية الحقوق، جامعة القاهرة، 2004، ص111.

# المطلب الثاني

# مسألة الاختصاص في ظل التشريع السوري

استعمل المشرع السوري في قانون العقوبات تعبير (الصلاحية) للدلالة على(الاختصاص)، وأخذ بأربعة مبادئ لتحديد اختصاصه الجزائي الدولي، هي: الصلاحية الإقليمية، والصلاحية الذاتية (أو العينية)، والصلاحية الشخصية، والصلاحية الشاملة (أو العالمية).

ومن الملاحظ أن المشرع السوري قد أخذ بالصلاحية الإقليمية كمبدأ أساسي، أسوة بالتشريع المقارن، إلاّ أنه لم يقنع بإنفراده، لذلك جمع بين هذه الصلاحيات الأربعة حتى تكمل بعضها البعض، كي يطال الجرائم المرتكبة خارج إقليم الدولة التي يرى فيها مساساً بمصالحه واعتباراته.

## أولاً- الصلاحية الإقليمية:

يقصد بمبدأ إقليمية القانون الجزائي، أن القانون الجزائي لدولة ما يطبق على كل جريمة ترتكب على إقليم هذه الدولة، سواء أكان الجاني يحمل جنسية هذه الدولة أم يحمل جنسية دولة أجنبية، وسواء أكان المجني عليه مواطناً أم أجنبياً.

ويستند هذا المبدأ إلى عدة مبررات، منها فكرة سيادة الدولة على إقليمها، إذ إن تطبيق القانون الجزائي إقليمياً هو من أهم مظاهر السيادة على الإقليم، فالقانون الجزائي هو الذي يضمن حماية الحقوق الدستورية والقانونية. أضف إلى ذلك أن محكمة مكان ارتكاب الجريمة أقدر على جمع الأدلة والإحاطة بجميع ظروفها وشهودها وفاعلها، كما أن محاكمة الجاني في مكان ارتكاب

الجريمة يحقق الردع العام، ويقضي على الاضطراب الاجتماعي الذي أحدثته الجريمة بالمجتمع[1].

ولمبدأ إقليمية القانون الجزائي نتيجتان: الأولى إيجابية، وهي أن يكون للقانون الجزائي تطبيق شامل على كافة الجرائم المرتكبة على إقليم الدولة، الأمر الذي يؤدي بالضرورة إلى عدم تطبيق القوانين الجزائية الأجنبية على هذه الجرائم. أما النتيجة الثانية فسلبية، وهي تقضي بعدم تطبيق القانون الجزائي على أية جريمة ترتكب خارج حدود الدولة[2].

وقد أخذ المشرع السوري بمبدأ الإقليمية في المادة /15/ من قانون العقوبات ، حيث نصت هذه المادة على ما يلي:

(1-يطبق القانون السوري على جميع الجرائم المقترفة في الأرض السورية.

2-تعد الجريمة مقترفة في الأرض السورية:

أ-إذا تمّ على هذه الأرض أحد العناصر التي تؤلف الجريمة، أو فعل من أفعال جريمة غير متجزئة، أو فعل اشتراك أصلي أو فرعي.

ب-إذا حصلت النتيجة في هذه الأرض، أو كان متوقعاً حصولها فيها.)

ومن الملاحظ أن المشرع السوري في الفقرة الثانية من هذه المادة أراد أن يوسع من صلاحيته الإقليمية لتشمل مختلف الجرائم التي تهدد الحقوق المحمية بموجب القانون السوري، وقد استخدم في هذا التوسع الركن المادي (سلوك

---

(1) د.محمود نجيب حسني: شرح قانون العقوبات اللبناني – القسم العام, المجلد الأول ، الطبعة الثالثة (معدلة ومنقحة)، منشورات الحلبي الحقوقية، بيروت، عام 1988، ص180. د.عبد الوهاب حومد: المفصل في شرح قانون العقوبات – القسم العام، المطبعة الجديدة، دمشق، عام 1990، ص1080. د. عبود السراج، المرجع السابق، ص165.

(2) د.محمود نجيب حسني: شرح قانون العقوبات اللبناني – القسم العام، المرجع السابق، ص180.

ونتيجة وعلاقة سببية) كمعيار لتحديد ما إذا كانت الجريمة قد وقعت على الأرض السورية أم لا[1]، وهو مسلكٌ مرحبٌ به، لأن الفقه والقضاء لم يقبلا بالركن المعنوي بمفرده كمعيار لتحديد الاختصاص[2].

والواقع أن تطبيق مبدأ الإقليمية على جريمة الاحتيال عبر الإنترنت لا يثير أية صعوبة إذا كانت جميع عناصر الجريمة قد وقعت على الأرض السورية، فإذا قام شخص مقيم في سورية مثلاً باستخدام الإنترنت لاختراق النظام المعلوماتي لأحد المصارف العاملة في سورية، ثم قام بتحويل أرصدة بعض الحسابات إلى حسابه المصرفي، فإن جميع عناصر جريمة الاحتيال تكون قد وقعت على الأرض السورية.

لكن تطبيق مبدأ الإقليمية ليس دوماً بهذه السهولة، فالغالب أن جريمة الاحتيال عابرة للحدود، وبالتالي فإن عناصر الجريمة تتوزع على أقاليم عدة دول، الأمر الذي يفرض علينا طرح الأسئلة التالية:

- **متى تعتبر جريمة الاحتيال عبر الإنترنت مقترفة على الأرض السورية؟**
- **ما هو المقصود بالإقليم السوري في إطار جرائم الإنترنت؟**
- **وهل يوجد استثناءات لمبدأ الإقليمية في إطار جرائم الإنترنت؟**

---

(1) د. عبود السراج، المرجع السابق، ص166.

(2) د.عبد الوهاب حومد: المرجع السابق، ص1093.

## أ-الحالات التي تعتبر فيها جريمة الاحتيال عبر الإنترنت مقترفة على الأرض السورية:

تعد جريمة الاحتيال عبر الإنترنت مقترفة على الأرض السورية، وفق الفقرة الثانية من المادة /15/ من قانون العقوبات السوري، في الحالات التالية:

1- **إذا تمّ على الأرض السورية أحد العناصر التي تؤلف جريمة الإنترنت.** ومثال ذلك، قيام شخص موجود في سورية بإنشاء موقع للاحتيال عبر الإنترنت- سواء كان الموقع مستضافاً على مُخدّم سوري أم أجنبي- ثم يقع ضحية هذا الموقع شخص مقيم في الصين.

وغني عن البيان أن الأعمال التحضيرية لا تدخل ضمن عناصر الجريمة، ولا ترتقي إلى الأفعال التنفيذية، فلو قام شخص مقيم في لبنان مثلاً بإرسال رسالة إلكترونية إلى شخص مقيم في الصين، تتضمن فوز المرسل إليه بجائزة وهمية بقصد الاحتيال عليه، فإن القانون السوري لا يطبق لمجرد قيام الجاني بشراء الحاسوب من سورية.

2- **إذا تمّ على الأرض السورية فعل من أفعال جريمة غير متجزئة.** ويدخل في مفهوم الجريمة غير المتجزئة، الجريمة المستمرة والجريمة المتتابعة وجريمة العادة. وجريمة الاحتيال من الممكن أن تكون متتابعة (متعاقبة)، فإذا قام شخص موجود في لبنان مثلاً، بالاحتيال على شخص موجود في سورية عن طريق البريد الإلكتروني، ثم قام هذا الجاني بالاحتيال عدة مرات على ذات المجني عليه، عن طريق الإنترنت، ففي هذه الحالة تكون جريمة الاحتيال متتابعة (متعاقبة) بسبب وحدة الإرادة الجرمية، ووحدة الحق المعتدي عليه، ووحدة الغرض.

3- **إذا وقع على الأرض السورية فعل اشتراك أصلي أو فرعي.** كما لو اشترك شخص موجود في سورية بعملية اختراق لنظام معلوماتي عبر الإنترنت عائد لأحد المصارف الأمريكية بقصد الاحتيال مع شخص آخر موجود في اليابان. فيتحقق هنا (الاشتراك الأصلي).

أما إذا قام شخص موجود في سورية بتقديم إرشادات لشخص موجود في اليابان، لاختراق نظام معلوماتي لأحد المصارف الأمريكية بهدف تمكينه من الاحتيال. فيتحقق هنا التدخل (الاشتراك الفرعي).

4- **إذا حصلت النتيجة الجرمية على الأرض السورية أو كان متوقعاً حصولها فيها.** فإذا قام شخص موجود في كندا بإنشاء موقع للاحتيال عبر الإنترنت لتداول الأسهم الوهمية، ووقع ضحية هذا الموقع شخص موجود في سورية، فتكون النتيجة الجرمية هنا قد وقعت في سورية.

**وتكون النتيجة متوقعاً حصولها في سورية وإن لم تحصل فعلاً.** إذا قام شخص موجود في الإمارات مثلاً باستخدام بطاقة ائتمان مزورة للشراء من أحد المواقع الإلكترونية لشركة سورية، إلاّ أن الجريمة توقفت عند حد الشروع لظروف خارجة عن إرادة الفاعل.

**ويرى الباحث** أن وصول البث إلى سورية لا يكفي بحد ذاته لانعقاد اختصاص القانون الجزائي السوري على أساس أن النتيجة وقعت في سورية، لأن مواقع الإنترنت يصل بثها بطبيعة الحال إلى أي مكان في العالم، بل لا بد من أن يكون المجني عليه موجوداً في سورية. وهذا التطبيق يشبه إلى حدٍ بعيد نظرية الاستهداف التي قام القضاء الأمريكي بتطبيقها.

**ب-الإقليم السوري[1]:**

حددت المادتان /16/ و /17/ من قانون العقوبات نطاق الإقليم السوري، والذي يتألف من أربعة أقاليم هي: الإقليم البري، والإقليم البحري، والإقليم الجوي، والإقليم الاعتباري.

**1-الإقليم البري:**

وهو المساحة من الكرة الأرضية التي تقع ضمن الحدود السورية المعينة سياسياً ودولياً بموجب الاتفاقيات. ويشمل هذا الإقليم سطح الأرض وما في باطنها إلى ما لانهاية حتى مركز الأرض، كما يشمل البحيرات والأنهار الداخلية والأجزاء التابعة للدولة من الأنهار الدولية والبحار المغلقة.

**2-الإقليم البحري:**

وهو البحر المتصل بالأرض السورية، ويبدأ من أدنى مستوى لمياه الجزر المنحسرة حتى مسافة عشرين كيلو متراً. ويشمل هذا الإقليم الخلجان والمضائق والقنوات والموانئ البحرية.

**3-الإقليم الجوي:**

ويشمل طبقات الهواء التي تغطي الإقليمين البري والبحري إلى ما لانهاية في الارتفاع.

**4-الإقليم الاعتباري:**

يعتبر في حكم الأرض السورية بحسب المادة /17/ من قانون العقوبات:

- السفن والمركبات الهوائية السورية أينما وجدت، سواء أكانت ملكاً للدولة أم للأفراد، ما دامت مسجلة في سورية.

---

(1) د. عبود السراج، المرجع السابق، ص168- 169 . د.عبد الوهاب حومد: المرجع السابق، ص1082 وحتى 1094.

- الأرض الأجنبية التي يحتلها الجيش السوري، إذا كانت الجرائم المقترفة عليها تنال من سلامة الجيش أو من مصالحه.

وتطبيقاً لذلك، فالفرنسي الذي يقوم أثناء ركوبه في طائرة أو سفينة سورية، بإرسال رسالة إلكترونية تحمل مضموناً احتيالياً من حاسوبه إلى شخص موجود في إيطاليا، يخضع للقانون السوري أينما وجدت هذه الطائرة أو السفينة.

والواقع أن هناك تساؤلاً يتبادر للأذهان أثناء دراسة الإقليم الاعتباري، وهو: **أليس من الجائز اعتبار تلك المساحة من الإنترنت، الخاضعة لإدارة الدولة السورية التي تنتهي باللاحقة sy. جزءاً من الإقليم الاعتباري السوري أو بحكم الأرض السورية؟**

نعتقد بأن الإجابة على هذا السؤال تكون بالإيجاب، للسببين التاليين:

- إن المبررات المتعلقة بسيادة الدولة على إقليمها، والتي دفعت المشرع الجزائي إلى اعتبار الطائرة أو السفينة السورية بحكم الأرض السورية، متوفرة في ذلك **النطاق العلوي السوري** على الإنترنت، الذي يخضع لإدارة الحكومة السورية (المنتهي بـ sy)[1]، فهذا النطاق يحمل العلم السوري أو الجنسية السورية، وبالتالي فإن اعتباره بحكم الأرض السورية يتفق مع فلسفة المشرع السوري.
- هناك مبررات عملية تدفعنا إلى اعتبار النطاق الوطني السوري على الإنترنت بحكم الأرض السورية، وهي أن هناك جرائم من الممكن أن

(1) عرفت المادة الأولى من قانون التوقيع الإلكتروني وخدمات الشبكة رقم 4 لعام 2009 **النطاق العُلوي الوطني** بأنه: (اسم نطاق عُلوي قياسي تندرج تحته جميع مواقع أو موارد الإنترنت التي تديرها سلطة واحدة ذات صبغة وطنية.) والنطاق العُلوي السوري هو المنتهي باللاحقة (sy.)

ترتكب عبر هذا النطاق السوري، دون أن تطولها قواعد الاختصاص الجزائي الدولي السورية، ونضرب على ذلك المثال التالي:

إذا أنشأت شركة فرنسية موقعاً إلكترونياً لها على النطاق السوري المنتهي بـ (.SY) ، ثم قامت عبر هذا الموقع بالاحتيال على بعض الإيطاليين الموجودين في إيطاليا، فإن هذه الجريمة لا تخضع للقانون الجزائي السوري، لأن قواعد الاختصاص الدولي لا تسمح بذلك، فلا تنطبق على هذا المثال الصلاحية الإقليمية أو الشخصية أو الذاتية أو الشاملة، مع العلم أن الجريمة تمّت عبر النطاق الوطني السوري على الإنترنت.

وبناءً على ما تقدم، فإن **الباحث يقترح** على المشرع السوري في مشروع قانون الجريمة الإلكترونية، الأخذ بهذا الرأي لكي لا تبقى بعض الجرائم المرتكبة على هذا النطاق بدون حساب.

## ج-استثناءات مبدأ إقليمية القانون الجزائي:

أشار قانون العقوبات السوري إلى استثناءين لمبدأ إقليمية القانون الجزائي، الأول يتعلق ببعض الجرائم، والثاني يتعلق ببعض الأشخاص.

### 1-الجرائم التي لا يشملها الاختصاص الإقليمي:

نصت الفقرة /18/ من قانون العقوبات على ما يلي:

(لا يطبق القانون السوري:

1-في الإقليم الجوي السوري، على الجرائم المقترفة على متن مركبة هوائية أجنبية، إذا لم تتجاوز الجريمة شفير المركبة.

على أن الجرائم التي لا تتجاوز شفير المركبة الهوائية تخضع للقانون السوري إذا كان الفاعل أو المجني عليه سورياً، أو حطّت المركبة الهوائية في سورية بعد اقتراف الجريمة.

2-في البحر الإقليمي السوري أو في المدى الجوي الذي يغطيه، على الجرائم المقترفة على متن سفينة أو مركبة هوائية أجنبية إذا لم تتجاوز الجريمة شفير السفينة أو المركبة الهوائية.).

وتطبيقاً لذلك، فقيام فرنسي باختراق النظام المعلوماتي لأحد المصارف الأمريكية بقصد الاحتيال، أثناء ركوبه في طائرة تابعة للخطوط الجوية الألمانية، وهي تعبر الأجواء السورية، لا يدخل ضمن الاختصاص الإقليمي السوري. وهذا الأمر يتفق مع المنطق، لأن هذه المركبات الهوائية الأجنبية تعتبر جزءاً من إقليم الدولة التابعة لها، إضافةً إلى أن هذه الجرائم لا تمسّ المصالح السورية. ويختلف الأمر إذا تحققت إحدى الاستثناءات الواردة في نهاية الفقرة الأولى من المادة /18/ وهي[1]:

- إذا تجاوزت الجريمة شفير المركبة الهوائية.
- إذا كان الجاني أو المجني عليه سورياً.
- إذا حطت المركبة الهوائية في سورية بعد اقتراف الجريمة.

ومن الملاحظ أنه يصعب عملياً تخيل ارتكاب جريمة إنترنت على متن مركبة هوائية أجنبية وهي تعبر الإقليم الجوي السوري دون أن تتجاوز شفير أو حدود هذه المركبة، وذلك بسبب الطبيعة العالمية لجرائم الإنترنت. على أن هذا الاختصاص الواسع لا ضير فيه، طالما أن تحريك الدعوى العامة أمر يدخل في السلطة التقديرية النيابة العامة.

---

(1) د. عبود السراج: المرجع السابق، ص171-172.

أما الجرائم المنصوص عليها في الفقرة الثانية من المادة /18/، والمرتكبة في البحر الإقليمي أو في المدى الجوي الذي يغطيه، على متن سفينة أو مركبة هوائية أجنبية دون أن تتجاوز شفير السفينة أو المركبة الهوائية، فإن المشرع السوري جعلها خارج الصلاحية الإقليمية دون أي استثناء.

**2-الأشخاص الذين لا يشملهم الاختصاص الإقليمي:**

يُستثنى من مبدأ إقليمية القانون الجزائي فئتان من الأشخاص، هما:

- موظفو السلك الخارجي والقناصل الأجانب، بالنسبة للجرائم التي يقترفوها على الأرض السورية، ما داموا يتمتعون بالحصانة التي يخولهم إياها القانون الدولي (المادة 22 من قانون العقوبات).
- رجال القوات الحربية الأجنبية الذين يرابطون في الإقليم السوري بإذن من حكومته، بالنسبة للجرائم التي يقترفوها أثناء أداء عملهم وفي داخل المناطق المخصصة لهم[1].

والواقع إن تطبيق جرائم الإنترنت على هذين الاستثناءين لا يثير أي مشكلة، وله ذات المبررات التي شُرّع من أجلها في الجرائم التقليدية.

**ثانياً- الصلاحية الذاتية أو العينية:**

يقصد بمبدأ الذاتية أو العينية، تطبيق القانون الجزائي على الجرائم التي تمسّ المصالح الأساسية للدولة، والمرتكبة خارج إقليمها، أيّاً كانت جنسية مرتكبها. وهذا المبدأ يفرضه حرص الدولة على حماية مصالحها الأساسية[2].

(1) د. عبود السراج: المرجع السابق، ص173. د.محمود نجيب حسني: شرح قانون العقوبات اللبناني – القسم العام، المرجع السابق، ص194.

وقد أخذ المشرع السوري بهذا المبدأ في المادة /19/ من قانون العقوبات، التي نصت على ما يلي:

(1-يطبق القانون السوري على كل سوري أو أجنبي، فاعلاً كان أو محرضاً أو متدخلاً، أقدم خارج الأرض السورية على ارتكاب جناية أو جنحة مخلّة بأمن الدولة، أو قلّد خاتم الدولة، أو قلّد أو زوّر أوراق العملة أو السندات المصرفية السورية أو الأجنبية المتداولة شرعاً أو عرفاً في سورية.

2-على أن هذه الأحكام لا تطبق على الأجنبي الذي لا يكون عمله مخالفاً لقواعد القانون الدولي.).

وتطبيقاً لذلك، فإن بعض الجرائم المحددة في هذا النص يمكن أن ترتكب عبر الإنترنت، فإذا قام شخص في الخارج باختراق النظام المعلوماتي لوزارة الدفاع السورية عبر الإنترنت، بقصد الحصول على معلومات سرية، يكون مرتكباً لجريمة التجسس المنصوص عليها بالمادة /272/ عقوبات.

وأيضاً من يقوم في الخارج بنشر كتابات عبر الإنترنت لم تجزها الحكومة السورية، فعكّر صلات سورية بدولة أجنبية، يكون مرتكباً لجريمة ماسة بالقانون الدولي حسب المادة /278/ عقوبات.

وغني عن البيان بأن جريمة الاحتيال (موضوع البحث) ليست من ضمن الجرائم المحددة بالمادة /19/ عقوبات، إلاّ إن طبيعة قواعد الاختصاص الدولي تفرض علينا التعرض للصلاحية الذاتية بعجالة.

## ثالثاً- الصلاحية الشخصية:

---

(2) د. عبود السراج: المرجع السابق، ص175. د.محمود نجيب حسني: شرح قانون العقوبات اللبناني – القسم العام، المرجع السابق، ص197. د.عبد الوهاب حومد: المرجع السابق: ص1095.

يطبق مبدأ الصلاحية الشخصية بطريقتين: إيجابية وسلبية. ويقصد **بالطريقة الإيجابية** تطبيق القانون الجزائي على مرتكب الجريمة الذي يحمل جنسية الدولة ولو ارتكبت الجريمة خارج إقليمها. أما **الطريقة السلبية**، فيقصد بها تطبيق القانون الجزائي على كل جريمة يكون المجني عليه حاملاً لجنسية الدولة، ولو ارتكبت الجريمة خارج إقليمها، وأيّاً كانت جنسية مرتكب الجريمة.

وتطبيق مبدأ الشخصية بالطريقة الإيجابية، يؤدي إلى تجنب فرار المجرم الذي يسيء إلى سمعة وطنه عندما يرتكب جريمته خارج إقليم دولته ثم يفر إليها، إذ إن دولته لا تستطيع معاقبته على أساس مبدأ الإقليمية، ولا تستطيع تسليمه إلى الدولة التي ارتكب الجرم على أرضها، لأنه من رعاياها كما هو سائد في معظم التشريعات الجزائية. أما تطبيق مبدأ الشخصية بالطريقة السلبية، فهو يؤمن حماية رعايا الدولة من الاعتداءات الجرمية عليهم[1].

والمشرع السوري أخذ بمبدأ الشخصية في وجهه الإيجابي فقط بالمادة /20/ من قانون العقوبات، ولم يأخذ بهذا المبدأ في وجهه السلبي، لأنه انطلق من مبدأ الثقة بالقضاء الأجنبي، وقدرته على حماية المواطنين السوريين، إذا ارتكبت بحقهم جرائم معاقب عليها في القانون الأجنبي.

وقد نصت المادة /20/ من قانون العقوبات على ما يلي:

(يطبق القانون السوري على كل سوري، فاعلاً كان أو محرضاً أو متدخلاً، أقدم خارج الأرض السورية، على ارتكاب جناية أو جنحة يعاقب عليها القانون السوري.

---

(1) د.محمود نجيب حسني: شرح قانون العقوبات اللبناني – القسم العام، المرجع السابق، ص 201– 202.

ويبقى الأمر كذلك ولو فقد المدعى عليه الجنسية السورية أو اكتسبها بعد ارتكاب الجناية أو الجنحة.).

كما أكّد المشرع السوري بالمادة /21/ من قانون العقوبات، على تطبيق هذا المبدأ بالنسبة للجرائم التي يقترفها الموظفون السوريون في الخارج، أثناء ممارستهم وظائفهم أو بمناسبة ممارستهم لها، وعلى الجرائم التي يرتكبها أيضاً موظفو السلك الخارجي والقناصل السوريون الذين يتمتعون بالحصانة الدبلوماسية.

والمشرع السوري لم يأخذ بمبدأ الشخصية على إطلاقه في جميع الجنح التي يرتكبها المواطن السوري في الخارج، إذ يمكن أن نميز في نطاق الجنحة بين حالتين[1]:

1- إذا كانت الجنحة المرتكبة من قبل السوري في الخارج معاقباً عليها بالحبس ثلاث سنوات فأكثر وفق القانون السوري، فإن القانون السوري يطبق على الجاني دون النظر فيما إذا كان القانون الأجنبي يعاقب عليها أم لا.

2- إذا كانت الجنحة المرتكبة من قبل السوري في الخارج معاقباً عليها بالحبس أقل من ثلاث سنوات وفق القانون السوري، فيجب أن يكون القانون الأجنبي في هذه الحالة قد عاقب على هذه الجنحة أيضاً بعقوبة مهما كان نوعها، حتى نستطيع تطبيق القانون السوري، أي يجب أن يتحقق شرط المعاقبة في القانون الأجنبي، أما إذا لم يكن القانون الأجنبي

---

(1) د.عبد الوهاب حومد: المرجع السابق، ص1098. د. عبود السراج: المرجع السابق، ص 183. د.محمود نجيب حسني: شرح قانون العقوبات اللبناني – القسم العام، المرجع السابق، ص 213.

قد نص على أية عقوبة لهذا الفعل، فإن القانون السوري لا يمكن تطبيقه.

أما في الجنايات، فمبدأ الشخصية يطبق على إطلاقه، فكل سوري ارتكب جناية في الخارج، سواء أكان القانون الأجنبي يعاقب عليها أم لا، يعاقب وفق القانون السوري (المادة 24 عقوبات).

وتطبيقاً لذلك، فالسوري الذي يقوم في الخارج بإنشاء موقع على الإنترنت ينتحل فيه الاسم التجاري لإحدى الشركات، ويقوم من خلاله بالاحتيال على أشخاص موجودين خارج سورية أيضاً، يمكن ملاحقته وفقاً للصلاحية الشخصية، إذا كان القانون الأجنبي يعاقب على هذا الفعل بعقوبة مهما كان نوعها، لأن عقوبة الاحتيال وفق القانون السوري جنحية الوصف، وهي الحبس من ثلاثة أشهر إلى سنتين والغرامة من مائة إلى خمسمائة ليرة سورية (المادة 641 عقوبات)، أي أن هذه العقوبة لا تبلغ ثلاث سنوات، ومن ثم يجب تحقق شرط المعاقبة في القانون الأجنبي.

وبناءً على ما تقدم، **فالباحث يقترح** على المشرع السوري في مشروع قانون الجريمة الإلكترونية، أن يرتفع بالحد الأعلى لعقوبة الحبس إلى ثلاث سنوات في جميع الجرائم الإلكترونية المعاقب عليها بعقوبة جنحية، وذلك حتى يتجنب الشرط المتعلق بضرورة تجريم الفعل في الدولة التي ارتكبت الجريمة فيها، عند تطبيق مبدأ الشخصية على الجرائم الإلكترونية.

## رابعاً– الصلاحية الشاملة:

أخذ المشرع السوري بهذا المبدأ في المادة /23/ من قانون العقوبات، التي نصت على ما يلي:

(يطبق القانون السوري على كل أجنبي مقيم على الأرض السورية، أقدم في الخارج سواء أكان فاعلاً أو محرضاً أو متدخلاً، على ارتكاب جناية أو جنحة غير منصوص عليها في المواد 19 ،20 ،21 إذا لم يكن استرداده قد طلب أو قُبل.).

لا يعد هذا الاختصاص، اختصاصاً رئيسياً وإنما هو اختصاص ثانوي أو احتياطي. أي أن سورية لا تعاقب المجرمين الذين يقيمون على أرضها، إلاّ إذا لم يوجد من يعاقبهم من الدول الأجنبية.

وينطوي هذا الاختصاص على نوع من التعاون أو التضامن الدولي في مكافحة الإجرام، فهو يضمن عدم إفلات المجرمين الذين سولت لهم أنفسهم ارتكاب الجرائم في دولة، ثم الفرار إلى دولة أخرى تملصاً من المسؤولية[1].

وعليه فالأجنبي الذي يرتكب جريمة في الخارج، ويلقى القبض عليه في سورية، يمكن محاكمته بموجب هذا الاختصاص الشامل، ولو لم يكن للقانون السوري اختصاص رئيسي في محاكمته، بشرط أن لا تطلب دولة أجنبية تسليمه من سورية، أو طلبت تسليمه لكن سورية رفضت التسليم، كأن يكون لاجئاً سياسياً مثلاً.

وتطبيقاً لذلك، فإذا قام هولندي موجود في الخارج مثلاً، باختراق النظام المعلوماتي لمصرف إيطالي، وتحويل الأرصدة إلى حسابه احتيالاً، ثم حضر إلى سورية وألقي القبض عليه فيها، فيمكن محاكمته وفقاً للصلاحية الشاملة إذا لم يكن استرداده قد طلب من سورية أو قُبل.

## الاختصاص الداخلي:

(1) د. عبود السراج: المرجع السابق، ص 178– 179. د.عبد الوهاب حومد: المرجع السابق، ص1103–1104. د.محمود نجيب حسني: شرح قانون العقوبات اللبناني – القسم العام، المرجع السابق، ص 208–209.

بعد انعقاد الاختصاص الدولي للقانون الجزائي السوري وفقاً للصلاحيات السابق ذكرها، يتم تطبيق قواعد الاختصاص الداخلي بأنواعه الولائي والشخصي والنوعي والمكاني.

فبموجب **الاختصاص الولائي**، يكون القضاء الجزائي العادي، صاحب الاختصاص العام بالنظر في جميع جرائم الإنترنت ومنها الاحتيال.

ويختص **قضاء الأحداث** شخصياً بمحاكمة الأحداث الذين يرتكبون جرائم الإنترنت وفق قانون الأحداث رقم /18/ لعام 1974وتعديلاته.

كما يختص **القضاء العسكري** بالنظر في جرام الإنترنت المرتكبة من قبل العسكريين أو عليهم، أو المرتكبة ضد مصالح الجيش مباشرة، وفق قانون العقوبات العسكري الصادر بالمرسوم التشريعي رقم /61/ لعام 1950 وتعديلاته[1].

وتختص **محكمة أمن الدولة** بالنظر في الجرائم المخلّة بأمن الدولة الداخلي والخارجي المرتكبة عبر الإنترنت، إضافةً إلى الجرائم الأخرى المنصوص عليها بالمرسوم رقم /6/ لعام 1965، وذلك وفق قانون إحداث محكمة أمن الدولة العليا الصادر بالمرسوم التشريعي رقم /47/ لعام 1968.

أما **الاختصاص النوعي**، فيقصد به توزيع الاختصاص داخل القضاء الواحد بعد أن ينعقد له الاختصاص الولائي أو الشخصي. والضابط أو المعيار في توزيع الدعاوى ضمن القضاء العادي هو جسامة الجريمة (جناية أو جنحة أو مخالفة). فمحكمة الجنايات تختص بالقضايا التي من نوع الجناية، ويكون

---

(1) المواد 50 و 132 وحتى 141 من قانون العقوبات العسكري. وتجدر الإشارة إلى أنه في حال وقوع الجريمة على العسكري, فيجب أن تنال الجريمة من شخصه أو إرادته . وبناءً عليه فالسرقة الواقعة على مال العسكري لا تدخل ضمن اختصاص القضاء العسكري. أما الاحتيال على العسكري فيدخل في اختصاص القضاء العسكري؛ لأن فيه تعرض لإرادته. نقض قرار رقم 2596 تاريخ 1967/10/31 , أديب استانبولي والمحامي ياسين دركزلي, المجموعة الجزائية لقرارات محكمة النقض السورية, الجزء الأول, القاعدة 226,ص 114.

التحقيق بهذه القضايا إلزامياً أمام قاضي التحقيق ثم أمام قاضي الإحالة. أما محكمة البداية فتختص بالجنح الهامة التي تزيد عقوبتها على الحبس سنة. وتختص محكمة الصلح بالمخالفات والجنح البسيطة التي لا تزيد عقوبتها عن الحبس سنة، وبالجرائم المنصوص عليها على سبيل الحصر في المادة /166/ أصول محاكمات جزائية.

كما يمكن للنائب العام أو المدعي الشخصي في الجنح الهامة أن يقيما الدعوى أمام قاضي التحقيق حسب مقتضيات الحال (المواد 51 و 57 أصول محاكمات جزائية).

أما **الاختصاص المكاني**، فيتحدد في القضاء الجزائي العادي بموجب ثلاثة ضوابط وهي: مكان وقوع الجريمة، أو موطن المدعى عليه، أو مكان إلقاء القبض عليه. أما إذا وقعت جريمة احتيال عبر الإنترنت في الخارج، وكانت تدخل في اختصاص القانون السوري، ولم يكن لمرتكبها محل إقامة في سورية، ولم يلقَ القبض عليه فيها، فتقام دعوى الحق العام عليه أمام المراجع القضائية في العاصمة (المادة 3 من قانون أصول محاكمات جزائية).

## رأي الباحث في مسألة الاختصاص:

بناء على ما تقدم، فإن الباحث لا يجد ما يمنع قانوناً من تطبيق الصلاحيات الإقليمية والذاتية والشخصية والشاملة المنصوص عليها في قانون العقوبات السوري، على جريمة الاحتيال عبر الإنترنت وسائر جرائم الإنترنت الأخرى. فمن الثابت فقهاً أن القواعد الإجرائية الجزائية يمكن أن تفسر تفسيراً واسعاً، إضافةً إلى إمكانية اللجوء إلى القياس أيضاً عند فقدان النص الإجرائي، وذلك بخلاف القواعد الموضوعية .

والعبرة في التفريق بين القاعدة الموضوعية والقاعدة الإجرائية، هو لما تضمنته القاعدة القانونية من تجريم وعقاب، وليست العبرة لورود هذه القاعدة في قانون العقوبات أو في قانون أصول المحاكمات الجزائية[1].

لذلك **فالباحث يقترح** على المشرع السوري في مشروع قانون الجريمة الإلكترونية أن يطبق الصلاحيات المنصوص عليها في قانون العقوبات العام على مختلف الجرائم الإلكترونية، كما هو معمول به في معظم الدول الأخرى، وذلك بإضافة النص التالي إلى مشروع القانون:

(1-تطبق القواعد المتعلقة بالصلاحيات الإقليمية والذاتية والشخصية والشاملة، المنصوص عليها في قانون العقوبات العام على الجرائم الإلكترونية.

2-يعتبر بحكم الأرض السورية النطاق العلوي السوري على الإنترنت المنتهي بـ sy.).

**كما نقترح** عليه أن يرتفع بالعقوبات الجنحية في الجرائم الإلكترونية، إلى الحبس ثلاث سنوات، كي يتجنب الشرط المتعلق بتجريم القانون الأجنبي عند

---

(1) د.حسن الجوخدار: المرجع السابق، الجزء الأول، ص3. د.محمود نجيب حسني: شرح قانون الإجراءات الجنائية,المرجع السابق، المرجع السابق، ص 11 – 12.

تطبيق مبدأ الشخصية. وبهذا يكون المشرع قد عالج مسألة الاختصاص من مختلف جوانبها، دون أن يغادر صغيرة ولا كبيرة إلاّ وأحصاها.

# المبحث الثاني

# التحقيـق

لا يبدأ تحريك الدعوى العامة من الفراغ، بل لا بد أن يبنى على أسباب معقولة أقلها اكتشاف الجريمة ومعرفة فاعلها وجمع أدلتها. فعند اكتمال هذه العناصر، تستطيع النيابة العامة ممارسة سلطتها التقديرية في إقامة الدعوى العامة أو عدم إقامتها. ومن هنا تظهر أهمية أعمال التحري أو الاستدلال، التي تبدأ منذ وقوع الجريمة وتستمر حتى تحريك الدعوى العامة. ويطلق الفقه في سورية على هذه المرحلة تسمية "مرحلة التحقيق الأولي أو التمهيدي"، أما الفقه في مصر وبعض البلدان الأخرى، فيطلق عليها "مرحلة جمع الاستدلالات"[1].

وفي جريمة الاحتيال عبر الإنترنت، وسائر جرائم العالم الافتراضي الأخرى، فإن أهمية هذه المرحلة تبلغ أعلى مستوياتها، لأنها تعد حجر الزاوية الذي سيتم على أساسه بناء الدعوى برمتها، فما يتم جمعه من معلومات وأدلة رقمية في المرحلة التي تعقب ارتكاب الجريمة مباشرة، قد لا يبقى متاحاً بعد مرور وقت قصير على ارتكابها، والسبب في ذلك يعود إلى الطبيعة التقنية لهذه الجرائم.

ففي كثير من قضايا الاحتيال عبر الإنترنت، لم يترك الجاني وراءه سوى ذلك التعبير الذي يعتري وجوه الذين قاموا بتعقبه، وهو تعبير ممزوج بالإحباط والإعجاب معاً، وتقليب الكفين على ما فات.

ولقد دفع تزايد هذه الجرائم المستحدثة معظم الدول إلى إنشاء أجهزة مختصة في مكافحتها على المستوى الوطني والإقليمي والدولي.

---

(1) د.حسن الجوخدار: المرجع السابق، الجزء الثاني، ص3.

وفي سورية فإن الضابطة العدلية هي صاحبة الاختصاص العام في مكافحة جميع الجرائم، وجريمة الاحتيال عبر الإنترنت لا تخرج عن هذا الأصل العام. وللضابطة العدلية مجموعة من الاختصاصات، منها ما تمارسها في الظروف العادية، كاستقصاء الجرائم، وجمع الأدلة، وتلقي الإخبارات والشكاوى، وتنظيم المحاضر والضبوط. ومنها ما تمارسها في الظروف الاستثنائية، حيث تتسع صلاحيات هذه الضابطة، فتقوم بقسط وافر من وظائف قاضي التحقيق، كالقبض على فاعل الجريمة، والتفتيش، وضبط الأشياء الناتجة عن التفتيش. **ولذلك فالباحث** و حرصاً على عدم التكرار لن يتطرق لمرحلة التحقيق الابتدائي، لأننا سنتناول أهم الأعمال التحقيقية ( القبض والتفتيش والضبط ) من خلال دراستنا للسلطات الاستثنائية للضابطة العدلية، ناهيك عن أن التحقيق الابتدائي ليس إلزامياً في الجنح، ومنها جنحة الاحتيال .

وبناءً على ما تقدم فإننا سنقسم هذا المبحث إلى ثلاثة مطالب ، هي:

المطلب الأول: الأجهزة المختصة بمكافحة جرائم الإنترنت.

المطلب الثاني: اختصاصات الضابطة العدلية في مكافحة جرائم الإنترنت في الظروف العادية.

المطلب الثالث: اختصاصات الضابطة العدلية في مكافحة جرائم الإنترنت في الظروف الاستثنائية.

## المطلب الأول

## الأجهزة المختصة بمكافحة جرائم الإنترنت

أمام التزايد المستمر لجرائم الإنترنت، لم تَسلم أجهزة الضبط القضائي من ضرورات التطور التقني والتكنولوجي. ونتيجةً لهذا التحدي قامت معظم الدول بإحداث أجهزة مختصة بمكافحة هذا النوع من الإجرام المستحدث، وقد حملت هذه الأجهزة تسميات مختلفة، منها شرطة الإنترنت، أو درك الإنترنت، أو متحري الإنترنت، وغير ذلك من التسميات.

وتختلف هذه الأجهزة عن الأجهزة المختصة بضبط الجرائم التقليدية من حيث طريقة التكوين، فهي لا تعتمد على التدريبات الجسدية التي يتلقاها عادةً رجال الشرطة، وإنما تعتمد على البناء العلمي والتكنولوجي لأفرادها، وهي تتولي مهمة التحري عن جرائم العالم الافتراضي لكشف النقاب عنها[1]. ولا يقتصر دور هذه الأجهزة على المستوى الوطني، بل هناك أجهزة مختصة على المستوى الدولي والأوربي. لذلك سوف نستعرض أهم هذه الأجهزة.

## أولاً- الأجهزة المختصة بمكافحة جرائم الإنترنت على المستوى الوطني:

ظهرت العديد من الأجهزة المختصة بمكافحة جرائم الإنترنت على المستوى الوطني، سواء على صعيد الدول الأجنبية أم على صعيد الدول العربية. لذلك سنلقي الضوء على هذه الأجهزة الموجودة في هذه الدول.

### أ-الدول الأجنبية:

كانت الدول المتقدمة سباقة بإحداث هذه الأجهزة؛ إذ إن مكافحة جرائم الإنترنت يرتبط بمدى تقدم الدول من الناحية التقنية، وبمدى توفر الإمكانيات المادية اللازمة لإنشاء هذه الأجهزة.

---

(1) نبيلة هبه هروال: المرجع السابق، ص 99- 100.

## 1-الولايات المتحدة الأمريكية:

قامت الولايات المتحدة الأمريكية بإنشاء عدة أجهزة لمكافحة جرائم الإنترنت، ومنها:

- شرطة الوبّ web police، وهي نقطة مراقبة على الإنترنت، إضافةً إلى أنها تقوم بتلقي الشكاوى من مستخدمي الشبكة، وملاحقة الجناة والقراصنة، والبحث عن الأدلة ضدهم وتقديمهم إلى المحاكمة[1].
- مركز تلقي شكاوى جرائم الإنترنت IC3 [2]، الذي تمّ إنشاؤه من قبل مكتب التحقيقات الفيدرالي FBI في أيار عام 2000. وفي كانون الأول من عام 2003 تمّ دمج مركز شكاوى الاحتيال عبر الإنترنت المعروف بـ IFCC[3] مع هذا المركز. ويعمل مركز IC3 بصورة تشاركية مع مكتب التحقيقات الفيدرالي، والمركز الوطني لجرائم الياقات البيضاء NW3C[4].

ويقوم هذا المركز بتلقي الشكاوى عبر موقعه على الإنترنت، حيث يقوم الشاكي بملء استمارة إلكترونية، ثم يقوم المختصون في هذا المركز بتحليل الشكاوى وربطها بالشكاوى الأخرى المستلمة من قبل، ثم يتم إحالة المعلومات الناتجة عن عملية التحليل إلى الجهات المسؤولة عن تطبيق القوانين الأمريكية[5].

---

(1) د.جميل عبد الباقي الصغير: الجوانب الإجرائية للجرائم المتعلقة بالإنترنت, المرجع السابق، ص 77.

(2) وهو اختصار لـ Internet Crime Complaint center، الموقع www.IC3.gov

(3) وهو اختصار لـ Internet Fraud Complaint center، الموقع www.ifcc.gov . Report of IC3 2004 Internet Fraud

(4) وهو اختصار لـ National white collar center، الموقع www.NW3C.org .

(5) Michael Kunz and Patrick Wilson, op-cit- 16.

- قسم جرائم الحاسوب والعدوان على حقوق الملكية الفكرية الذي تمّ تأسيسه في عام 1991، ويختص هذا القسم بالتعريف بهذه الجرائم والكشف عنها وملاحقة مرتكبيها[1].
- نيابة جرائم الحاسوب والاتصالات CTC[2]، وتتألف من مجموعة من قضاة النيابة العامة الذين تلقوا تدريبات مكثفة على نظم المعالجة الآلية للبيانات، وتمّ منحهم صلاحيات واسعة في مجال الاستعانة بغيرهم من خبراء وزارة العدل، لا سيما قسم جرائم الحاسوب والعدوان على حقوق الملكية الفكرية، وهم مرتبطون بنظام تأهيلي وتدريبي مستمر[3].
- المركز الوطني لحماية البنية التحتية، التابع للمباحث الفيدرالية الأمريكية. وقد حدّد هذا المركز البنى التحتية التي تعتبر هدفاً للهجومات والاعتداءات عبر الإنترنت، وعلى رأسها شبكات الاتصالات والمصارف وغيرها.

وإضافةً إلى هذه الأجهزة، يوجد أيضاً في الولايات المتحدة وحدة متخصصة بمكافحة الإجرام المعلوماتي تابعة لقسم العدالة الأمريكي، تتكون من خبراء في نظم الحوسبة والإنترنت، ومن مستشارين قانونيين[4].

## 2-بريطانيا:

قامت السلطات البريطانية بتخصيص وحدة تضم نخبة من رجال الشرطة المتخصصين في البحث والتنقيب عن جرائم الإنترنت، كالجرائم الجنسية الواقعة على الأحداث، والقرصنة ونشر الفيروسات وغيرها.

---

(1) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت,المرجع السابق، ص 812.

(2) وهو اختصار لـ Computer and Telecommunication Coordinator

(3) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت,المرجع السابق، ص 893.

(4) نبيلة هبه هروال: المرجع السابق، ص 108- 109.

وتضم هذه الوحدة نحو /80/ عنصراً على درجة عالية من الكفاءة في المجال التقني. وقد بدأت هذه الوحدة نشاطها عام 2001 ومركزها لندن[1].

## 3-فرنسا:

قامت الحكومة الفرنسية بإنشاء عدة أجهزة لمكافحة جرائم الإنترنت، نذكر منها:

- القسم الوطني لقمع جرائم المساس بالأموال والأشخاص، ويتكون هذا القسم من المحققين المختصين في التحقيق بجرائم العالم الافتراضي، وقد بدأ هذا القسم مهامه عام 1997.
- المكتب المركزي لمكافحة الإجرام المرتبط بتكنولوجيا المعلومات والاتصالات. ويعد هذا المكتب سلاح الدولة الفرنسية في مكافحة جرائم الإنترنت، وقد تمّ إنشاؤه في 2000/5/15.
- تكوين مجموعة من الشرطة والدرك المتخصصين في التحقيق بجرائم الإنترنت[2].

## 4-اسبانيا:

قامت الحكومة الاسبانية بتأسيس وحدة التحريات المركزية المعنية بجرائم الإنترنت، وهي تعمل مع الإدارة المركزية في وزارة الداخلية على مراقبة مرتكبي هذه الجرائم وملاحقتهم[3].

## 5- بعض الدول الآسيوية:

---

(1) نبيلة هبه هروال: المرجع السابق، ص 111.

(2) نبيلة هبه هروال: المرجع السابق، ص 111 وما بعدها.

(3) نبيلة هبه هروال: المرجع السابق، ص 108.

* **هونكونـغ:** قامت بتأسيس ما يعرف بـ "قوة مكافحة قرصنة الإنترنت" وذلك في كانون الأول عام 1999. وتمكّنت هذه القوة من إلقاء القبض على اثني عشر شخصاً في خمسة قضايا خلال مدة ستة أشهر من إنشائها.

* **الصين:** قامت بتأسيس ما يعرف بـ "القوة المضادة للهكرة"، وهي تختص برقابة المعلومات التي يسمح لمواطنيها الدخول إليها عبر الإنترنت[1].

* **فيتنـام:** قامت بتشكيل وحدة خاصة من الشرطة للتحقيق في جرائم الإنترنت، والحد من توزيع المنشورات المحظورة من خلالها[2].

## ب-الدول العربيـة:

لم تقف الدول العربية مكتوفة الأيدي أمام الخطر المتزايد لجرائم الإنترنت، فقد قامت بعض الدول بإنشاء أجهزة متخصصة لمكافحة هذه الجرائم. ومن بين هذه الدول:

### 1- مصر:

قامت جمهورية مصر العربية بتكليف بعض الجهات بمكافحة جرائم الإنترنت، ونذكر منها:

- الإدارة العامة لمباحث الأموال، وتختص هذه الإدارة بمكافحة الجرائم الاقتصادية، سواء كانت تقليدية أو مستحدثة كجرائم الإنترنت.
- الإدارة العامة للتوثيق والمعلومات، وتعتبر هذه الإدارة من أكبر الإدارات بوزارة الداخلية تعاملاً مع جرائم المعلوماتية. وفي عام 2002 تمّ إنشاء

---

(1) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت,المرجع السابق، ص 812.

(2) نبيلة هبه هروال: المرجع السابق، ص 108.

الإدارة العامة لمكافحة جرائم الحاسبات وشبكات المعلومات، وهي تابعة للإدارة العامة للتوثيق والمعلومات. وتتكون هذه الإدارة من ضباط على مستوى عالٍ من التخصص في مجال تكنولوجيا الحاسبات والشبكات، وتختص بمكافحة جرائم الإنترنت على مختلف أنواعها[1].

وإلى جانب هذه الأجهزة الحكومية، فقد تمّ تأسيس "الجمعية المصرية لمكافحة جرائم المعلوماتية والإنترنت"، وهي منظمة غير حكومية خاضعة للقانون المصري، ومشهرة تحت رقم /2176/ لعام 2005، وتهدف إلى تقديم الدعم العلمي للمؤسسات والأفراد، وتنمية الكوادر البشرية في مجال مكافحة الإجرام عبر الإنترنت[2].

## 2- الأردن:

في عام 1988، أنشأت الأردن قسماً خاصاً بجرائم الحاسوب تابعاً لمديرية الأمن، ويتعامل هذا القسم مع مختلف جرائم الحاسوب والإنترنت منذ ذلك العام[3].

وفي عام 2006، تمّ تأسيس جمعية خاصة باسم "الجمعية الأردنية للحد من جرائم المعلوماتية والإنترنت"، مركزها عمان ، وتهدف إلى تقديم الدعم

---

(1) نبيلة هبه هروال: المرجع السابق، ص 141 ومابعدها.

(2) د.عبد الله عبد الكريم عبد الله: المرجع السابق، ص 94 وما بعدها. متوفر على الموقع www.eapiic.net

(3) د.علي حسن محمد الطوالبة: المرجع السابق, ص 94.

العلمي للمؤسسات والأفراد، وتنمية الكوادر البشرية في مجال مكافحة الإجرام عبر الإنترنت[1].

## 3- الجزائر:

قامت الجزائر بإنشاء مركز لمكافحة جرائم الإنترنت على مستوى الدرك الوطني، وقد بدأ مهامه في أواخر عام 2006 [2].

## 4-الإمارات العربية المتحدة:

لم تقم الإمارات بإنشاء جهاز متخصص بمكافحة جرائم الإنترنت وإنما قامت بإحكام الرقابة على شبكة الإنترنت، عن طريق ما يعرف بنظام "الرقيب" Proxy، الذي يقوم بمراجعة الخدمات المقدمة على الشبكة. فعندما يطلب المشترك الدخول إلى موقع ما، تصل الإشارة إلى الرقيب، الذي يقوم بدوره بمراجعة المواقع الممنوعة أو المحظورة، فإذا تبين بأن الموقع المطلوب من هذه المواقع المحظورة، فلا يستطيع المشترك الولوج إليه[3].

## 5- سورية:

لا يوجد في سورية حتى الآن جهاز متخصص بمكافحة جرائم الإنترنت، بيد أن مشروع قانون الجريمة الإلكترونية، نص على إحداث وحدات شرطية متخصصة لمكافحة هذه الجرائم في وزارة الداخلية.

---

(1) د.عبد الله عبد الكريم عبد الله: المرجع السابق، ص 101- 102. متوفر على الموقع www.uaegroup.net

(2) نبيلة هبه هروال: المرجع السابق، ص 145.

(3) د.جميل عبد الباقي الصغير: الجوانب الإجرائية للجرائم المتعلقة بالإنترنت, المرجع السابق، ص 78.

## ثانياً- الأجهزة المختصة بمكافحة جرائم الإنترنت على المستوى الدولي والأوربي:

تتصف جرائم الإنترنت كما ذكرنا بأنها عابرة للحدود، ويمكن أن يتعدى أثرها عدة دول؛ لذلك كان لا بد من وجود تعاون دولي من أجل مكافحة هذا النوع من الإجرام. ومن أساليب التعاون الدولي، التعاون الشرطي الذي يمكن أن يحقق أهدافاً لا قِبلَ للشرطة الإقليمية بتحقيقها. ومن أبرز هذه الأجهزة في مجال مكافحة جرائم الإنترنت:

### 1-المنظمة الدولية للشرطة الجنائية ( الإنتربول):

تعد هذه المنظمة من أهم الأجهزة على المستوى الدولي لمكافحة الإجرام بشكل عام، ومنها جرائم الإنترنت. وهي منظمة تتخذ مقراً لها في مدينة باريس. وتسعى هذه المنظمة لتحقيق التعاون المتبادل بين أجهزة الشرطة في مختلف الدول الأطراف، بهدف مكافحة الجرائم ذات الطابع العالمي، بما في ذلك الإجرام المرتبط بالإنترنت. وتستخدم هذه المنظمة وسيلتين لتحقيق أهدافها:

الأولى: تجميع البيانات والمعلومات المتعلقة بالجريمة والمجرم، عن طريق مكاتب هذه المنظمة الموجودة في أقاليم الدول الأعضاء.

والثانية: التعاون في ملاحقة المجرمين الفارين، وإلقاء القبض عليهم، وتسليمهم إلى الدول التي تطلب تسليمهم.

ولقد أنشأت هذه المنظمة وحدة متخصصة في مكافحة جرائم التكنولوجيا، كما تقوم بتزويد الشرطة في الدول الأطراف بكُتيبات إرشادية حول جرائم الإنترنت، وكيفية التدريب على مكافحتها والتحقيق فيها.

ومن بين إنجازات هذه المنظمة في مجال مكافحة جرائم الإنترنت، العملية التي قامت بها بالتعاون مع المباحث الفيدرالية الأمريكية FBI، والمتعلقة

بملاحقة الهاكر الذي قام بإرسال فيروس الحب Love BUG عبر الإنترنت في الفلبين[1].

وإلى جانب الإنتربول، تقوم منظمة التعاون الاقتصادي والتنمية OECD[2] بمعالجة إشكاليات مواجهة جرائم الإنترنت.

كما قامت مجموعة الدول الثمانية الاقتصادية، وبالتعاون مع بعض المنظمات الدولية، وبعض الدول الأخرى مثل الصين ومصر، بتكوين قوة دولية أطلق عليها DOT FORCE[3]، و تهدف إلى تحقيق الأمن على شبكة الإنترنت[4].

## 2- مركز الشرطة الأوربية أو الأوروبول :

وهو جهاز على مستوى الاتحاد الأوربي، مقره في مدينة "لاهاي" بهولندا. وقد تم إنشاء الأوروبول من قبل المجلس الأوربي في لكسمبورغ عام 1991، ليكون بمثابة حلقة وصل بين الشرطة الوطنية في مختلف الدول الأعضاء، بهدف تسهيل عملية الملاحقة للجرائم العابرة للحدود.

وللأوروبول دور فعال في مكافحة جرائم الإنترنت، حيث يقوم مثلاً بالتحقيقات المتعلقة بامتلاك المواقع الإباحية ونشرها عبر الإنترنت في الدول الأوربية[5].

## 3-الأورجست:

---

(1) نبيلة هبه هروال: المرجع السابق، ص 149 وما بعدها.

(2) وهو اختصار لـ Organization for Economic co-operation and Development

(3) وهو اختصار لـ Digital Opportunity Task Force

(4) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت,المرجع السابق، ص 814.

(5) د.جميل عبد الباقي الصغير: الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، 2002، ص 79. نبيلة هبه هروال: المرجع السابق، ص 158.

وهو جهاز يعمل على المستوى الأوربي إلى جانب الأوروبول في مجال مكافحة جميع أنواع الجرائم، وينعقد اختصاصه عندما تمسّ الجريمة دولتين على الأقل من الدول الأعضاء في الاتحاد الأوربي، أو دولة عضو مع دولة من دول العالم الثالث، أو دولة عضو مع الرابطة الأوربية. ويشمل هذا الاختصاص الأفراد والمؤسسات على حدٍ سواء.

ويعد الأورجست بمثابة الدعامة الفعّالة في مجال التحقيقات والمطاردات التي تقوم بها السلطات القضائية الوطنية، وخصوصاً فيما يتعلق بجرائم الإنترنت[1].

## 4-شنجن:

إلى جانب الأوروبول والأورجست، تمّ إنشاء فضاء جماعي لا حدود له، أُطلق عليه اسم شنجن (Schengen)، وهو اسم مأخوذ من الاتفاقية الموقعة في عام 1985.

وقد استحدثت هذه الاتفاقية وسيلتين جديدتين لتعزيز التعاون الشرطي الأوربي في مواجهة التحديات الجديدة ومنها جرائم الإنترنت، وهاتان الوسيلتان هما: مراقبة المشتبه بهم عبر الحدود، وملاحقة المجرمين[2].

---

(1) نبيلة هبه هروال: المرجع السابق، ص 159.

(2) نبيلة هبه هروال: المرجع السابق، ص 161.

## المطلب الثاني
## اختصاصات الضابطة العدلية
## في مكافحة جرائم الإنترنت في الظروف العادية

يقوم موظفو الضابطة العدلية في سورية في الظروف العادية بمجموعة من الوظائف وهي: استقصاء الجرائم، وجمع الأدلة، وتلقي الإخبارات والشكاوى، وتنظيم المحاضر المتعلقة بهذه الجرائم[1].

ويقصد بالظروف العادية، جميع الأحوال التي يصل فيها إلى علم موظف الضابطة العدلية نبأ وقوع الجريمة، سواء عن طريق الإخبار أو الشكوى. ويخرج عن هذه الأحوال، الظروف الاستثنائية التي تتسع فيها صلاحيات موظفي الضابطة العدلية، كحالة الجرم المشهود، والجناية أو الجنحة الواقعة داخل مسكن، والإنابة.

ويقوم بوظائف الضابطة العدلية في سورية: النائب العام ووكلاؤه ومعاونوه وقضاة التحقيق؛ ويقوم بها أيضاً قضاة الصلح في المراكز التي لا يوجد فيها قضاة نيابة عامة[2].

ويساعد النائب العام في إجراء وظائف الضابطة العدلية المحافظون، ومديرو المناطق، ومديرو النواحي، وقائد قوى الأمن الداخلي[3]، وقادة شرطة المحافظات، ورئيس شعبة الأمن السياسي، ومدير إدارة الأمن الجنائي، وضباط الشرطة، وصف ضباط الشرطة وأفراد الشرطة المكلفون رسمياً برئاسة الأقسام

---

(1) المواد 14 حتى 27 من قانون أصول المحاكمات الجزائية.

(2) المادة 7 من قانون أصول المحاكمات الجزائية.

(3) لم تعد هذه التسمية موجدة من الناحية العملية, إذ إن صلاحيات قائد قوى الأمن الداخلي أصبحت من اختصاص معاون وزير الداخلية.

والمخـافر أو الشّـعب، ومختـارو القـرى وأعضـاء مجالسـها، ورؤسـاء المراكـب البحرية والجوية[1].

ولا بـدّ لنـا هنـا مـن التمييـز بـين الضـابطة الإداريـة والضـابطة العدليـة. فالضابطة الإدارية هي الشرطة أو قوى الأمن الداخلي التي يرأسها المحافظ في المحافظـة، وينحصـر اختصاصـها فـي القيـام بالأعمـال الوقائيـة، أي الأعمـال التي تحول دون وقوع الجريمة، والسهر على حفظ النظام. فإذا وقعت الجريمـة، فإن دور الضابطة الإدارية ينتهي ليبدأ عندها دور الضابطة العدلية[2].

وموظفو الضـابطة العدليـة أصـحاب اختصـاص عـام و شـامل، أي أنهـم يقومون بالوظائف الموكلة إليهم مهما كان نوع الجريمة، مادامت تدخل ضمن اختصاصهم المكاني.

وجريمـة الاحتيـال عبـر الإنترنـت لا تخـرج عـن هـذا الاختصـاص العـام للضـابطة العدليـة، إلاّ أن هنـاك اختلافـاً فـي كيفيـة قيـام الضـابطة العدليـة بوظائفها فـي إطـار جـرائم الإنترنـت، فالتسـاؤلات التـي يمكـن طرحهـا فـي هـذا المجال هي:

- هل تختلف طريقة تقديم الإخبار أو الشكوى في جرائم الإنترنت عن تلك المتّبعة في نطاق الجرائم التقليدية؟

---

(1) المـادة 8 مـن قـانون أصـول المحاكمـات الجزائيـة. القـرار الجمهـوري رقـم /118/ المـؤرخ فـي 1958/3/13، الذي وحّد قوى الدرك والشرطة والأمن العام والبادية تحت تسمية واحدة, وهي هيئة الشرطة، فلم يعد هناك ما يعرف بقوى الدرك أو الأمن العام.

(2) المرسوم التشريعي رقم /77/ لعام 1947 وتعديلاته، المتعلق بالملاك الخاص بالشرطة السورية، حيث قضت المادة الأولى منه بأن قوى الأمن الداخلي تقوم بوظائف الضابطة الإدارية والعدلية والعسكرية، القرار رقم 1962 لعام 1930 المتضمن قانون نظام خدمة الشرطة، حيث حددت المادة /15/ منه وظائف الضابطة الإدارية. د.عبد الوهاب حومد: أصول المحاكمات الجزائية، الطبعة الرابعة (منقحة ومزيدة)، المطبعة الجديدة، دمشق، 1987، ص86.

- ثم كيف تتم عملية استقصاء جرائم الإنترنت وجمع أدلتها؟
- وكيف تتم معاينة مسرح الجريمة في جرائم الإنترنت ؟

## أولاً- الإخبارات والشكاوى:

### أ-الإخبار:

وهو "إجراء يقوم بواسطته شخص لم يتضرر من الجريمة بإبلاغ نَبئها إلى الضابطة العدلية"[1].

والإخبار يمكن أن يقدم من قبل الموظفين ويسمى **الإخبار الرسمي**، أو من قبل الأشخاص العاديين ويسمى **الإخبار العادي**.

وقد أوضحت المادة /27/ من قانون أصول المحاكمات الجزائية **الشكل** الذي يكون عليه الإخبار، فنصت على ما يلي:

(1-يحرر الإخبار صاحبه أومن ينيبه عنه بموجب وكالة خاصة، أو النائب العام إذا طلب إليه ذلك، ويوقع على كل صفحة النائب العام والمخبر أو وكيله.

2-إذا كان المخبر أو وكيله لا يعرف كتابة إمضائه، فيستعاض عن إمضائه ببصمة إصبعه، وإذا تمنع وجبت الإشارة إلى ذلك.

3-تبقى الوكالة مرفقة بورقة الإخبار، وللمخبر إذا شاء أن يستخرج على نفقته الخاصة صورة عن إخباره.).

وتجدر الملاحظة هنا بأن الواقع العملي يشير إلى عدم التقيد التام بأحكام هذه المادة عند تقديم الإخبارات. ففي أغلب الأحوال، يمتنع المخبر في الإخبارات الشفهية عن الإدلاء باسمه الحقيقي، خوفاً من الانتقام، أو خشيةً من أن يلاحق بجرم الافتراء إذا لم يتم إثبات الجريمة. وقد أقرّ الفقه الجزائي هذا

---

(1) د.حسن الجوخدار: المرجع السابق، الجزء الثاني، ص 12.

النوع من التطبيق، فلم يرَ مانعاً من أن تقبل النيابة العامة الإخبارات الشفهية، مادامت هي التي تقرر إقامة الدعوى العامة أو عدم إقامتها[1].

وبناءً على ذلك فالإخبار يمكن أن يكون **مادياً**، كما لو حضر مقدم الإخبار إلى قسم الشرطة للتبليغ؛ كما يمكن أن يكون **معنوياً**، كما لو قام شخص بالإبلاغ عن الجريمة عن طريق الهاتف. كما يصح أن يكون مقدم الإخبار شخصاً مجهول الهوية أو شخصاً معلوم الهوية، فكل ما يشترط في الإخبار هو إعلام السلطات المختصة بوقوع الجريمة.

**ب- الشكوى:**

وهي "إجراء يقوم بواسطته المجني عليه بإبلاغ نبأ وقوع الجريمة عليه إلى السلطة المختصة"[2]. ويمكن أن تقدم الشكوى إلى النيابة العامة، أو قاضي التحقيق، أو إلى أحد موظفي الضابطة العدلية، فيحيلها إلى النيابة العامة.

والأصل أن للنيابة العامة سلطة تقديرية في تحريك الدعوى العامة متى علمت بوقوع الجريمة؛ بيد أن المشرع قيّد هذه السلطة في جرائم محددة، بحيث لا تستطيع النيابة تحريك الدعوى العامة ما لم يتقدم المجني عليه بشكواه.

وعلة لزوم الشكوى في هذه الجرائم هو أن هذه الجرائم بسيطة لا تتعدى حدود الجنح، أو أن الحق الخاص للمعتدى عليه فيها أقوى من الحق العام. وقد رتّب المشرع على تقديم الشكوى في هذه الجرائم عودة السلطة التقديرية إلى النيابة العامة؛ أي أن لها أن تقيم الدعوى العامة أو تحفظ الأوراق. وقد تقترن

---

(1) د.عبد الوهاب حومد :أصول المحاكمات الجزائية,المرجع السابق ,ص143.

(2) د.حسن الجوخدار: المرجع السابق، الجزء الثاني، ص 13.

الشكوى بادعاء شخصي، فعندئذ تُجبر النيابة العامة على تحريك دعوى الحق العام[1].

وقد حدد المشرع على سبيل الحصر الجرائم التي لا يجوز للنيابة العامة تحريك الدعوى العامة فيها إلاّ بعد تقديم شكوى من المجني عليه، ومن هذه الجرائم جميع الجنح المشار إليها في المادة (661) من قانون العقوبات، وهي:

- جرائم الأموال إذا وقعت على الأصول أو الفروع أو الأزواج أو ذوي الولاية الشرعية أو الفعلية (المادة 660 عقوبات).
- جريمة التهويل (المادة 636 عقوبات).
- جريمة استعمال أشياء الغير بدون وجه حق (المادة 637 عقوبات)
- إساءة الائتمان والاختلاس (المادتان 656 و 657 عقوبات).
- كتم اللقطة والأفعال المنصوص عليها بالمادة (659) عقوبات.
- الأفعال التي تجري مجرى الاحتيال، والتي نصت عليها المادة (644) بقولها:

( كل من حمل الغير على تسليمه بضاعة مع حق الخيار أو لوعدة، وهو ينوي عدم دفع ثمنها أو كان يعرف أنه لا يمكنه الدفع، عوقب بالحبس حتى ستة أشهر، وبغرامة حتى مائة ليرة، إذا لم يردها أو لم يدفع ثمنها بعد إنذاره.).

ولابد من الإشارة بأن الإخبار والشكوى يجمع بينهما أن كلاً منهما يتضمن إخطاراً إلى السلطة المختصة بشأن وقوع الجريمة. والفرق بينهما أن الإخبار هو إخطار بالجريمة يقدمه أي شخص، أما الشكوى فهي إخطار بالجريمة

---

(1) د.حسن الجوخدار: المرجع السابق، الجزء الأول، ص 81 وما بعدها. المواد (3 ,51 , 57 , 58) من قانون أصول المحاكمات الجزائية.

يقدمه المجني عليه أو المضرور من الجريمة، وإذا تضمنت الشكوى مطالبة بتعويضات سميت "ادعاءً شخصياً"[1].

## ج- كيفية تقديم الإخبار أو الشكوى عن جرائم الإنترنت:

لا تختلف أحكام الإخبار أو الشكوى في جرائم الإنترنت كثيراً عن ما هو عليه الحال في الجرائم التقليدية. فمن الممكن أن يتم الإخبار عن جرائم الإنترنت **بالأسلوب المادي**، كأن يتوجه مقدم الإخبار بنفسه إلى أقرب قسم للشرطة أو للنيابة العامة للإدلاء ببلاغه. كما يمكن أن يتم الإخبار **بالأسلوب المعنوي** عن طريق الهاتف أو البريد العادي.

وإلى جانب هذين الأسلوبين، ظهر أسلوب ثالث في إطار جرائم الإنترنت، وهو **الأسلوب الرقمي**، حيث أصبح من الممكن تقديم الإخبار أو الشكوى عن طريق الإنترنت بإحدى الطريقتين التاليتين:

**الطريقة الأولى:** وهي كتابة رسالة إلكترونية تتضمن الإبلاغ عن جريمة الإنترنت، وإرسالها إلى عنوان البريد الإلكتروني العائد لأحد الأجهزة المختصة بمكافحة جرائم الإنترنت، كالقيام بكتابة رسالة إلكترونية تتضمن الإخبار عن وجود مواقع إلكترونية أُعدت للاحتيال أو مواقع إباحية مثلاً، وإرسالها إلى عنوان البريد الإلكتروني للجهة المختصة، كموقع المباحث الفيدرالية الأمريكية FBI ، أو موقع إدارة العدل الأمريكية USDJ، أو موقع وكالة المخابرات المركزية الأمريكية CIA، أو موقع هيئة حماية البرمجيات الأوربية APP، أو غيرها من المواقع الأخرى[2].

---

(1) د.محمود نجيب حسني: شرح قانون الإجراءات الجنائية,المرجع السابق، ص 517.

(2) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت,المرجع السابق، ص 825.

**الطريقة الثانية:** وهنا يتم التبليغ عن طريق ملء بيانات الاستمارة الرقمية، التي تكون متوفرة عادةً على المواقع الإلكترونية المخصصة لتلقي الإخبارات والشكاوى، كما هو متبع في المواقع التالية[1]:

- الموقع الإلكتروني لمركز تلقي شكاوى جرائم الإنترنت IC3[2].
- الموقع الإلكتروني لمركز جرائم الياقات البيضاء NW3C[3].
- موقع إدارة مكافحة جرائم الحاسبات وشبكات المعلومات، العائد للحكومة المصرية[4].
- الموقع الإلكتروني العائد للمكتب المركزي لمكافحة الإجرام المرتبط بتكنولوجيا المعلومات والاتصالات في فرنسا. فبعد أن يتم تلقي البلاغات عن طريق هذا الموقع الفرنسي، تتم عملية تحليل ودراسة تلك البلاغات، للتأكد من صحة ما ورد فيها من معلومات حول واقعة الجريمة، ثم يتم إبلاغ مصالح الدرك والشرطة حسب الاختصاص الإقليمي؛ كما يتم إعطاء مقدم الإخبار رقم الاستمارة الرقمية الخاصة به حتى يتمكن من معرفة مستجدات التحقيقات[5].

ولابدّ من الإشارة إلى الدور الهام الذي يلعبه مقدم الإخبار أو الشاكي في إطار جرائم الإنترنت، لأنه في كثير من الأحيان يكون هذا الإخبار هو الوسيلة الوحيدة لعلم السلطات المختصة بوقوع الجريمة.

---

(1) نبيلة هبه هروال: المرجع السابق، ص182.

(2) www.IC3.gov

(3) www.NW3C.org

(4) www.ccd.gov.eg .

(5) نبيلة هبه هروال: المرجع السابق، ص187، وعنوان الموقع الفرنسي هو: www.internet-mineurs.gov

ومما تقدم، نجد أن تقديم الإخبار أو الشكوى عبر الإنترنت يسّهل عملية إعلام السلطات المختصة بوقوع الجريمة، كما يؤمّن الحماية لمقدم الإخبار الذي يظلّ مجهولاً في أغلب الأحيان. **لذلك نقترح** على أجهزة العدالة السورية أن تنشأ مواقع إلكترونية متخصصة في تلقي الإخبارات والشكاوى المتعلقة بجرائم الإنترنت.

## ثانياً- استقصاء الجرائم وإثباتها:

إن **الواجب الأول** الذي يقع على عاتق الضابطة العدلية هو استقصاء الجرائم، أي التحري عنها. فالاستقصاء هو البحث عن جريمة لم يثبت بعد وقوعها فعلاً، إما بناء على شكوى أو إخبار، أو بناء على تكليف من النيابة العامة، أو بناء على معلومات وصلت إلى رجل الضابطة العدلية من أي مصدر كان.

أما **الواجب الثاني**، وهو إثبات الجرائم، فيقصد به جمع الأدلة على وقوع الجريمة، ومعرفة مرتكبها والقبض عليه. والسرعة بجمع الأدلة يساعد على المحافظة على آثار الجريمة، وإحكام الطوق على الجاني[1].

ولرجال الضابطة العدلية في سبيل قيامهم بهذين الواجبين أن يسلكوا كل السبل المجدية لكشف الجريمة؛ فالقانون لم يحدد شكلاً خاصاً لاستقصاء الجرائم وجمع أدلتها، لذلك كان من حقهم أن يستعينوا بكل الوسائل المشروعة للتحري عن الجرائم، دون انتظار توجيه أمر لهم بذلك من رؤسائهم.

ولكن يجب على رجال الضابطة العدلية عدم اللجوء إلى الغش أو الخديعة من أجل الحصول على الأدلة، فلا تثريب عليهم إذا استعملوا بأي وسيلة بارعة لا تتصادم مع الأخلاق، مثل التخفي، وانتحال الصفات،

---

(1) د.عبد الوهاب حومد: أصول المحاكمات الجزائية,المرجع السابق، ص 100.

واصطناع المرشدين. فيمكن لرجل الضابطة العدلية أن يتظاهر بأنه مدمن مخدرات ويرغب في شراء كمية منها ليقبض على المروج. ولكن ليس له أن يخلق الجريمة من العدم، كأن يدفع الفاعل إلى ارتكابها، ثم يلقي القبض عليه، لأنه في ذلك لا يكتشف الجريمة بل يوجدها. والقانون لم ينظم قواعد التحري، لذلك يبقى الأمر اجتهاداً، غير أنه يجب ألاّ يخالف القواعد الدستورية أو القانونية[1].

ومن المؤكد أن قيام رجال الضابطة العدلية بأعمال الاستقصاء وإثبات الجرائم، إنما يهدف إلى مساعدة النيابة العامة على اتخاذ قرارها بتحريك الدعوى العامة أو عدم تحريكها؛ فإذا قامت بتحريكها، وجب عليهم أن يتوقفوا عن العمل من تلقاء أنفسهم، ولا يجوز لهم أن يباشروا أي عمل من أعمال الضابطة العدلية إلاّ إذا كلفهم قاضي التحقيق بذلك بموجب قرار ندب[2].

وإجراءات استقصاء الجرائم تعدّ من الأهمية بمكان، سواء أكانت الجرائم تقليدية أم مستحدثة . وفي إطار جرائم الإنترنت، فإن أبرز وسائل الاستقصاء وجمع الأدلة هي: وسيلة الإرشاد الجنائي، ووسيلة المراقبة الإلكترونية. وهذا ما سنتناوله على التتالي:

## أ-الإرشاد الجنائي عبر الإنترنت:

يعدّ الإرشاد الجنائي من أهم الوسائل التي يمكن أن يعتمد عليها رجال الضابطة العدلية في عملية تحري واستقصاء جرائم الإنترنت.

---

(1)د.عبد الوهاب حومد: أصول المحاكمات الجزائية,المرجع السابق، ص 101-103.

(2) د.عبد الوهاب حومد: أصول المحاكمات الجزائية,المرجع السابق، ص 100.

ويقصد بالإرشاد الجنائي قيام عنصر الضابطة العدلية أو الغير، بالولوج إلى الإنترنت، والدخول في حلقات النقاش والدردشة، مستخدماً اسماً أو صفةً مستعارة أو وهمية، وذلك بقصد البحث عن الجرائم ومرتكبيها، وإلقاء القبض عليهم، وإحالتهم إلى القضاء[1].

والفارق بين نظام الإرشاد الجنائي في الجرائم التقليدية ونظام الإرشاد الجنائي في جرائم الإنترنت، هو أن المرشد أو المخبر في الجرائم التقليدية غالباً ما يكون من الغير، أي ليس من رجال الضابطة العدلية، أما المرشد في جرائم الإنترنت، فمن الممكن أن يكون أحد رجال الضابطة العدلية، إذ إن الأمر لا يتطلب منه سوى الحصول على إذن رسمي من رؤسائه للقيام بهذه المهمة، ثم يلج بواسطة حاسوبه إلى شبكة الإنترنت، حيث يدخل إلى حلقات الدردشة والنقاش مثلاً، مستخدماً اسماً مستعاراً أو صفة وهمية، فيتناول الأحاديث العادية مع الغير، دون أن يدفعه إلى ارتكاب الجريمة، فيظهر وكأنه يسعى لإضاعة الوقت والهروب من الملل، إلى أن يبرز هذا الغير مشروعه الإجرامي، كأن يدور الحديث حول طريقة الحصول على أرقام بطاقات الائتمان بصورة احتيالية، أو كيفية إعداد المواقع الخلاعية، أو المواقع المعدة لبيع المسروقات، أو كيفية اختراق المواقع، أو زرع الفيروسات...الخ. ويمكن للمرشد أيضاً أن يقوم بطرح الأسئلة على الغير، حتى يتمكن من الحصول على أكبر قدر ممكن من المعلومات، وعندما تتضح الصورة كاملةً، يقوم المرشد –إذا كان من الغير– بإيصال هذه المعلومات إلى الجهات المختصة، التي تباشر عملها في تعقب هذا المجرم والقبض عليه، مستخدمة في ذلك برمجيات معينة تقودها إلى مزود خدمة الإنترنت الذي يتحرك فيه هذا المجرم؛ أما إذا كان المرشد أحد رجال الضابطة العدلية، فيقوم باستدراج المجرم حتى يتم القبض عليه[2].

---

(1) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت,المرجع السابق ,ص 838.

(2) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت,المرجع السابق، ص 838– 839.

ومن أمثلة الإرشاد الجنائي، قيام مكتب التحقيقات الفيدرالي FBI، بضبط أفراد عصابة "فاستلان" Fastlan المنتشرين حول العالم، الذين امتهنوا قرصنة البرمجيات وتحميلها على مواقع للهكرة، وجنوا أرباحاً وصلت إلى مليون دولار في فترة زمنية قصيرة، حيث تم إلقاء القبض على تسعة منهم في الولايات المتحدة الأمريكية، وتمّت إدانتهم أمام هيئة المحلفين العليا في شيكاغو. وقد استعملت المباحث الفيدرالية في هذه القضية أسلوب الإرشاد الجنائي، عندما دسّت أحد عناصرها في هذه العصابة إلى أن تمّ إلقاء القبض عليهم[1].

وفي مثال آخر، فقد قام المدعو Roots أثناء وجوده في إحدى حلقات الدردشة عبر الإنترنت بالتحدث مع فتاة لم تتجاوز الرابعة عشرة من عمرها في موضوعات جنسية؛ وتناول الحديث عرضه لها ممارسة الأفعال الجنسية معها، وتمّ تحديد موعد اللقاء بينهما في أحد المتاجر؛ وعندما وصل تمّ القبض عليه، إذ تبين أن الفتاة الصغيرة لم تكن سوى أحد أعضاء فريق مكافحة الجريمة عبر الإنترنت، في حالة تنكر بهيئة فتاة صغيرة بتكليف من الإدارة التي تعمل فيها[2].

والحقيقة أن نظام الإرشاد الجنائي عبر الإنترنت هو من أهم وسائل تحري واستقصاء جرائم الإنترنت ومنها الاحتيال، وهو نظام لا بدّ من الأخذ به في جميع الدول التي تسعى للحدّ من هذه الجرائم.

## ب-المراقبة الإلكترونية Electronic Surveillance:

(1) د.سليمان أحمد فضل: المرجع السابق، ص 275.

(2) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت,المرجع السابق، ص276.

يقصد بالمراقبة الإلكترونية "ذلك العمل الذي يقوم به المراقب، باستخدام التقنية الإلكترونية، لجمع المعلومات عن المشتبه به، سواء أكان شخصاً أم مكاناً أم شيئاً، وذلك لتحقيق غرض أمني" [1].

فالمشتبه به الإلكتروني يمكن أن يكون شخصاً، أو موقعاً، أو بريداً إلكترونياً مخالفاً للقانون. وتشمل المراقبة الإلكترونية جميع تحركات المشتبه به عبر الإنترنت، بما في ذلك بريده الإلكتروني.

ويشترط في المراقبة الإلكترونية أن تكون مشروعة. والغرض من هذه المشروعية هو تحقيق نوع من التوازن بين حق الأفراد في الخصوصية، وحق المجتمع في مكافحة الجريمة بوسائل فعّالة، حفاظاً على أمنه. وعلى ذلك فيمكن لرجل الضابطة العدلية أن يقوم طبقاً للقانون بمراقبة أحد الهكرة أثناء اختراقه لحاسوب المجني عليه، أو أن يراقب أحد المواقع التي أُعدت للاحتيال على الناس...الخ.

ومن الملاحظ أن معظم الدول أخذت بنظام المراقبة الإلكترونية ضمن شروط معينة، بهدف رصد الجرائم المستحدثة، ومنها جريمة الاحتيال عبر الإنترنت.

**ففي الولايات المتحدة الأمريكية**، نظّم قانون خصوصية الاتصالات الإلكترونية ECPA[2] كيفية حصول أجهزة العدالة على المعلومات المخزنة في مُخدّمات مزودي خدمة الإنترنت، فأعطى الحق لرجل الضبط القضائي في الحصول على المعلومات الأساسية للمشترك (كالاسم والعنوان وغيرها)، أو

---

(1) د.مصطفى محمد موسى: المراقبة الإلكترونية عبر شبكة الإنترنت (دراسة مقارنة)، سلسلة اللواء الأمنية في مكافحة الجريمة الإلكترونية، العدد الخامس، مطابع الشرطة للطباعة والنشر والتوزيع، القاهرة،2003, ص192.

(2) وهو اختصار لـ The Electronic Communication Privacy Act وقد تمّ تعديله بموجب القانون الوطني الأمريكي 2001 Patriot Act، ومتوفر على الموقع: www.wikipedia.org

المعلومات المتعلقة ببريده الإلكتروني أو بريده الصوتي ، بمجرد توجيه أمر من المحكمة إلى مزود خدمة الإنترنت تأمره فيه بالكشف عن محتويات الحساب[1].

وبعد أحداث 11 أيلول عام 2001، منحت حكومة الرئيس جورج بوش، مكتب التحقيقات الفيدرالي FBI سلطات وصلاحيات إضافية لمراقبة الأشخاص والمنظمات السياسية والدينية وأماكن العبادة ومواقعها على الإنترنت، دون أن يكون هناك دليل على أن جريمة ما ارتكبت أو سترتكب، كل ذلك بهدف تسهيل مهمة مكتب التحقيقات الفيدرالي في مكافحة ومنع الإرهاب[2].

كما نظم قانون المراقبة المعرُف بـ The Wiretap Statue[3] كيفية المراقبة الإلكترونية لمحتويات الاتصالات في الزمن الذي يتم فيه بثّ هذه الاتصالات، حيث يمكن بموجب هذا القانون مراقبة اتصالات الإنترنت، بما في ذلك مراسلات البريد الإلكتروني خلال فترة بثها بين أطراف الاتصال، ولا يشمل ذلك الحصول على المعلومات الإلكترونية المخزنة أو المسجلة. فتعبير المراقبة وفق هذا القانون ينصرف فقط إلى الاتصالات التي يتم التقاطها أثناء عملية البث[4].

---

(1) د.عمر بن يونس: الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي,المرجع السابق، ص 271 .

(2) د.مصطفى محمد موسى: المرجع السابق، ص 202.

(3) يُعرف هذا القانون أيضاً باسم 18 used sec.2510-22 أو باسم الباب الثالث (Title III) وقد صدر في عام 1968، وتمّ تعديله عام 1986، ومتوفر على الموقع www.wikipedia.org.

(4) د.عمر بن يونس: الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي, المرجع السابق، ص 366 وحتى 368.

ALBERT .J . Marcella , Robert .s. Green Field, Cyber Forensics, Field Manual for collecting Examining and Preserving Evidence of computer crimes, published by CRC Press, 2002, P-119 .

ويحظر هذا القانون المراقبة الإلكترونية، إلا إذا توفرت إحدى الحالات التالية[1]:

- الحصول على أمر من المحكمة.
- موافقة أحد أطراف الاتصال.
- الاستثناء المقرر لمزودي الخدمة، وذلك بغية مراقبة الاتصالات بهدف حماية حقوق مزودي الخدمة.
- استثناء منتهك الحاسوب، إذ يسمح هذا القانون لضحايا الهجوم على الحاسوب بمراقبة الاتصالات الإلكترونية للمعتدي.
- استثناء الهاتف الامتدادي، وهو استثناء مقرر لربّ العمل لمراقبة اتصالات الموظفين لديه، لأجل هدف مشروع مرتبط بالعمل.
- استثناء الحصول على دليل جنائي.
- استثناء المألوف للجمهور، ويقصد به مراقبة غرف المحادثة المعدة للجمهور، أو المجموعات الإخبارية.

**أما الاتفاقية الأوربية حول الجريمة الافتراضية لعام 2001**، فقد سمحت المادتان /20/ و /21/ منها بمراقبة حركة البيانات ومحتواها أثناء عملية التراسل[2].

**وفي فرنسا**، أصدر المشرع الفرنسي القانون المؤرخ في 2000/8/1، الذي عدّل قانون حرية الاتصالات المؤرخ في 1986/9/30، حيث سمح بمقتضى هذا التعديل لمزودي الخدمات بمراقبة حركة أعضاء الإنترنت[3].

---

(1) د.عمر بن يونس: الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي, المرجع السابق، ص 271 وما بعدها.

(2) د.عمر بن يونس: الاتفاقية الأوربية حول الجريمة الافتراضية، المرجع السابق ص161.

**وفـي هولنـدا**، يجـوز لقاضـي التحقيـق أن يـأمر بالتنصـت علـى شـبكات الاتصالات الحاسوبية، إذا كانت هناك جرائم خطيرة ارتكبها المتهم[1].

والسؤال المطـروح هنـا هـو: **مـا هـي التقنيـة المسـتخدمة فـي المراقبـة الإلكترونية؟**

تعددت التقنيات المستخدمة في مجال المراقبة الإلكترونية، فهناك برامج مخصصة لفحص الرسائل الإلكترونية الصادرة والواردة، وبرامج تقوم باستعادة الرسائل التي تمّ إلغاؤها أو محوها، وأخرى تقوم بتعقب المواقع الإباحية، وغير ذلك من هذه البرمجيات. وسنتناول فيما يلي أبرز أنواع هذه البرمجيات:

**1-تقنية برنامج "كارنيفور" للتنصت على البريد الإلكتروني:**

طـورت إدارة تكنولوجيـا المعلومـات التابعـة لمكتـب التحقيقـات الفيـدرالي FBI، برنـامج أطلـق عليـه اسـم "كـارنيفور"، حيـث يقـوم هـذا البرنـامج بتعقـب وفحص رسائل البريد الإلكتروني الصادرة والواردة عبر المخدمات المستخدمة من قبل مزودي خدمة الإنترنت، إذا كان هناك اشتباه بأن هذه الرسائل تحمل معلومات عن جرائم أو حوادث جرمية. فهذا البرنامج يقوم بفحص وتسجيل الرسائل التي تحتوي كلمات أو معلومات يشتبه في أن لها علاقة بالجرائم، ويتجاهل الرسائل الأخرى[2].

**2-برامج استعادة الوثائق الإلكترونية الممحاة:**

في عام 1988، أسس الأمريكي "جون جيسين" شركة تدعى "اكتشاف الأدلة أو القرائن الإلكترونية". وقد اتجهت هذه الشركة لتسهيل عملها في البحث

---

(3) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت,المرجع السابق، ص 202.

(1) د.علي حسن محمد الطوالبة: المرجع السابق، ص 150.

(2) د.مصطفى محمد موسى: دليل التحري عبر شبكة الإنترنت، دار الكتب القانونية، القاهرة، ص 189.

والتحري نحو الوثائق الإلكترونية، باعتبار أن هذه الوثائق تترك وراءها أثراً لاُ يمحى، ويمكن استعادتها مهما اجتهد الفاعل في محوها، وذلك على عكس الوثائق الورقية التي تتحول إلى مادة يصعب استرجاع المعلومات منها بعد حرقها أو تمزيقها.

وقد طورت هذه الشركة العديد من برامج البحث في ذاكرة الحاسوب عن الرسائل الممحاة والمعلومات المصاحبة لها، والتي لا يراها متلقو الرسائل في معظم الأحيان. وهذه المعلومات تشمل الطريق الذي سلكته الرسالة والمرفقات التي أُرسلت معها، وأجهزة الحاسوب التي مرت بها. فهذا البرنامج يخرج الحي من الميت، ويخرج الميت من الحي .

ومن أشهر القضايا الذي اعتمدت على هذا الأسلوب، القضية التي رفعتها وزارة العدل الأمريكية وتسع عشرة ولاية ضد شركة مايكروسوفت، لمحاولتها احتكار أنظمة تصفح الإنترنت. فبعد البحث في نظام البريد الإلكتروني العائد لهذه الشركة، تم اكتشاف رسائل إلكترونية تتعلق بمحاولة الإضرار بالمنافسين التجاريين، التي اعتقد أصحابها أنهم قاموا بمحوها. ومن أشهر الرسائل الممحاة التي استخدمت في هذه القضية، الرسالة التي سأل فيها رئيس مايكروسوفت عدداً من كبار الموظفين في شركته عمّا إذا كان لديهم خطة تتعلق بما يمكن فعله من أجل إلحاق الضرر بالخصوم التجاريين[1].

**3-برنامج مراقبة البريد الإلكتروني:**

وهو برنامج صمّمه المبرمج الأمريكي "ريتشارد إتوني"، حيث يقوم هذا البرنامج بسبر محتوى البريد الإلكتروني موضوع المراقبة، وقراءة الرسائل التي قام صاحبها بإتلافها، أو تلك التي لم يقم بتخزينها أصلاً، ويمكن تحميل هذا البرنامج على أي جهاز حاسوب بهدف مراقبة بريده الإلكتروني. وقد استخدمت

(1) د.مصطفى محمد موسى: دليل التحري عبر شبكة الإنترنت، المرجع السابق ص 193-194.

المخابرات الأمريكية هذا البرنامج لكشف مشتبه به من الجنسية الروسية حاول اختراق بعض المواقع على شبكة الإنترنت[1].

**4-برنامج تعقب المواقع الإباحية:**

ويعرف هذا البرنامج باسم "نوبد شرطة الإنترنت" وهو يقوم بالبحث عن الصور الجنسية المخلّة بالأخلاق في أنظمة الحواسيب التي تعمل وفق برنامج تشغيل ويندوز بإصداراته الحديثة، ثم يقوم بتبليغ الهيئات الحكومية عنها، بهدف تطهير شبكة الإنترنت من هذه المواقع والصور[2].

ومن الأمثلة الشهيرة للمراقبة الإلكترونية، أنه تمّ الكشف عن العلاقة الغرامية بين الرئيس الأمريكي السابق "كلينتون" والآنسة "مونيكا لوينسكي"، عن طريق مراقبة البريد الإلكتروني لهما[3].

**رأي الباحث في مدى إمكانية القيام بالمراقبة الإلكترونية في ظل التشريع السوري:**

نصت المادة /96/ من قانون أصول المحاكمات الجزائية على ما يلي:

( لقاضي التحقيق أن يضبط لدى مكاتب البريد، كافة الخطابات والرسائل والجرائد والمطبوعات والطرود، ولدى مكاتب البرق كافة الرسائل البرقية، كما يجوز له مراقبة المحادثات الهاتفية، متى كان لذلك فائدة في ظهور الحقيقة ).

والحقيقة أن **الباحث لا يرى** ما يمنع قانوناً من تطبيق هذه المادة على المراقبة الإلكترونية عبر الإنترنت، للأسباب التالية:

---

(1) د.مصطفى محمد موسى: المراقبة الإلكترونية عبر شبكة الإنترنت، المرجع السابق ص216.

(2) د.مصطفى محمد موسى: المراقبة الإلكترونية عبر شبكة الإنترنت، المرجع السابق ص217.

(3) Eoghan Casey, op-cit, P-41.

1- يقرّ الفقه الإجرائي بإمكانية التوسع في تفسير القوانين الأصولية، فيجيز اللجوء إلى القياس أو الاستنتاج، أو قاعدة من باب أولى، وذلك على خلاف قواعد التفسير في النصوص الجزائية الموضوعية؛ ومن ثم فعلى القاضي أن يقوم بكل إجراء غير ممنوع في القانون ليصل إلى الحقيقة التي تسعى العدالة إليها[1].

وإذا كانت العلة من قيام قاضي التحقيق بضبط الرسائل والخطابات والرسائل البرقية والمحادثات الهاتفية تكمن في إظهار الحقيقة، فإن هذه العلة متوفرة أيضاً في المراقبة الإلكترونية، بما في ذلك مراقبة البريد الإلكتروني. وبالتالي فيمكن قياس المراقبة الإلكترونية على مراقبة الرسائل والخطابات والمحادثات الهاتفية، لاتحادهما في العلة، وهي إظهار الحقيقة. ناهيك عن أن كلمة "الخطابات" الواردة في هذا النص جاءت عامة دون قيد، فهي تشمل مختلف أنواع الخطابات، سواء كانت ورقية أم إلكترونية كالبريد الإلكتروني.

2- إن التطور التاريخي لشبكة الإنترنت يشير إلى أن هذه الشبكة قد استخدمت خطوط الهاتف في عملية الاتصال. فمثلاً في حالة الاتصال السلكي بشبكة الإنترنت، يقوم معدل الموجات "المودم"[2]، بتحويل الإشارة الرقمية المستخدمة في الحاسوب إلى إشارة كهربائية تنتقل عبر خطوط الهاتف. الأمر الذي يشير إلى مدى التشابه بين مراقبة المحادثات الهاتفية والمراقبة الإلكترونية من الناحية التقنية.

وبناءً على ما تقدم، فإنه يمكن لموظف الضابطة العدلية القيام بالمراقبة الإلكترونية في ظل التشريع السوري، بعد أن يحصل على إنابة من قبل قاضي التحقيق المختص.

---

(1) د.عبد الوهاب حومد: أصول المحاكمات الجزائية,المرجع السابق، ص 764-765.

(2) المودم Modem، وهو اختصار لـ Modulator Demodulator .

و**يقترح الباحث** على المشرع السوري أن يسمح بالمراقبة الإلكترونية من قبل موظفي الضابطة العدلية في مشروع قانون الجرائم الإلكترونية، بشرط الحصول على إنابة من قبل قاضي التحقيق المختص، أو بناءً على إذن من النيابة العامة، حتى يتمكن هؤلاء الموظفون من القيام بالمراقبة الإلكترونية على وجه السرعة، تماشياً مع طبيعة جرائم الإنترنت.

## ثالثاً- المعاينة:

هي "الكشف الحسي المباشر لإثبات حالة شيء أو شخص". وتتم المعاينة إما بانتقال موظف الضابطة العدلية إلى مكان الجريمة، أو بجلب موضوعها لمعاينته في مقره، كما هو الحال في معاينة العملات المزوّرة أو الأسلحة وغير ذلك[1].

والمعاينة إجراء يمكن لموظفي الضابطة العدلية القيام به، سواء كان الجرم مشهوداً أم لا، كما يمكن لقاضي التحقيق القيام به متى دخلت الدعوى العامة في حوزته، وللمحكمة أيضاً القيام بالمعاينة متى رأت ضرورة لذلك[2].

وتكمن أهمية المعاينة في الجرائم التقليدية بأنها تتيح لموظف الضابطة العدلية جمع الأدلة قبل أن تمتد إليها يد العبث والتشويه، كما تتيح له اتخاذ إجراءات فورية، لم يكن يتاح له القيام بها ما لم ينتقل إلى مكان الجريمة فوراً، كسماع الشهود الحاضرين ومواجهة بعضهم ببعض، وغير ذلك من الإجراءات[3].

والمعاينة لا تصلح لضبط أدلة جميع الجرائم، فهناك جرائم لا تصلح بطبيعتها لأن تكون محلاً للمعاينة، مثل جريمة الذم والقدح، والرشوة، وترك

---

(1) د.حسن الجوخدار: المرجع السابق، الجزء الثاني، ص 145.

(2) د.حسن الجوخدار: المرجع السابق، الجزء الثاني، ص 145-146.

(3) د.محمود نجيب حسني: شرح قانون الإجراءات الجنائية,المرجع السابق، ص 640.

العمل، وغير ذلك من الجرائم، باعتبار أن المعاينة غير مجدية في هذه الجرائم[1].

## أ-أهمية المعاينة في جريمة الاحتيال عبر الإنترنت:

لا تتمتع المعاينة في جريمة الاحتيال عبر الإنترنت بذات الأهمية التي لها في معظم الجرائم التقليدية، وذلك للأسباب التالية:

- قلة الآثار المادية التي تخلّفها وراءها جريمة الاحتيال عبر الإنترنت.
- التغيرات التي يمكن أن تطرأ على مسرح الجريمة، نتيجة تردد عدد من الأشخاص إلى هذا المسرح في الفترة الفاصلة بين اقتراف الجريمة والكشف عنها ومعاينتها.
- إمكانية التلاعب بالبيانات عن بعد من قبل الجاني، وذلك عن طريق المحو أو التحريف مثلاً[2].

## ب-كيفية الانتقال إلى العالم الافتراضي:

يستطيع موظف الضابطة العدلية الانتقال إلى مسرح الجريمة في العالم الافتراضي، عن طريق الحاسوب الموجود في مكتبه، أو عبر مقهى الإنترنت. كما يمكن أن يلجأ إلى مقر مزود الخدمة، الذي يعد أفضل الأماكن لإجراء المعاينة. وله في جميع هذه الحالات أن يستعين بخبير مختص في هذا المجال[3].

وتختلف الوسائل المستعملة في معاينة جرائم الإنترنت بحسب نوع الجريمة، غير أن هناك وسائل تتفق مع معظم جرائم الإنترنت، ومنها تصوير

---

(1) عفيفي كامل عفيفي: المرجع السابق، ص 354.

(2) نبيلة هبه هروال: المرجع السابق، ص 217. : المستشار الدكتور عبد الفتاح بيومي حجازي: مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر، المحلة الكبرى، 2007، ص 315.

(2) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت,المرجع السابق، ص 895.

شاشة الحاسوب بواسطة آلة تصوير تقليدية[1]، أو استخدام برمجية خاصة تقوم بحفظ ما يظهر على شاشة الحاسوب، وهو ما يعرف بمصطلح تجميد الشاشة "frozen" أو عن طريق حفظ موقع الإنترنت باستخدام تعليمة الحفظ "save as" المتوفرة في نظام التشغيل.

وتماشياً مع متطلبات السرعة في معاينة مسرح الجريمة الافتراضية، أجاز القانون الأمريكي 18 uscode see 2703 لعضو النيابة المعلوماتية CTC أن يرسل رسالة إلى مزود خدمة الإنترنت يلزمه فيها بالتحفظ على السجلات المطلوبة، إلى حين صدور أمر من المحكمة باتخاذ هذا الإجراء أو غيره[2].

وبناءً على ما تقدم، فإنه يمكن لموظف الضابطة العدلية القيام بمعاينة مسرح الجريمة الافتراضية في **ظل التشريع السوري**، كأن يقوم مثلاً بمعاينة الموقع الإلكتروني المستخدم في الاحتيال عبر الإنترنت، ثم يقوم بتجميد الشاشة أو تصويرها للمحافظة على صفحة الوبّ المتعلقة بهذا الموقع، من أجل تقديمها للقضاء في وقت لاحق.

---

(1) د.جميل عبد الباقي الصغير: الجوانب الإجرائية للجرائم المتعلقة بالإنترنت, المرجع السابق، ص28.

(2) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت,المرجع السابق، ص 895-896.

## المطلب الثالث

## اختصاصات الضابطة العدلية

## في مكافحة جرائم الإنترنت في الظروف الاستثنائية

ليس لموظف الضابطة العدلية في الأصل سوى القيام بأعمال التحقيق الأولي، إلاّ أن المشرع خرج عن هذا الأصل في بعض الحالات الاستثنائية، وأعطى موظفي الضابطة العدلية بعض الصلاحيات التي هي من اختصاص قاضي التحقيق.

وقد حدد المشرع الحالات التي يجوز فيها للضابطة العدلية القيام بهذه الصلاحيات الاستثنائية على وجه الحصر، وهي:

1- الجرم المشهود[1].

2- الجناية أو الجنحة الواقعة داخل منزل، عندما يطلب صاحب المنزل من النائب العام إجراء تحقيق بشأنها[2].

3- إنابة موظفي الضابطة العدلية ببعض إجراءات التحقيق من قبل السلطة المختصة[3].

والصلاحيات الاستثنائية التي أجازها القانون هي: الانتقال إلى موقع الجناية المشهودة، ومنع الحاضرين من الابتعاد، والقبض على فاعل الجريمة، وتفتيش المنازل، وضبط الأشياء الناتجة عن التفتيش [4].

---

(1) المواد / 28 و 29 و 231 وحتى 237 /من قانون أصول المحاكمات الجزائية.

(2) المادة /42/ من قانون أصول المحاكمات الجزائية.

(3) المواد / 48 و 85 و 86 و 87 و 101/ من قانون أصول المحاكمات الجزائية.

(4) المواد /29 حتى 41 و231 حتى237/ من قانون أصول المحاكمات الجزائية.

ويقصد بالجرم المشهود الحالات الأربعة التي نصت عليهم المادة /28/ من قانون أصول المحاكمات الجزائية، وهي:

1- الجرم الذي يشاهد حال ارتكابه.

2- الجرم الذي يشاهد عند الانتهاء من ارتكابه.

3- حالة القبض على مرتكب الجريمة بناء على صراخ الناس.

4- حالة ضبط مرتكب الجريمة، ومعه أشياء أو أسلحة أو أوراق، يستدل منها على أنه فاعل الجريمة ، وذلك في الأربع والعشرين ساعة من وقوع الجريمة.

ويشترط أن تكون مشاهدة هذه الحالات من قبل موظف الضابطة العدلية بالذات. وتثبت المشاهدة بكل الحواس، فالأذن تسمع الشتيمة وإطلاق الرصاص، والعين ترى الواقعة، والأنف يشم رائحة المخدرات، والذوق يكشف المواد الكحولية.

ولا يجوز إثبات الجرم المشهود بطرق غير مشروعة، كالنظر من خصاص الباب، أو من أسطح الجيران... كما لا يجوز التحريض على ارتكاب الجريمة لضبطها، لأن مهمة رجل الضابطة العدلية تنحصر في كشف الجريمة وليس خلقها من العدم[1].

ومن الملاحظ أن الحالة الأولى فقط من حالات الجرم المشهود هي الحالة الحقيقية له، أما الحالات الثلاث الأخرى، فهي كما يسميها الفقه حالات اعتبارية للجرم المشهود، لأن المشاهدة فيها لا تنصبّ على الجريمة حال

(1) د.عبد الوهاب حومد: أصول المحاكمات الجزائية,المرجع السابق، ص 110.

وقوعها، بل على آثارها الباقية بعد فترة وجيزة. وغني عن البيان أن هذه الحالات لا يجوز القياس عليها، لأنها وردت على سبيل الحصر[1].

وعلة التوسع في اختصاصات الضابطة العدلية في هذه الحالات هي أن أدلة الجريمة تكون واضحة وناطقة بحد ذاتها، فيتعين فحصها وضبطها على الفور، لأنه يخشى إذا تراخت الإجراءات أن تضعف هذه الأدلة، أو أن تمتد إليها يد التشويه، إضافةً إلى أن وضوح الأدلة هنا لا يحتمل التعسف أو الخطأ[2].

والمشرع فرّق في نطاق الجرم المشهود بين الجناية المشهودة والجنحة المشهودة؛ فالأولى تعطي الحق لموظف الضابطة العدلية بالقبض على المشتبه به، وتفتيشه وتفتيش مسكنه، دون تفتيش مسكن غيره، أما الثانية –وهي الجنحة المشهودة– فيقتصر حق موظف الضابطة العدلية فيها على القبض على المشتبه به وتفتيشه، دون الحق بتفتيش منزله[3]. ولكن إذا كانت الجريمة مشهودة ولم تتبين طبيعتها في الحال، أي لم يتأكد موظف الضابطة العدلية من أنها جناية أو جنحة (كالسرقة مثلاً)، فإنه يحق له مباشرة الإجراءات الخاصة بالجناية، حتى لو تبيّن فيما بعد أن الجريمة جنحية الوصف[4].

ومثال الجرم المشهود في جريمة الاحتيال عبر الإنترنت أن يكون موظف الضابطة العدلية في أحد مقاهي الإنترنت يتصفح بريده الإلكتروني، فيشاهد شخصاً آخر في المقهى يقوم باختراق النظام المعلوماتي لأحد المصارف، بهدف إجراء تحويلات غير مشروعة للأموال. ففي هذه الحالة تنعقد لموظف

---

(1) د.حسن الجوخدار: المرجع السابق، الجزء الثاني، ص 22 –23.

(2) د.محمود نجيب حسني: شرح قانون الإجراءات الجنائية,المرجع السابق، ص 533.

(3) المواد من 28 وحتى 41 ومن 231 وحتى 237 من قانون أصول المحاكمات الجزائية.

(4) د.عبد الوهاب حومد: أصول المحاكمات الجزائية,المرجع السابق، ص 112.

الضابطة العدلية جملة الاختصاصات الاستثنائية المترتبة على الجرم المشهود، لأن الموظف شاهد الجرم حال ارتكابه.

ومثال على الجنايات أو الجنح الواقعة داخل المنزل، أن يلاحظ أحد الآباء أن ابنه يقوم بإدارة موقع إلكتروني للاحتيال التجاري، وذلك عن طريق الحاسوب الموجود في المنزل، فيطلب الأب من النائب العام إجراء تحقيق بشأن هذه الواقعة.

أما الإنابة، فيقصد بها ذلك الصك الذي ينقل بموجبه القاضي المختص، صلاحياته إلى قاض آخر أو إلى ضابط عدلي؛ ليقوم مقامه بإجراء عمل تحقيقي يتعذر عليه أن يقوم به شخصياً[1]. وللإنابة فائدة عملية تكمن في التخفيف من أعباء القاضي، كالإنابة في سماع شاهد، أو إجراء خبرة، وغير ذلك. ولا يجوز أن تكون الإنابة عامة، أي أن تنيب سلطة التحقيق موظف الضابطة العدلية بكامل التحقيق؛ لأن في ذلك تنازلاً من المحقق عن كامل سلطته المقررة بالقانون، بل يجب أن تكون الإنابة خاصة بعمل أو أكثر من أعمال التحقيق، ما عدا استجواب المدعى عليه.

وبناءً على ذلك ، فقاضي التحقيق يستطيع أن ينيب موظف الضابطة العدلية بتفتيش جميع البرامج والمعلومات الموجودة على حاسوب المشتبه به، وضبط ما كان متعلقاً منها بالجريمة .

ومن الجدير بالذكر أننا سنقتصر في دراسة الصلاحيات الاستثنائية للضابطة العدلية على القبض والتفتيش والضبط، نظراً لما تطرحه هذه الصلاحيات من إشكاليات في ظل جريمة الاحتيال عبر الإنترنت.

## أولاً- القبض:

(1) د.عبد الوهاب حومد: أصول المحاكمات الجزائية,المرجع السابق، ص 748.

القبض هو" إمساك الشخص من جسمه، وتقييد حركته وحرمانه من حق التجول، دون أن يتعلق الأمر على فترة زمنية معينة ." [1]

والقبض بطبيعته إجراء ماس بالحرية الشخصية، التي هي حق أساسي للإنسان، ولذلك حرص الدستور على حمايتها، وفصّل القانون في ضوابط هذه الحماية[2]. فالفقرة الثانية من المادة 28 من دستور الجمهورية العربية السورية لعام 1973 نصت على ما يلي : ( لا يجوز تحري أحد أو توقيفه إلا وفقاً للقانون.).

أما قانون أصول المحاكمات الجزائية فلم يجز القبض على أحد إلا في حالتين فقط ، هما[3] :

1- الجرم المشهود ( جناية مشهودة أو جنحة مشهودة ).

2- وجود أمر من قاضي التحقيق، في حالات الجنايات والجنح غير المشهودة .

وفي إطار جريمة الاحتيال عبر الإنترنت، فالسؤال الذي يطرح نفسه هنا هو: **كيف يتم تعقب المشتبه به في جريمة الاحتيال عبر الإنترنت أو في مختلف جرائم الإنترنت ؟ بمعنى أخر، كيف يتم القبض على مجرم الإنترنت؟**

للإجابة عن هذا السؤال سنلقي الضوء على آلية تعقب المشتبه به في جرائم الإنترنت، ثم نتعرض لأشهر الشركات التي تقوم بعملية التتبع، ومن ثم معرفة كيفية تتبع البريد الإلكتروني المزيف .

## أ- آلية تعقب المشتبه به في جرائم الإنترنت:

---

(1) د.عبد الوهاب حومد: أصول المحاكمات الجزائية,المرجع السابق، ص 125.

(2) د.محمود نجيب حسني: شرح قانون الإجراءات الجنائية,المرجع السابق، ص 556.

(3) المواد 29 و112 و231 و102 حتى 116 من قانون أصول المحاكمات الجزائية . د.عبد الوهاب حومد: أصول المحاكمات الجزائية,المرجع السابق، ص 123.

تتيح البنية التحتية للإنترنت إمكانية التعرف على عنوان الحاسوب المستخدم في ارتكاب الجريمة فقط، وهو ما يعرف بعنوان Internet (IP) Protocol ، الذي يشير إلى رقم يتم بموجبه تحديد الحاسوب الذي تمّ النفاذ من خلاله إلى الإنترنت. وبعد تحديد هوية الحاسوب المستخدم بارتكاب الجريمة ، تبدأ عملية اتخاذ الإجراءات اللازمة لإلقاء القبض على المشتبه به[1].

ويمكن تشبيه عنوان الإنترنت الرقمي IP Address بأرقام الهواتف. فعنوان الإنترنت يزودنا بالمنطقة الجغرافية التي انطلقت منها الرسالة (البلد والمدينة، واسم المضيف Hostname، وتحديد الموقع التقريبي)، وبفضل هذه المعلومات يمكن في أغلب الأحوال تعيين المشتبه به[2].

وعنوان الإنترنت الرقمي يمكن الحصول عليه عن طريق مزود خدمة الإنترنت، إذ إن مزود الخدمة يقوم بالحصول على مجموعة كبيرة من العناوين عن طريق الجهات المسؤولة جغرافياً عن إدارة وتخصيص هذه العناوين. فمثلاً الريب RIPE NCC[3] وهي إحدى الجهات المرخص لها من قبل الآيكان ICANN، تقوم بتخصيص عناوين النفاذ لمنطقة أوربا والشرق الأوسط وبعض دول آسيا وإفريقيا. وسورية تنتمي إلى هذه المنطقة، وتملك النطاق العلوي "sy." حسب ترتيبات الآيكان، وتدير المؤسسة العامة للاتصالات في سورية حالياً هذا النطاق، حيث تقوم بتخصيص أسماء النطاقات الداخلية للراغبين في الحصول عليها لقاء رسوم سنوية.

---

(1) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت,المرجع السابق، ص 811.

(2) www.WhatIsMyIPAddress.com وهو موقع مخصص للتعرف على بروتوكول الـ IP.

(3) وهو اختصاص لـ Reseau IP Europeans Network Coordination Center ومتوفر على الموقع www.ripe.net

أما تخصيص عناوين الإنترنت فيتم بطريقتين، هما[1]:

**الطريقة الأولى: ثابتة Statically**. ووفقاً لهذه الطريقة يتم تخصيص عنوان محدد للمشترك عن طريق مزود خدمة الإنترنت. فعلى سبيل المثال، لو أن مزود الخدمة حصل على /1000/ عنوان رقمي عن طريق الجهات المسؤولة، وأراد تخصيص هذه الأرقام لزبائنه بالطريقة الثابتة، فإن إجمالي عدد هؤلاء الزبائن سيكون /1000/ مشترك.

**الطريقة الثانية: متحركة أو ديناميكية Dynamically**. وفي هذه الحالة لا يتم تخصيص زبائن مزود خدمة الإنترنت بعناوين محددة. فمثلاً عندما يريد المشترك الدخول إلى الإنترنت، فإنه يطلب ذلك عن طريق مزود الخدمة المشترك معه، حيث يكون لدى هذا المزود مُخدّم يسمى DHCP[2]، وهو عبارة عن حاسوب يحتوي على قائمة من العناوين الرقمية المتاحة، بحيث يمنح هذا المُخدّم أحدها للمشترك بشكل ديناميكي.

ومن الملاحظ أن مزود خدمة الإنترنت يعلم أن جميع المشتركين لديه لن يدخلوا إلى شبكة الإنترنت في نفس الوقت، لذلك يلجأ في الغالب إلى اتباع الطريقة الديناميكية، التي تؤمّن له مضاعفة عدد زبائنه، وتؤدي إلى تخفيض كلفة الحصول على العناوين الرقمية، ومن ثم تحقيق عائدات مالية أكبر.

وتجدر الإشارة إلى أن بروتوكول الإنترنت المشار إليه، الذي يحدد هوية الحاسوب، لا يتم منحه بطريقة واحدة على المستوى العالمي. ففي الولايات المتحدة الأمريكية وكندا وبعض الدول المتقدمة، يقوم الشخص باقتناء IP

---

(1) Anthony Reys and others, Cyber Crime Investigations, Bridging The Gaps Between Security Professional Law, Enforcement and Prosecutors. Published by Elsevier Since and Technology, 2007, P-200-201.

(2) وهو اختصار لـ Dynamic Host of Configuration، ويعني بروتوكول التشغيل الديناميكي.

خاص به، ومن ثم يمكن تحديد هويته بسهولة عند ارتكابه جريمة إنترنت. أما في بعض الدول الأخرى –ومنها أغلب الدول العربية– فإن العنوان الرقمي يكون محلاً للتغير بين عدة مشتركين، وبالتالي فإن تحديد هوية المشتبه به تكون أكثر صعوبة[1]. ويمكن القول إنه بمجرد وجود شخص في سورية على الإنترنت، فإنه يملك فوراً هوية رقمية محددة IP، إلاّ أنه إذا حدث وانقطع الإرسال، فإن الشخص إذا عاود الاتصال من جديد، فإن الهوية السابقة قد لا تبقى له، بل لغيره، وقد يظهر بهوية جديدة، أي بـ IP جديد.

كما تجدر الملاحظة بأن الشبكات الداخلية تعد من الأمور الشائعة في مجال الشركات، حيث يحتاج العاملون في هذه الشركات إلى التواصل وتبادل الملفات فيما بينهم. ويمكن استخدام عنوان خارجي واحد لتشغيل عدد من الحواسيب المرتبطة فيما بينها عن طريق شبكة داخلية[2].

وفي حال ارتكاب جريمة إنترنت، عن طريق أحد الحواسيب الموصولة إلى شبكة داخلية، فإن على موظف الضابطة العدلية أن يتوصل إلى رقم العنوان الخارجي، ثم يتم تحديد الحاسوب المطلوب عن طريق العنوان الداخلي، ومن ثم يتم معرفة الشخص المقصود.

## ب–أشهر الشركات المختصة بعملية التتبع عبر الإنترنت:

بدأ العديد من الشركات التي تعمل في مجال التكنولوجيا بتقديم نسخٍ متطورة من التقنيات التي تقوم بتحديد الموقع الجغرافي للمستخدم.

ومن أشهر هذه الشركات شركة Akamai، وهي شركة تقدم خدمة Edge Shape لزبائنها، بحيث تسمح هذه الخدمة بتتبع المستخدم عبر الإنترنت، وتحديد موقعه الجغرافي، عن طريق رسم خريطة للعنوان الرقمي العائد لهذا

(1) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت,المرجع السابق، ص 811.

(2) Anthony Reys and others, op-cit, P-203.

المستخدم، ثم يتم جمع هذه المعلومات في قاعدة بيانات على موقع الشركة الإلكتروني، بحيث تصبح متاحة لزبائنها.

فإذا اشترك مالك أحد المواقع الإلكترونية في خدمة Edge Shape، فإن أي شخص يقوم بالدخول إلى هذا الموقع في أي وقت، يتم جمع بيانات تفصيلية عنه، مثل البلد الذي تمّ الدخول منه، والموقع الجغرافي في هذا البلد، واسم مزود الخدمة الذي دخل من خلاله.

ومن الشركات التي تعمل في نفس المضمار أيضاً شركة Quova، وهي شركة مقرها "كاليفورنيا"، وقد طورت هذه الشركة خدمة Geopoint، حيث تصل دقة هذه الخدمة في تحديد متصفحي الإنترنت ومواطنهم ومواقعهم إلى نسبة 85% إلى 98%. وقد استخدمت شركة Cinema Now المحدودة المسؤولية خدمة Geopoint، وهي شركة مقرها في "كاليفورنيا"، وتعمل في مجال توزيع الأفلام السينمائية عبر الإنترنت، من أجل حماية حقوقها على هذه الأفلام، والتأكد من أن عملية التوزيع تتم وفق الاتفاقيات القانونية للتوزيع والنشر [1].

## ج- تتبع البريد الإلكتروني المزيف:

يقوم بعض المجرمين بتزييف أو تزوير البريد الإلكتروني، بغية إخفاء هويتهم الحقيقية. وكثيراً ما تخفق هذه المحاولات في إخفاء الهوية؛ لأن الرسائل المزيفة أو المزورة تحتوي على عناوين الإنترنت العائدة للمرسلين. ومن الملاحظ أن معظم المحتالين عبر الإنترنت يستخدمون هذا الأسلوب لإخفاء هويتهم الحقيقية.

---

(1) Adam D Thierer , op-cit, P-114 .

ولمعرفة كيفية التلاعب بعناوين الإنترنت، لا بدّ لنا من التعرف على الآلية التي تتم بها عملية إرسال الرسائل الإلكترونية. فالبريد الإلكتروني يشبه البريد العادي في العديد من الجوانب. فعندما يتم إرسال رسالة إلكترونية، يقوم وكيل نقل الرسائل MTA[1]– وهو يشبه مكتب البريد العادي– بختم هذه الرسالة مع وضع وقت الإرسال، واسم وكيل نقل الرسائل، ومعلومات تقنية أخرى، وتكون هذه المعلومات موجودة في ترويسة الرسالة الإلكترونية، ويتم وضع هذه المعلومات من قبل جميع وكلاء نقل الرسائل التي تمرّ الرسالة الإلكترونية عبرهم، إلى أن تصل إلى الجهة المقصودة.

ومن أجل إخفاء عناوين الإنترنت، يقوم مزيفو البريد الإلكتروني بإدخال عناوين وهمية إلى ترويسة الرسالة الإلكترونية لتضليل المحققين، التي تحوي عادة على عناوين المُخدّمات التي مرّت عبرها الرسالة كما ذكرنا. إلاّ أن الخبير التقني يستطيع عن طريق التدقيق الجيد اكتشاف عدم التناسق بين العنوان الوهمي وباقي العناوين الصحيحة في ترويسة الرسالة. ناهيك عن أن الرسالة الإلكترونية ستحمل كحد أدنى العنوان الصحيح الذي تمّ من خلاله إرسال الرسالة الإلكترونية[2].

ومما تقدم نجد أنه من الأهمية بمكان توفير الأجهزة التقنية والخبرات الفنية لدى موظفي الضابطة العدلية، حتى يتمكنوا من تتبع الأثر الافتراضي للجاني، وتحديد مكانه وإلقاء القبض عليه.

---

(1) وهو اختصار لـ Message Transfer Agents ويقصد به الحاسوب أو المخدم المسؤول عن نقل الرسائل الإلكترونية.

(2) Eoghn Casey: op-cit, P-465,466 .

## ثانياً– التفتيش:

يعدّ التفتيش من أخطر الإجراءات التحقيقية، لأنه يمسّ السر الخاص بالأشخاص؛ ولذلك تضمنت أغلب دساتير العالم مبدأ المحافظة على الأسرار الخاصة بالأشخاص.

فدستور الجمهورية العربية السورية لعام 1973 نص على عدم جواز تحري أحد، ونص على حرمة المساكن وعدم جواز دخولها إلاّ في الأحوال التي يجيزها القانون، كما نص على سرية المراسلات البريدية والاتصالات[1]. أما قانون العقوبات السوري فقد تضمّن نصوصاً تعاقب على خرق حرمة المنزل، وعلى إفشاء الأسرار[2].

### أ–تعريف التفتيش:

هو: "الاطلاع على محل منحه القانون حماية خاصة، باعتباره مستودع سر صاحبه، ويستوي في ذلك أن يكون المحل مسكناً أو ما هو في حكمه أو أن يكون شخصاً"[3]. والتفتيش كإجراء، هو في الأصل من اختصاص سلطة التحقيق الابتدائي، إلاّ أنه استثناءً يدخل في صلاحية موظفي الضابطة العدلية في الأحوال التي عيّنها القانون.

### ب–شروط التفتيش:

يمسّ التفتيش الأسرار الخاصة للأشخاص، لذلك فهو إجراء خطير، ولا بدّ أن تتحقق فيه مجموعة من الشروط الموضوعية والشكلية:

---

(1) المواد من 28 وحتى 32 من دستور الجمهورية العربية السورية لعام 1973.

(2) المواد 557 و 558 و 565 وحتى 567 من قانون العقوبات.

(3) يعود هذا التعريف إلى الدكتور أحمد فتحي سرور، نظرية البطلان في قانون الإجراءات الجنائية, رسالة دكتوراه, جامعة القاهرة ,دار النهضة العربية– القاهرة, ص 449. مشار إليه عند د.علي الطوالبة: المرجع السابق، ص10.

**وشروطه الموضوعية هي[1]:**

- أن تقع جريمة من نوع الجناية أو الجنحة.
- أن يكون هناك أدلة قوية على ارتكاب الشخص المطلوب تفتيشه أو تفتيش مسكنه هذه الجريمة.
- أن تكون الغاية من التفتيش جمع الأدلة التي تساعد على ظهور الحقيقة.

**أما شروطه الشكلية فهي[2]:**

- إعلام النيابة العامة، إذا كان القائم بالتفتيش قاضي التحقيق.
- اصطحاب الكاتب لتنظيم الضبط.
- حضور المدعى عليه أو من يقوم مقامه تفتيش منزله.
- تفتيش الأنثى يجب أن يتم بمعرفة أنثى تُندب لذلك.

## ج-التفتيش كإجراء تحقيقي والتفتيش الإداري:

يختلف التفتيش كإجراء يدخل في صلاحيات سلطة التحقيق عن التفتيش الإداري الذي تقوم به السلطة العامة لضرورات الأمن العام. فالتفتيش الإداري لا يتم بغرض ضبط أدلة جريمة قد وقعت، بل يهدف إلى الكشف عن الجرائم قبل وقوعها؛ فهو إجراءٌ إداريٌ بحت. ومن أمثلته، تفتيش الأشخاص عند دخولهم الأماكن الحكومية، وتفتيش العمال عند مغادرتهم المصانع، والتفتيش الإداري الذي تقوم به السلطة على مقاهي الإنترنت وأماكن مزودي خدمة الإنترنت، للتأكد من تنفيذ الأنظمة والقوانين المفروضة على هذه الجهات. لذلك فالتفتيش الإداري لا يرتبط بحدود معينة، فمن الممكن أن يمتد ليشمل تفتيش

---

(1) د.حسن الجوخدار: المرجع السابق، الجزء الثاني، ص155-156.

(2) المواد من 55 و 36 و 90 و 91 و 93 و 94 من قانون أصول المحاكمات الجزائية.

الحقائـب والحواسـيب والهواتـف النقالـة...الخ. وذلـك تبعـاً لضـرورات الحالـة الأمنية[1].

وغني عن البيان أن التفتيش كإجراء من إجراءات التحقيق هو مدار هذا البحث دون غيره.

## د-محل التفتيش:

لا يرد التفتيش إلا على الأسرار الخاصة. فالاطلاع على الأشياء المعلنة للجمهور لا يعدّ تفتيشاً، لأن محل التفتيش هو مستودع السر، ومن ثم فالتفتيش يمكن أن يرد على الشخص ذاته، أو على مكانه الخاص كالمنزل وملحقاته[2].

**أما محل التفتيش في جريمة الاحتيال عبر الإنترنت، فيرد على ما يلي:**

- **الحاسوب بمكوناته المادية والمعنوية(البرمجيات)**، لأنه وسيلة النفاذ إلى العالم الافتراضي، إضافةً إلى الشخص الذي يستخدم الحاسوب موضوع التفتيش.
- **شـبكة الإنترنـت**، بمـا تشـمل مـن مكوّنـات، كالمُخـدّمات والمضـيفات والبرمجيات والملحقات التقنية الأخرى.

**وتشمل المكونات المادية للحاسوب ما يلي:**

- وحدة الإدخال.
- وحدة الذاكرة الرئيسية.
- وحدة الحساب والمنطق.
- وحدة الإخراج.

---

(1) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت,المرجع السابق، ص 855. د.حسن الجوخدار: المرجع السابق، الجزء الثاني، ص157.

(2) د.حسن الجوخدار: المرجع السابق، الجزء الثاني، ص 158.

– وحدات التخزين الثانوية.

**كما تشمل المكونات المعنوية أو البرمجية للحاسوب ما يلي:**

– الأنظمة الأساسية، كأنظمة التشغيل.

– الكيانات المنطقية التطبيقية، كالبرامج التي تستخدم للقيام بعمل معين، ومثالها البرمجيات التطبيقية بأنواعها، كبرامج ألعاب الأطفال وغيرها[1].

– البيانات المخزنة في الحاسوب بأنواعها .

وسنشرع فيما يلي بدراسة تفتيش المكونات المادية والمعنوية للحاسوب، ثم ننتقل لدراسة تفتيش شبكات الحاسوب.

## 1–تفتيش مكونات الحاسوب المادية والمعنوية (البرمجية):

التفتيش وسيلة للإثبات، فهو ليس غاية في ذاته، لأنه يهدف إلى ضبط الأشياء المادية المتعلقة بالجريمة، والتي تفيد في إظهار الحقيقة.

والواقع أن تفتيش مكونات الحاسوب المادية لا يثير أية مشكلة، لأن هذه المكونات تدخل بطبيعتها في مفهوم الأشياء المادية، ومن ثم يمكن لموظف الضابطة العدلية أن يقوم بتفتيش جهاز الحاسوب أو الطابعة أو الماسح الضوئي أو السماعات... الخ، بحثاً عن الأشياء الممنوعة كالمخدرات أو العملة المزورة، أو لمعرفة فيما إذا كانت هذه الأجهزة مهربة أم لا.

لكن المشكلة تكمن في مدى صحة تفتيش المكونات البرمجية للحاسوب، نظراً لغياب المظهر المادي المحسوس للمعلومات المجردة عن دعامتها أو وسيط التخزين.

والسؤال الذي يطرح نفسه هنا هو:

---

(1) المستشار الدكتور عبد الفتاح بيومي حجازي: مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، المرجع السابق, ص389. د.سليمان أحمد فضل: المرجع السابق، ص307.

**هل يصح قانوناً تفتيش المكونات المعنوية أو البرمجية للحاسوب، بحثاً عن الأدلة الرقمية التي تفيد في كشف الجريمة أو كيفية ارتكابها؟**

للإجابة على هذا السؤال لا بد لنا من التعرف على الرأي الفقهي والتشريعي من مسألة تفتيش البرمجيات .

- **الموقف الفقهي :**

ذهب الفقه العربي في إجابته عن هذا السؤال إلى اتجاهين ، هما[1]:

**الاتجاه الأول:**

يرى أصحاب هذا الاتجاه أن النصوص الحالية في قوانين الأصول الجزائية لا تنسحب إلى المكونات المعنوية للحاسوب، ولا تسمح بالبحث والتنقيب عن الأدلة في برامج الحاسوب وبياناته.

ويستند أصحاب هذا الرأي إلى أن بعض التشريعات الأصولية العربية، حدّدت الهدف من التفتيش بأنه البحث عن (شيء) أو (أشياء) وضبطها[2]، وهذا (الشيء) يقتصر مفهومه على المال ذي الحيز المادي المحسوس، ولا يمتد إلى المعلومات والبيانات والبرامج غير المحسوسة، ذلك أن الأصل في الأشياء أن تكون مادية.

**الاتجاه الثاني:**

---

(1) د.علي الطوالبة: المرجع السابق، ص 29-30.

(2) ومن أمثلة التشريعات العربية التي أوردت كلمة" شيء أو أشياء"، القانون المصري في المواد (46 حتى 50، 53، 55، 90 حتى 94، 98، 109)، والقانون اللبناني في المواد (من 30 حتى 36)، والقانون المغربي في المواد (61، 102، 105)، والقانون الجزائري في المواد (41 حتى 44، 84)، والقانون الليبي في المواد (75، 78، 82 حتى 92)، والقانون الأردني في المواد (34، 81، 86).

علـى عكـس أصـحاب الاتجـاه الأول، يـرى أصـحاب هـذا الاتجـاه، أن النصـوص المتعلقـة بـالتفتيش فـي بعض التشريعات الأصـولية العربيـة[1] تسمح بتفتيش المعلومات والبيانات والبرمجيات، ذلك لأن صياغة هذه النصوص لم تقتصر على ذكر الأشياء بل سمحت بالبحث عن أي أثر للجريمة[2]. فهذا الاتجاه يقوم بتفسير النصوص على نحو أوسع، بحيث تشمل تفتيش وضبط الكيانات البرمجية للحاسوب.

- **<u>موقـف بعـض التشـريعات الأجنبيـة مـن مسـألة تفتـيش المكونات المعنوية أو البرمجية للحاسوب:</u>**

قامت بعض الدول الأجنبية بسنّ تشريعات إجرائية حديثة، قنّنت فيها موضوع تفتيش مكونات الحاسوب البرمجية وضبطها، ومن هذه الدول:

**الولايات المتحدة الأمريكية**، حيث نظم المشرع الأمريكي إجراءات تفتيش وضبط المكونات البرمجية للحاسوب، من خلال القوانين الإجرائية الفيدرالية المتعلقة بجرائم الحاسوب المنصوص عليها في القسم 42usc 2000[3].

---

(1) ومن هذه القوانين، قانون دولة الكويت رقم 17 لعام 1960 في المواد (77 ، 79، 80 وحتى 83، 89، 91 وحتى 97)، والقانون البحريني لسنة 1966 في المواد (44، 45 وحتى 57، 60)، والقانون القطري رقم 23 لعام 2004 في المواد (50 وحتى 56، 75، 76).

(2) تنص المادة 83 من قانون الإجراءات والمحاكمات الجزائي الكويتي الصادر بالقانون رقم 17 لعام 1960 على ما يلي:

"تفتيش المساكن يكون بدخولها والبحث فيها **عن شيء أو أثر يفيد التحقيق أو يلزم له**. وللقائم بتفتيش المسكن أن يبحث عن الأشياء المطلوب ضبطها في جميع أجزاء المسكن ومحتوياته". متوفر على موقع تشريعات مجلس دول التعاون الخليجي www.gcc-legal.org.

(3) نبيلة هبة هروال: المرجع السابق، ص 226.

كما أصدر المشرع الأمريكي دليلاً استرشادياً يعرف باسم (المرشد الفيدرالي الأمريكي لتفتيش وضبط الحواسيب، توصلاً إلى الدليل الإلكتروني في التحقيقات الجنائية.)[1].وهذا المرشد تمّ وضعه أول مرة عام 1964، وتمّ تعديله عدة مرات، كان آخرها عام 2002، حيث تضمن التعديل الأخير تنظيم طرق الحصول على الدليل الإلكتروني، وفق القانون الوطني الأمريكي المعروف بـ The Patriot Act of 2001. ويقتصر تطبيق قواعد هذا المرشد على الحواسيب المرتبطة بالشبكات، والحالات التي يجوز فيها تفتيش أو ضبط الحواسيب بإذن أو من دون إذن[2].

وقد حدّد هذا المرشد الخطوات اللازم اتباعها من أجل نجاح عملية تفتيش وضبط الحواسيب. وهذه الخطوات هي[3]:

- إعداد فريق يتكون من رجل الضبط القضائي المكلف بالقضية، والمدعي العام، وخبير فني، قبل القيام بعملية التفتيش.
- التعرف قدر الإمكان على نظام الحاسوب المراد تفتيشه قبل وضع خطة التفتيش أو طلب الإذن بذلك.
- وضع خطة لتنفيذ التفتيش مبنية على المعلومات التي تمت معرفتها عن نظام الحاسوب المستهدف.
- يجب أن يتضمن إذن التفتيش، محل التفتيش المراد ضبطه بدقة، وشرح استراتيجية التفتيش الممكنة.

---

(1) "Searching and seizing computer to obtaining Electronic Evidence in Criminal Investigations" Guide.

(2) د.عمر بن يونس: الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي,المرجع السابق، ص 9-24-35-53-159 .

(3) د.عمر بن يونس: الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي,المرجع السابق، ص 162 وما بعدها.

**أما الاتفاقية الأوربية حول الجريمة الافتراضية لعام 2001**، فقد نظّمت تفتيش وضبط البيانات المخزنة في الحاسوب بالمادة 19 من هذه الاتفاقية، حيث سمحت هذه المادة بما يلي[1]:

- تفتيش نظام الحاسوب أو جزء منه والبيانات المخزنة فيه.
- تفتيش معالج تخزين البيانات في الحاسوب الذي يحوي على بيانات معينة. (الفقرة 1 من المادة 19).
- ضبط الحاسوب أو جزء منه، أو معالج تخزين البيانات في الحاسوب.
- الاحتفاظ بنسخة من تلك البيانات.
- الحفاظ على سلامة البيانات المخزنة في الحاسوب. (الفقرة 3 من المادة 19).
- إلزام مشغلي النظام بتقديم المساعدة المطلوبة أثناء تنفيذ التفتيش والضبط. (الفقرة 4 من المادة 19).

أما في **المملكة المتحدة**، فقد سمح المشرع بتفتيش الحاسوب، بالقسم الرابع عشر من قانون إساءة استخدام الكمبيوتر لعام 1990، وذلك بعد الحصول على إذن بالتفتيش من القاضي المختص[2].

**وفي بلجيكا**، أصدر المشرع البلجيكي القانون المؤرخ بـ 2001/11/28 المتضمن تعديل قانون التحقيق الجنائي، الذي أضاف المادة /88/ إلى هذا القانون، والتي سمحت لقاضي التحقيق أن يصدر إذن بتفتيش نظم المعلومات[3].

---

(1) المادة /19/ من الاتفاقية الأوربية. د.عمر بن يونس: الاتفاقية الأوربية حول الجريمة الافتراضية ,المرجع السابق, ص 149 وما بعدها.

(2) القاضي الدكتور غسان رباح: المرجع السابق، ص 159.

(3) د. عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت,المرجع السابق، ص 854.

ومن الأمثلة الواقعية لتفتيش برامج الحاسوب، أنه بعد تفجير بُرجي مركز التجارة العالمي في الولايات المتحدة الأمريكية في2001/9/11، ولدى تفتيش الحاسوب النقال العائد للمشتبه به "رمزي يوسف" تبيّن – بحسب رأي الـ FBI– بأن هذا الحاسوب كان يحوي الخطط اللازمة للقيام بعمليتي التفجير، كما أدّى هذا التفتيش إلى الكشف عن دور المدعو "زكريا الموسوي" في عملية التفجير الثانية. وقد تمّ فحص وتفتيش أكثر من مئة قرص صلب في هذه التحقيقات[1].

وفي قضية أخرى، تتلخص وقائعها بأن السيدة "شارون لوباتكا" غادرت منزلها بقصد زيارة صديقتها، إلا أنها تغيبت عن المنزل لعدة أيام، ولدى تفتيش الحاسوب الشخصي العائد لها، وجدت الشرطة مئات الرسائل الإلكترونية بين السيدة "شارون" وشخص يدعى "روبرت غلاس"، وقد تضمنت هذه الرسائل تخيلات عن التعذيب والموت. ولدى قيام الشرطة بالتحقيق مع "غلاس"، اعترف بأنه قتل شارون خطأً أثناء نومه معها، كما قام بإرشاد الشرطة إلى مكان جثتها في شمال كاليفورنيا، حيث وجدت الشرطة أيدي وأرجل شارون مربوطة، ثم تبين أنها ماتت خنقاً[2].

## 2–تفتيش شبكات الحاسوب:

من المشكلات التي تواجه القائم بالتفتيش، مشكلة اتصال الحاسوب موضوع التفتيش بحاسوب آخر موجود داخل أو خارج إقليم الدولة. فكثيراً ما يقوم مرتكب الجريمة بتخزين معلوماته في حواسيب أو مُخدّمات أخرى؛ بهدف عرقلة التحقيقات.

والسؤال الذي يطرح نفسه هنا هو:

---

(1) Eoghan Casey, op-cit, p-19.

(2) Eoghan Casey, op-cit, p-20.

**هل يشمل التفتيش الحواسيب الأخرى المرتبطة بالحاسوب المطلوب تفتيشه؟**

للإجابة على هذا السؤال هناك احتمالان:

**الاحتمال الأول:**

**أن يكون حاسوب المتهم متصلاً بحاسوب أو مُخدّم موجود في مكان آخر داخل الدولة.**

هناك من يرى في **الفقه الألماني** أنه في هذه الحالة يمكن أن يمتد التفتيش إلى المعلومات والبيانات المخزنة في حاسوب أو مُخدّم الآخر، وذلك استناداً إلى القسم 103 من قانون الإجراءات الجزائية الألماني.

كما نصت المادة 125 من مشروع قانون الحاسوب في **هولندا** على جواز أن يمتد التفتيش في هذه الحالة إلى نظم المعلومات الموجودة في حاسوب أو مُخدّم آخر، بشرط أن تكون هذه المعلومات والبيانات ضرورية لإظهار الحقيقة، وذلك مع مراعاة بعض القيود[1].

أما الفقرة الثانية من المادة 19 من **الاتفاقية الأوربية حول الجريمة الافتراضية لعام 2001**، فقد سمحت بتفتيش نظام حاسوب آخر أو جزء منه، إذا كان هناك أساس يدعو إلى الاعتقاد بأن البيانات المطلوبة قد تمّ تخزينها

---

(1) Kaspersen (W.K.Henrik):"computer crime and crime against information in Netherlands"R.I.D.p1993,p.479.

مشار إليه عند المستشار الدكتور عبد الفتاح بيومي حجازي: مبادئ الإجراءات الجنائية في جرام الكمبيوتر والإنترنت، المرجع السابق، ص 381 – 382. د.علي الطوالبة:المرجع السابق,ص40–41. نبيلة هبة هروال: المرجع السابق، ص 239–240.

في نظام ذاك الحاسوب، بشرط أن يكون نظام الحاسوب الآخر ضمن النطاق الإقليمي للدولة[1].

**الاحتمال الثاني:**

**أن يكون حاسوب المتهم متصلاً بحاسوب أو مُخدّم آخر موجود في مكان آخر خارج الدولة.**

في هذه الحالة هناك من يرى في **الفقه الألماني** أن استرجاع المعلومات والبيانات التي تم تخزينها في الخارج يعتبر انتهاكاً لسيادة الدولة الأخرى[2].

أما المادة 125 من مشروع قانون الحاسوب **في هولندا**، فقد سمحت بتفتيش نظم الحاسوب المرتبطة بحاسوب المتهم، حتى ولو كانت موجودة في دولة أخرى، بشرط أن يكون هذا التدخل مؤقتاً، وأن تكون المعلومات والبيانات لازمة لإظهار الحقيقة[3].

أما المادة 32 من **الاتفاقية الأوربية حول الجريمة الافتراضية لعام 2001**، فقد سمحت بتفتيش حاسوب موجود في دولة أخرى في حالتين: الأولى

---

(1) المادة /19/ من الاتفاقية الأوربية. د.عمر بن يونس: الاتفاقية الأوربية حول الجريمة الافتراضية ,المرجع السابق, ص 149 وما بعدها.

(2) Mohrenschl ager (Manfred):computer crimes and other crimes against information technology in GermanyR.I.P,1993, p.351.
مشار إليه عند المستشار الدكتور عبد الفتاح بيومي حجازي: مبادئ الإجراءات الجنائية في جرام الكمبيوتر والإنترنت، المرجع السابق، ص 382.

(3) Durham (colo):The emerging structures of criminal information law: tracing the contours of a new pardign general report for the A.I.D.P. 1993,p.115.
مشار إليه عند المستشار الدكتور عبد الفتاح بيومي حجازي: مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، المرجع السابق، ص 383.

إذا تعلق التفتيش ببيانات متاحة للجمهور. والثانية إذا رضي صاحب البيانات بالتفتيش[1].

ففي إحدى قضايا الاحتيال عبر الإنترنت، تبين بنتيجة البحث أن حاسوب المتهم الموجود في ألمانيا متصل بحواسيب أخرى في سويسرا، حيث تم تخزين المعلومات في هذه الحواسيب الخارجية. وعندما رغبت السلطات الألمانية بالحصول على هذه المعلومات، لم تستطع ذلك إلاّ من خلال طلب المساعدة المتبادلة[2].

وفي اليابان، قامت مجموعة من المخربين بمهاجمة العديد من المواقع الخاصة في الحكومة اليابانية، واستخدموا في ذلك حواسيب موجودة في الصين والولايات المتحدة الأمريكية. وقد طلبت الشرطة اليابانية المساعدة من بكين وواشنطن من أجل تسليم المعلومات والبيانات المسجلة على هذه الحواسيب في كلتا الدولتين، حتى تتمكن من التوصل إلى هؤلاء المجرمين[3].

والواقع أن هناك سؤالاً يتبادر إلى الأذهان في موضوع التفتيش، هو:

**هل يشمل الإذن بتفتيش مكان ما، تفتيش الحواسيب الموجودة فيه؟ وهل يشمل تفتيش الشخص، تفتيش حاسوبه الشخصي المحمول؟**

تترتب آثار مختلفة بحسب الإجابة عن هذا السؤال بالنفي أو الإيجاب. فإذا اعتبرنا أن الحاسوب جزء من المكان المطلوب تفتيشه، فإن مجرد صدور إذن التفتيش لمكان ما، يشمل ما بداخله من حواسيب. أما إذا اعتبرنا أن

---

(1) المادة /32/ من الاتفاقية الأوربية. د.عمر بن يونس: الاتفاقية الأوربية حول الجريمة الافتراضية ,المرجع السابق, ص227.

(3) المستشار الدكتور عبد الفتاح بيومي حجازي: مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، المرجع السابق، ص 383.

(3) المستشار الدكتور عبد الفتاح بيومي حجازي: مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، المرجع السابق، ص 383.

الصيغة العامة لإذن التفتيش لا تشمل الحواسيب الموجودة في المكان موضوع التفتيش، ففي هذه الحالة يجب أن يتضمن الإذن صراحة جواز تفتيش جميع الحواسيب الموجودة في هذا المكان.

ويذهب الرأي الغالب في الفقه إلى اعتبار الحاسوب جزء من المكان المطلوب تفتيشه، كما يرى أصحاب هذا الرأي أنه كلما أجاز القانون القبض على شخص ما، أمكن تفتيشه وتفتيش ما بحوزته بما في ذلك حاسوبه النقال[1].

## تفتيش المكونات المعنوية أو البرمجية للحاسوب في ظل التشريع السوري:

نص المشرع السوري في قانون أصول المحاكمات الجزائية على التفتيش في العديد من المواد، نذكر منها:

**المادة 32:**

(1- يضبط النائب العام الأسلحة وكل ما يظهر أنه استعمل في ارتكاب الجريمة، أو أُعدّ لهذا الغرض، كما يضبط **كل ما يرى من آثار الجريمة وسائر الأشياء** التي تساعد على إظهار الحقيقة.

2- يستجوب النائب العام المدعى عليه عن الأشياء المضبوطة بعد عرضها عليه، ثم ينظّم محضراً يوقعه مع المدعى عليه، وإذا تمنع هذا الأخير عن التوقيع، صُرح بذلك في المحضر.).

**المادة 33:**

(إذا تبين من ماهية الجريمة أن الأوراق والأشياء الموجودة لدى المدعى عليه يمكن أن تكون مدار استدلال على ارتكابه الجريمة، فللنائب العام أن

(1) د. عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت,المرجع السابق، ص 854- 855.

ينتقل حالاً إلى مسكن المدعى عليه للتفتيش **عن الأشياء** التي يراها مؤدية إلى إظهار الحقيقة.).

**المادة 89:**

(1-لا يجوز دخول المنازل وتفتيشها إلاّ إذا كان الشخص الذي يراد دخول منزله وتفتيشه مشتبهاً فيه بأنه فاعل الجرم أو شريك أو متدخل فيه أو حائز **أشياء** تتعلق بالجرم، أو مخفٍ شخصاً مدعى عليه.

2-إن دخول القاضي أحد المنازل بحال عدم توفر الشروط المذكورة آنفاً يعتبر تصرفاً تعسفياً من شأنه أن يفسح المجال للشكوى من الحكام.).

**المادة 90:**

(مع مراعاة الأحكام السابقة، يحق لقاضي التحقيق أن يقوم بالتحريات في جميع الأمكنة التي يحتمل وجود **أشياء** فيها يساعد اكتشافها على ظهور الحقيقة.).

وباستقراء هذه النصوص، يمكن القول إن النصوص الحالية المتعلقة بالتفتيش، تسمح بتفتيش المكونات المعنوية للحاسوب، للأسباب التالية:

1- سبق وأن ذكرنا بأن المعلومات أو البرامج وإن لم يكن لها كيان مادي محسوس، إلاّ أنها تشغل **حيزاً مادياً** في ذاكرة الحاسوب أو وسائط التخزين، يمكن قياسه بمقياس معين وهو "البايت" (byte)؛ إذ إن سعة أو حجم الذاكرة الداخلية للحاسوب تقاس بعدد الحروف التي يمكن أن تُخزن فيها. فالبيانات تكون على شكل نبضات إلكترونية ممثلة بالرقمين صفر أو واحد (0-1)، وهي

تشبه التيار الكهربائي الذي اعتبره التشريع السوري من الأشياء المنقولة[1]، وبالتالي فإن البرامج يمكن أن تدخل في نطاق الأشياء المادية[2].

2- إن عبارة **(آثار الجريمة وسائر الأشياء)**، الواردة في نص المادة /32/ من قانون أصول المحاكمات الجزائية، تسمح بتفتيش المكونات المعنوية أو البرمجية للحاسوب، لأن هذه المكونات تعدّ أثراً من آثار الجريمة عندما تتضمن أدلة تساعد في كشف الحقيقة. ولا يوجد ما يمنع من التوسع في تفسير القواعد الأصولية بحيث تشمل تفتيش هذه المكونات المعنوية.

3- **أما فيما يتعلق بتفتيش الحاسوب أو المُخدّم المرتبط بحاسوب المتهم.** فإن **الباحث يرى** أن تفتيش الحاسوب الآخر أمر تفرضه أهداف التفتيش والضرورات العملية. إذ إن عدم القيام بتفتيش هذه الأجهزة يفقد التفتيش هدفه الرئيسي، وهو الحصول على الأدلة الرقمية الضرورية لإظهار الحقيقة.

**كما أن امتداد التفتيش إلى حاسوب أو مُخدّم موجود في دولة أخرى** لا يشكّل انتهاكاً لسيادة هذه الدولة، لأن الطبيعة العالمية للإنترنت تسمح بمثل هذا الإجراء. كما أن متطلبات السرعة في إجراء عملية التفتيش تقتضي عدم انتظار إذن الدولة التي يوجد فيها الحاسوب أو المُخدّم الآخر، مع ضرورة إعلام هذه الدولة في وقت لاحق. وتجنباً لهذا المحظور فإننا **نقترح** على المشرع السوري إبرام العديد من الاتفاقيات الدولية التي تضمن التعاون الشرطي والقضائي في هذا المجال .

4- **أما بالنسبة إلى مسألة مدى اعتبار الحاسوب جزءاً من المكان المطلوب تفتيشه،** فإن الواقع العملي في سورية يشير إلى أن إذن التفتيش المتعلق بالمكان الخاص، يشمل جميع الحواسيب الموجودة في هذا المكان.

---

(1) المادة 621 من قانون العقوبات السوري.

(2) د.علي الطوالبة: المرجع السابق، ص30.

ففي إحدى القضايا الحديثة في سورية التي تتلخص وقائعها بأن شركة وهمية للوساطة والاستثمارات المالية، مقرها في دمشق، ولها موقع على الإنترنت، استولت بالخداع على مبالغ نقدية كبيرة من المواطنين، بحجة شراء الأسهم والمضاربة بالبورصة ، وبأنها وكيلة لشركة CIB الأمريكية العالمية للأوراق المالية.

وبعد أن حصل فرع الأمن الجنائي بدمشق على إذن بتفتيش مقر الشركة من السيد المحامي العام الأول بدمشق، تمّ ضبط أجهزة الحاسوب الموجودة في هذا المقر، وتمّ نقلها إلى فرع الأمن الجنائي بدمشق لفحصها من قبل خبير تقني، حيث تمّ العثور فيها على العديد من البرامج المتعلقة بمؤشرات البورصة، إضافةً إلى المعلومات التي تتضمن البيانات الشخصية العائدة للعديد من الضحايا من جنسيات مختلفة[1].

والحقيقة أن **الباحث يؤيد** هذا التوجه العملي، مادام تفتيش أجهزة الحاسوب الموجودة في المكان المطلوب تفتيشه تفيد في إظهار الحقيقة.

ومع إيماننا بأن النصوص الإجرائية الحالية تسمح بتفتيش المكونات المعنوية أو البرمجية للحاسوب وشبكة الإنترنت، إلاّ أننا **نقترح** على المشرع السوري في مشروع قانون الجريمة الإلكترونية أن ينص على جواز تفتيش المكونات المعنوية لحاسوب المشتبه به والحواسيب المتصلة به أيضاً، أيّاً كان مكان وجودها، ما دام في ذلك فائدة في إظهار الحقيقة. وبذلك يحسم المشرع السوري الخلاف الذيَ شجَرَ بين الفقهاء، ثم لا يجدون في أنفسهم حرجاً مما قضى ويسلموا تسليما.

## ثالثاً– الضبط:

(1) ضبط فرع الأمن الجنائي بدمشق رقم 94 تاريخ 2008/7/13، مسجل في سجلات النيابة العامة بدمشق برقم موجوداً 12823/م تاريخ 2008/7/20.

الضبط هو الأثر المباشر للتفتيش. والعلاقة وثيقة بين التفتيش والضبط، فإذا بطلت إجراءات التفتيش بطل الضبط. وقد يتم الضبط من غير تفتيش، فقد يقدم المتهم أو الشاهد باختياره الأشياء المتعلقة بالجريمة [1].

والضبط هو الوسيلة القانونية التي تضع بواسطتها السلطة المختصة يدها على جميع الأشياء التي وقعت عليها الجريمة أو نتجت عنها أو استعملت لاقترافها، كالأسلحة والأشياء المسروقة، والثياب الملوثة بالدم، والأوراق... وغير ذلك[2].

وقد أجاز القانون السوري ضبط كل ما يعدّ من آثار الجريمة، وسائر الأشياء والأوراق التي تساعد على إظهار الحقيقة، سواء أكانت تؤيد التهمة أم تنفيها. وقد أوجب القانون عرض الأشياء المضبوطة على المدعى عليه أو على من ينوب عنه للمصادقة والتوقيع عليها، فإذا امتنع، صرّح القائم بالضبط بذلك في المحضر[3].

والأصل أن الضبط يقع على الأشياء المادية، ولا ينصبّ على الأشياء المعنوية. والسؤال الذي يطرح نفسه هنا هو:

**هل يمكن أن ينصبّ الضبط على المكونات المعنوية للحاسوب أو الإنترنت؟**

انقسم الفقه في الإجابة على هذا السؤال إلى اتجاهين، هما[4]:

## الاتجاه الأول:

---

(1) د.علي الطوالبة: المرجع السابق، ص127.

(2) د.حسن الجوخدار: المرجع السابق، الجزء الثاني، ص 162.

(3) المواد 32 ، 34، 97 من قانون أصول المحاكمات الجزائية.

(4) نبيلة هبة هروال: المرجع السابق، ص265. د.علي الطوالبة: المرجع السابق، ص 138-139. عفيفي كامل عفيفي: المرجع السابق، ص378- 379. د.سليمان أحمل فضل: المرجع السابق، ص321-322.

ويرى أنصار هذا الاتجاه أن الضبط لا يمكن أن ينصبّ على المكونات المعنوية لانتفاء الكيان المادي لها، ولكن يمكن ضبط المعلومات والبيانات إذا كانت مخزنة في دعامة أو وسيط إلكتروني، أو كانت من مخرجات الحاسوب، كما لو كانت مطبوعة على الورق، أو في حالة تصوير أو تجميد شاشة الحاسوب.

ومن أنصار هذا الاتجاه الفقه الألماني واللوكسمبورغي والروماني والياباني.

**الاتجاه الثاني:**

وعلى عكس الاتجاه الأول، يرى أنصار هذا الاتجاه أنه لا يوجد ما يمنع من أن ينصب الضبط على المكونات المعنوية كالمعلومات والبيانات، مستندين في ذلك إلى أن غاية التفتيش هو ضبط الأشياء التي تفيد في كشف الحقيقة، وأن هذا المفهوم يمتد ليشمل المعلومات والبيانات.

ومن أنصار هذا الاتجاه الفقه والتشريع في بلجيكا وكندا والولايات المتحدة الأمريكية والاتفاقية الأوربية حول الجريمة الافتراضية لعام 2001.

و**يرى الباحث** أن الاختلاف بين هذين الاتجاهين هو اختلاف ظاهري، فالاتجاه الأول يشترط لضبط المعلومات أن تكون مخزنة في وسيط إلكتروني، وهذا ما لا يشترطه الاتجاه الثاني. والواقع أن المعلومات لا يمكن أن تكون مجردة عن وسيط التخزين، سواء أكان هذا الوسيط ذاكرة الحاسوب، أم قرصاً ممغنطاً أم غير ذلك من الوسائط.

وقد سبقت الإشارة إلى أن المكونات المعنوية أو البرمجية تشغل حيزاً مادياً في ذاكرة الحاسوب، ومن ثم فإن هذه المكونات يمكن ضبطها ضمن وسائط التخزين، مع مراعاة الإجراءات الواجب اتباعها أثناء عملية ضبط هذه المكونات.

## إجراءات ضبط المكونات المعنوية للحاسوب والإنترنت:

إن البيانات والمعلومات لا يمكن ضبطها بشكل منفصل عن أجهزة وأدوات التخزين، فالحاسوب والأجهزة الملحقة به، هي بمثابة الأوعية المادية التي تحتوي هذه المعلومات والبيانات، وهي تشبه الحقيبة التي تُحفظ فيها الأوراق.

ولذلك يرى الفقه المقارن أن على رجل الضابطة العدلية عندما يصل إلى مسرح الجريمة، أن يتبع في ضبط المعلومات الرقمية الإجراءات التالية[1]:

- تأمين مسرح الجريمة الرقمية من العبث، إذ يجب عزل الحواسيب عن الشبكة، لتجنب إجراء أي تغيير على الأدلة الرقمية من قبل الغير. كما يجب رفع البصمات عن الأجهزة لمقارنتها فيما بعد ببصمة المشتبه به.
- حجز الحاسوب أو القرص الصلب، وجميع الحاويات المادية والذواكر، كالسواقات والأقراص الممغنطة.
- وضع ملصقات على الأشياء المضبوطة، وتوثيقها وتغليفها، وتحضيرها لنقلها بالحالة التي كانت عليها إلى مكان الاختبار والفحص.
- تحرير محضر بعد إجراء عملية الفحص، يتضمن ذكر جميع الإجراءات السابقة، والنتائج التي تم التوصل إليها بنتيجة الفحص.

و**يرى الباحث** أن عملية الضبط يجب أن تراعى فيها طبيعة الأشياء المضبوطة. وهذا ما نصت عليه الفقرة الأولى من المادة /35/ من قانون أصول المحاكمات الجزائية، حيث قالت:

(يعنى بحفظ الأشياء المضبوطة بالحالة التي كانت عليها. فتحزم أو توضع في وعاء إذا اقتضت **ماهيتها** ذلك، وتختم في الحالتين بخاتم رسمي.).

---

(1) Anthony Reys and others, op-cit, P-141-142 .

وبناءً على ذلك، فإن ضبط الأدلة الرقمية يجب أن يتناسب مع ماهيتها، بحيث ينصبّ الضبط على جميع الأجهزة والأدوات التي تمّ تخزين المعلومات فيها، لأن ضبط المعلومات والبيانات لا يمكن أن يتم بمعزل عن وسائط التخزين.

# الفصل الثاني
# قواعد الإثبـات

كرّست معظم الدساتير في العالم مبدأ "المتهم بريء حتى يدان بحكم قضائي مبرم"، وذلك حفاظاً على كرامة الإنسان، إذا لم يقم الدليل القاطع على ارتكابه الجريمة[1].

ويقصد بالإثبات في المسائل الجزائية، إقامة الدليل لدى السلطة الجزائية المختصة على حقيقة واقعة ذات أهمية قانونية، وذلك بالطرق المقبولة قانوناً. فالإثبات يهدف إلى إعادة رواية ما حدث من وقائع جرمية أمام القضاء[2].

والإثبات هو العمود الفقري للعدالة الجزائية، إذ لا يمكن أن تتحقق هذه العدالة بدون اللجوء إلى نظام إثبات يضمن تحققها. وقد عرفت التشريعات الإجرائية الجزائية نظامين رئيسيين للإثبات، هما[3]:

**النظام الأول: نظام الإثبات المقيد**، حيث يقوم المشرع في هذا النظام بتحديد طرق الإثبات، والقوة الثبوتية لكل دليل من الأدلة بناءً على قناعة المشرع بها، ولا يكون لقناعة القاضي في هذا النظام أي دور في تقدير الأدلة أو البحث عنها.

---

(1) المادة /28/ من دستور الجمهورية العربية السورية لعام 1973.

(2) د.محمود نجيب حسني: شرح قانون الإجراءات الجنائية,المرجع السابق، ص 405.

(3) د.عبد الوهاب حومد: أصول المحاكمات الجزائية,المرجع السابق،ص 528 حتى 532. د.حسن الجوخدار: المرجع السابق، الجزء الثاني، ص 124 حتى 126. د.محمود نجيب حسني: شرح قانون الإجراءات الجنائية,المرجع السابق، ص 408 – 409.

أما **النظام الثاني: فهو نظام الإثبات الحر**، الذي يقوم على أساس حرية الإثبات؛ أي إن المشرع لا يقوم بتحديد الأدلة، بل يكون للقاضي دور إيجابي في البحث عن الأدلة وتقدير قوتها الثبوتية حسب قناعته بها.

والواقع أن الاختلاف بين هذين النظامين لا يشكل سوى التباين في أسلوب اعتراف المشرع بالحقيقة.

وقد أخذ المشرع الجزائي السوري بنظام الإثبات الحر كمبدأ عام في الإثبات؛ بيد أنه أخذ في بعض الحالات بمبدأ الإثبات المقيد استثناءً من هذا المبدأ العام، حيث أعطى المشرع بعض المحاضر أو الضبوط قوة ثبوتية معينة، واشترط توفر أدلة معينة لإثبات بعض الجرائم، كجريمة الزنا(المادة 473 عقوبات)، وجريمة الإغواء (المادة 504 عقوبات)، كما قرر أنه إذا كان وجود الجريمة مرتبطاً بوجود حق شخصي وجب على القاضي اتباع قواعد الإثبات الخاصة بهذا الحق (المادة 177 أصول محاكمات جزائية).

وقد نص المشرع على مبدأ الإثبات الحر في المادة /175/ من قانون أصول المحاكمات الجزائية الصادر بالمرسوم التشريعي /112/ لعام 1950، التي نصت على ما يلي:

(1-تقام البيّنة في الجنايات والجنح والمخالفات بجميع طرق الإثبات، ويحكم القاضي حسب قناعته الشخصية.

2-إذا نص القانون على طريقة معينة للإثبات، وجب التقيد بهذه الطريقة.

3-إذا لم تقم البيّنة على الواقعة، قرر القاضي براءة المدعى عليه.).

وقد كرّست محكمة النقض مبدأ الإثبات الحر حيث قالت: "إن القانون أمدّ القاضي في المسائل الجنائية بسلطة واسعة وحرية كاملة، في سبيل تقصي ثبوت الجرائم أو عدم ثبوتها، والوقوف على حقيقة علاقة المتهمين بها، ففتح له باب الإثبات على مصراعيه، يختار من كل طرقه ما يراه موصلاً إلى الكشف

عن الحقيقة، ويزن قوة الإثبات المستمدة من كل عنصر بمحض وجدانه، فيأخذ بما تطمئن إليه عقيدته، ويطرح ما لا يرتاح إليه. ولا رقيب عليه في ذلك غير ضميره وحده."[1].

كما أكّدت محكمة النقض أن قناعة القاضي ليست بلا قيد أو شرط، فهي مقيدة بسلامة التقدير والاستدلال، وإلاّ كان قراراه عرضة للنقض[2].

أما عبء الإثبات في القضايا الجزائية فيقع على كاهل النيابة العامة، لأنها هي المدعي في جميع القضايا الجزائية، فالبيّنة على من ادعى. أما المدعي الشخصي فيقوم بمساعدة النيابة العامة في عملية الإثبات عندما يرفع دعواه المدنية تبعاً للدعوى العامة أمام القضاء الجزائي.

ويعدّ موضوع الإثبات في جريمة الاحتيال عبر الإنترنت من الموضوعات الشائكة، لما تتصف به هذه الجريمة من سرعة في ارتكابها، وسهولة في طمس معالمها. ومع ذلك فإن الأدلة التقليدية كالشهادة والقرائن والاعتراف وغيرها لم تتلاش أمام هذه الجريمة المستحدثة، وإن كان دورها قد تضاءل في عملية الإثبات. الأمر الذي أدّى إلى ظهور ما يعرف بالدليل الرقمي، الذي يتم الحصول عليه من خلال عملية البحث والتحري في حاسوب الجاني أو المجني عليه، أو في غرف الدردشة، أو في المواقع الإلكترونية التي سبق وزارها كلّ منهما. فالأدلة الرقمية التي تنتج عن هذا الفحص التقني تبقى هي رأس الخيط الذي يوصل إلى تسلسل ما حدث فعلاً.

---

(1) الغرفة الجنائية أساس 577، قرار 711 تاريخ 1968/10/30، مجموعة القواعد القانونية في القضايا الجزائية من عام 1949 وحتى 1968، الطبعة الأولى، 1969، القاعدة رقم 79، ص40.

(2) الغرفة الجنائية أساس 902، قرار 794 تاريخ 1968/1/26، مجموعة القواعد القانونية 1968، القاعدة رقم 83، ص 42.

وغني عن البيان أن ما ينطبق على جريمة الاحتيال عبر الإنترنت في مجال الإثبات، ينطبق أيضاً على مختلف جرائم العالم الافتراضي.

وبناءً على تسلسل هذه الأفكار، سوف نقسم هذا الفصل إلى المبحثين التاليين:

المبحث الأول: طرق الإثبات التقليدية.

المبحث الثاني: طرق الإثبات المستحدثة (الدليل الرقمي).

# المبحث الأول
# طرق الإثبات التقليدية

لم يَضمر الدليل التقليدي في عصر المعلومات والتكنولوجيا. فمع أن الدليل التقليدي ليس له تلك القوة المعروفة في إثبات جرائم العالم المادي، إلاّ أنه يلعب دوراً لا غنى عنه في إطار جريمة الاحتيال عبر الإنترنت وسائر جرائم العالم الافتراضي، فالشهادة والقرائن والاعتراف والدليل الكتابي والخبرة، هي من الأدلة التي حافظت على وجودها في عصر الطفرة التكنولوجية والمعلوماتية التي نعيشها في هذه الآونة.

وبناء على ذلك، سوف نلقي الضوء على دور طرق الإثبات التقليدية في إثبات جريمة الاحتيال عبر الإنترنت من خلال المطالب التالية:

المطلب الأول: الشهادة.

المطلب الثاني: القرائن.

المطلب الثالث: الاعتراف.

المطلب الرابع: الدليل الكتابي.

المطلب الخامس: الخبرة.

# المطلب الأول

# الشـهادة

لا بدَّ لنا قبل التطرق للشهادة في جريمة الاحتيال عبر الإنترنت من أن نلقي الضوء على الأحكام العامة للشهادة.

## أولاً– الأحكام العامة للشهادة:

سنتناول من خلال هذه الأحكام، تعريف الشهادة وأنواعها، وشروطها، وسلطة المحكمة في تقديرها.

### أ–تعريف الشهادة وأنواعها:

الشهادة "تقرير يصدر عن شخص في شأن واقعة عاينها بحاسة من حواسه.[1]".

والشهادة يمكن أن تكون **مباشرة**، عندما يعاين الشاهد الواقعة بحواسه الشخصية، مثل المعاينة عن طريق البصر، كأن يروي الشاهد ما رآه بعينه، أو عن طريق السمع، كأن يروي ما سمعه بإذنه، أو عن طريق الشم، كأن يروي أنه شم رائحة المخدرات، أو عن طريق الحواس الأخرى كاللمس والذوق.

وقد تكون الشهادة **غير مباشرة**، وتسمى الشهادة السماعية أو شهادة النقل، وهي تفترض رواية الشاهد عن غيره، فهو لم يعاين الواقعة بنفسه، وإنما سمع غيره يذكر معلومات بشأنها، وهذه الشهادة يغلب أن تكون أقل قيمة من الشهادة المباشرة، ولكن يجوز للقاضي أن يبني عليها حكمه إذا اقتنع بها [2].

---

(1) د.محمود نجيب حسني: شرح قانون الإجراءات الجنائية,المرجع السابق، ص 441.

(2) د.محمود نجيب حسني: شرح قانون الإجراءات الجنائية,المرجع السابق، ص 441. ويرى الدكتور حسن الجوخدار بأن الشهادة غير المباشرة لا تكفي وحدها لبناء الحكم, فهي لا تصل إلى مرتبة الدليل، المرجع السابق، الجزء الثاني، ص 176.

**ب-الشـــهادة فـــي مرحلـــة التحقيـــق الابتـــدائي والتحقيـــق النهائي(المحاكمة):**

الإثبات بالشهادة طريق مشترك بين التحقيق الابتدائي والتحقيق النهائي، ولكن هناك فروق هامة بينهما لا بدّ من الإشارة إليها:

1- الشهادة تؤدى سراً أمام قاضي التحقيق، فلا يحق لأحد من الخصوم حضورها لصراحة المادة (70) من قانون أصول المحاكمات الجزائية. أما أمام المحاكم فالشهادة تؤدى بصورة علنية. والسرية في مرحلة التحقيق ضرورية من أجل عدم التأثير على الشهود، وطمس معالم الجريمة[1].

2- اختيار الشهود في مرحلة التحقيق الابتدائي من حق قاضي التحقيق ومن حق قاضي الإحالة، وللخصوم حق إرشاد المحقق إلى شهودهم، لكنه هو الذي يستدعيهم ويستدعي سواهم إذا شاء. أما في مرحلة التحقيق النهائي، فإن دعوة الشهود من حق الخصوم والنيابة العامة، أما المحكمة فيحق لها ذلك على سبيل الاستثناء[2].

3- الشهادة المؤداة أمام قاضي التحقيق لا تعتبر من عناصر القناعة في المحاكم، فهي لتهيئة الإضبارة لتكون جاهزة أمام محاكم الأساس. أما الشهادة أمام المحاكم فهي أحد الأدلة التي يمكن أن تستند المحكمة إليها في إصدار الحكم[3].

4- يستمع قاضي التحقيق حسب المادة (74) إلى الممنوعين من الشهادة أمام المحاكم، كأصول المتهم وفروعه، والمخبرين الذين يمنحهم القانون

---

(1) د.عبد الوهاب حومد: أصول المحاكمات الجزائية,المرجع السابق، ص575.

(2) المواد 74 ,282,283,266,147 من قانون أصول المحاكمات الجزائية. د.عبد الوهاب حومد: أصول المحاكمات الجزائية,المرجع السابق، ص 575 و576.

(3) د.عبد الوهاب حومد: أصول المحاكمات الجزائية,المرجع السابق، ص576.

مكافأة مالية على الإخبار، في حين أن شهادة هؤلاء باطلة أمام المحاكم، إلاّ إذا لم يعترض عليها النائب العام أو المدعي الشخصي[1].

## ج-شروط الشهادة:

حتى تكون الشهادة دليلاً يمكن أن يركن إليه القاضي في الإثبات، لا بدّ أن تتوفر فيها الشروط التالية[2]:

### 1-التمييز:

لا بدّ للشاهد حتى يكون أهلاً للشهادة أن يكون قد بلغ الخامسة عشرة من عمره وقت أداء الشهادة، ويجوز الاستماع إلى شهادة الذين لم يبلغوا هذه العمر على سبيل المعلومات، ودون تحليفهم اليمين (المادة 81).

### 2-تحليف اليمين:

أوجب قانون أصول المحاكمات الجزائية في المواد /77 و 192 و286/ تحليف الشاهد اليمين، بأن يشهد بواقع الحال، دون زيادة أو نقصان، فإذا لم يتم تحليف الشاهد هذه اليمين، تكون شهادته باطلة، ولا يجوز الاستناد إليها، لأن اليمين من متعلقات النظام العام.

### 3-ألا يكون الشاهد من الممنوعين من أداء الشهادة:

قدر المشرع أن هناك بعض الأشخاص لا تتوفر فيهم الضمانات الكافية لأداء الشهادة، وهؤلاء الأشخاص الممنوعون من الشهادة حسب المادتين 193 و292 هم:

- أصول المتهم وفروعه.

---

(1) المواد 74 و 81 و 193 و 292 من قانون أصول المحاكمات الجزائية. د.عبد الوهاب حومد: أصول المحاكمات الجزائية,المرجع السابق، ص577.

(2) د.حسن الجوخدار: المرجع السابق، الجزء الثاني، ص 177- 178. د.عبد الوهاب حومد: أصول المحاكمات الجزائية,المرجع السابق، ص596 وما بعدها.

- إخوته وأخواته.
- ذوو القرابة الصهرية الذين هم في هذه الدرجة.
- الزوج والزوجة ولو بعد الطلاق.
- المخبرون الذين يمنحهم القانون مكافأة مالية على الإخبار.

ولكن إذا سمعت شهادتهم ولم يعترض عليها النائب العام أو المدعي الشخصي أو المتهم فلا تكون باطلة، أما إذا تمّ الاعتراض بعد سماعهم فلا يؤثر ذلك على صحة شهاداتهم[1].

ومن الجدير بالذكر بأن محكمة النقض أجازت سماع المدعي الشخصي بصفته شاهد في الدعوى العامة، كما أجازت سماع شهادة أصول المدعي الشخصي وفروعه وإخوته وأخواته[2].

## د-سلطة المحكمة في تقدير الشهادة:

تخضع الشهادة إلى تقدير قاضي الموضوع، فإن شاء أخذ بها، وإن شاء رفضها، فيحق للقاضي أن يقتنع بشهادة شاهد واحد، وله أن يرفض شهادة عدة شهود، إذا لم يقتنع بها، ويجوز له تجزئة الشهادة، فيأخذ ما يطمئن إليه، ويطرح ما دون ذلك، بشرط أن يبين الأسباب التي دعت إلى ذلك.

ولا تخضع محكمة الموضوع لرقابة محكمة النقض في تقدير الشهادة، إلاّ إذا كان تقديرها للشهادة لا يأتلف مع المنطق، ولا يسلم به العقل[3].

---

(1) الغرفة الجنحية أساس 442، قرار 447 تاريخ 1954/3/29، مجموعة القواعد القانونية، القاعدة رقم 34، ص20.

(2) الغرفة الجنحية أساس 2333، قرار 2429 تاريخ 1968/10/13. الغرفة الجنحية أساس 1845، قرار 1621 تاريخ 1967/6/13، مجموعة القواعد القانونية، القاعدتان 32 و 33، ص19-20.

## ثانياً–الشاهد في الجريمة المعلوماتية:

من الممكن أن يكون الشاهد في الجريمة المعلوماتية صاحب الخبرة والتخصص في تقنية وعلوم الحاسوب، الذي تكون لديه معلومات جوهرية هامة للولوج إلى نظام المعالجة الآلية للبيانات، إذا كانت مصلحة التحقيق تقتضي ذلك. ويطلق على هذا النوع من الشهود مصطلح (الشاهد المعلوماتي)، تمييزاً له عن الشاهد التقليدي[1].

ويرى الفقه أن الشاهد المعلوماتي يمكن أن يكون من إحدى الطوائف التالية[2]:

- القائم على تشغيل الحاسوب.
- المبرمج.
- المحلل، وهو الذي يقوم بتحليل خطوات البرنامج وتجميعها.
- مدير النظام، وهو الذي يوكل إليه أعمال الإدارة في النظم المعلوماتية. ويدخل ضمن هذه الطائفة مدخل البيانات والمعلومات.

وتطبيقاً لذلك، فإن الشهادة في إطار جريمة الاحتيال عبر الإنترنت، من الممكن أن يدلي بها مدخلو البيانات العاملون في إحدى الشركات، الذين تمّ تكليفهم بإرسال الرسائل الإلكترونية إلى الزبائن، إذا تبيّن فيما بعد أن الشركة

---

(3) جناية أساس 344 , قرار 410 تاريخ 1961/10/21، مجموعة القواعد القانونية، القاعدة رقم 35، ص20. د.عبد الوهاب حومد: أصول المحاكمات الجزائية,المرجع السابق، ص 618 وما بعدها. د.حسن الجوخدار: المرجع السابق، الجزء الثاني، ص 186–187.

(1) د.سليمان أحمد فضل: المرجع السابق، ص 332. المستشار الدكتور عبد الفتاح بيومي حجازي: مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، المرجع السابق، ص339.

(2) د.سليمان أحمد فضل: المرجع السابق، ص 333. المستشار الدكتور عبد الفتاح بيومي حجازي: مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، المرجع السابق، ص 340.

كانت تقصد من وراء هذه الرسائل القيام بخداع الزبائن والاستيلاء على أموالهم، دون علم العاملين في الشركة.

وإذا كان الرأي السائد في الفقه هو عدم إجبار المشتبه به على الكشف عن الشفرات، أو كلمات السر الخاصة بالدخول إلى نظام المعلومات، أو عدم إجباره على تقديم البرمجية اللازمة لوقف نشاط الفيروس، لأنه لا يجوز إلزام الشخص بتقديم الأدلة على نفسه[1]، فإن التساؤل الذي يثور في هذا المجال هو: **ما مدى التزام الشاهد في جرائم الحاسوب والإنترنت بتقديم مثل هذه المعلومات؟**

ذهب الفقه في إجابته على هذا السؤال إلى اتجاهين، هما[2]:

## الاتجاه الأول:

يرى أصحاب هذا الاتجاه أنه لا يجوز إكراه الشاهد لحمله على الإفصاح عن كلمات المرور السرية، أو الكشف عن شفرات تشغيل النظام. وهذا هو رأي الفقه في ألمانيا وتركيا.

## الاتجاه الثاني:

يرى أصحاب هذا الاتجاه أنه من بين الالتزامات التي تقع على عاتق الشاهد، الإفصاح عن كلمات السر أو الشفرات الخاصة. ومن أنصار هذا الرأي الفقه الفرنسي، ومشروع قانون الحاسوب في هولندا، وقانون الإجراءات الجنائية اليوناني، والقانون الإنكليزي.

---

(1) د.سليمان أحمد فضل: المرجع السابق، ص 334. د.جميل عبد الباقي الصغير: أدلة الإثبات الجنائي التكنولوجيا الحديثة، دار النهضَة العربية، القاهرة، 2002، ص 104 وما بعدها.

(2) د.سليمان أحمد فضل: المرجع السابق، ص 335–336. المستشار الدكتور عبد الفتاح بيومي حجازي: مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، المرجع السابق، ص35. د.علاء عبد الباسط خلاف: المرجع السابق، ص 443.

**والباحث يؤيد الرأي الأول،** لأن القواعد الأصولية في سورية لا تلزم الشاهد بالإدلاء بمثل هذه المعلومات، وإن كانت تلزمه بتلبية مذكرة الدعوة، والحضور أمام القضاء تحت طائلة العقوبة، ما لم يبد عذراً مشروعاً.

## ثالثاً- الشهادة عبر الإنترنت:

يطلق على هذا النوع من الشهادة اسم "**الشهادة الإلكترونية الفورية**". وتفترض هذه النوعية من الشهادة حصولها في مرحلة التحقيق النهائي أمام محكمة الموضوع، حيث يكون الشاهد غير حاضرٍ مادياً أو جسدياً أمام المحكمة، وإنما يتم سماع شهادته عبر الإنترنت بشكل سمعي ومرئي[1].

والشاهد في هذه الحالة يبرز في هيئته الكاملة، فيبدو كما لو كان حاضراً، حيث تظهر للمحكمة ردود أفعاله الطبيعية عندما توجه له الأسئلة، الأمر الذي يفسح المجال أمام المحكمة لتقدير قيمة هذه الشهادة.

والقضاء الأمريكي قبل ظهور خدمات الدارات الاتصالية المتكاملة من مغلقة ومفتوحة[2]، كان يرفض بشدة إمكانية إجراء اتصال صوتي بين الشاهد وجلسة المحاكمة. أما بعد ظهور هذه الخدمة، فقد أخذ القضاء الأمريكي بها. كما رحّب الفقه الإجرائي بالشهادة الإلكترونية الفورية. ففي إحدى القضايا في الولايات المتحدة الأمريكية، قبلَ القاضي طلب الادعاء العام بسماع شاهد عبر دارة تلفزيونية مغلقة، لأن الشاهد كان موضوعاً في برنامج حماية الشهود، شريطة أن يكون حضور الشاهد عبر هذه الدارة كما لو كان حاضراً بالفعل، بحيث يكون كل ما يدور في الجلسة مرئياً للشاهد، وبالمقابل يجب أن يكون

---

(1) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت,المرجع السابق، ص 955.

(2) الدارة المغلقة تعني انغلاق الدارة الاتصالية بين جهتين فأكثر، يتم تحديدها مسبقاً، بحيث لا يستطيع الغير الدخول إلى هذه الدارة . د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت,المرجع السابق، ص 956 الهامش.

الشاهد مرئياً للمحكمة. وقد قررت المحكمة الفيدرالية العليا قبول نظام الشهادة عن بعد عبر الدارات المغلقة[1].

ويميز القضاء الأمريكي بين نوعين من الشهادة الإلكترونية المرئية، هما:

**النوع الأول** : الشهادة المرئية ذات الاتجاه الواحد. وفي هذه الحالة لا يرى الشاهد حين يدلي بشهادته سوى الكاميرا المسلطة عليه، فالرؤية تكون من طرف واحد وهو طرف المحكمة.

**النوع الثاني:** الشهادة المرئية ذات الاتجاهين. وفيها يرى الشاهد قاعة المحكمة، وبالمقابل يراه كل من في المحكمة.

واختيار أي من هاتين الشهادتين يخضع لتقدير المحكمة، بناءً على الأسباب التي تطرحها جهة الادعاء أو الدفاع[2].

## رابعاً– مدى إمكانية اللجوء إلى الشهادة عبر الإنترنت في ظل التشريع السوري:

تستند الأحكام الجزائية إلى قناعة القاضي الشخصية، وهذه القناعة يجب أن تستمد من الوقائع المثارة أمام المحكمة، فالأحكام تصدر بناء على ما يسمع القضاة من أقوال الخصوم والشهود، وما ترى أعينهم في قاعة المحكمة، فلا يجوز للمحكمة مبدئياً الاستناد إلى ضبوط الضابطة العدلية، ولا إلى محاضر التحقيق الابتدائي[3]. وهذا ما يعرف بمبدأ الشفوية الذي أخذ به المشرع السوري بالمادة 176 من قانون أصول المحاكمات الجزائية، التي نصت على ما يلي:

---

(1) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت,المرجع السابق، ص 956.

(2) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت,المرجع السابق، ص 957.

(3) د.عبد الوهاب حومد: أصول المحاكمات الجزائية,المرجع السابق، ص 823.

(لا يجوز أن يعتمد إلاّ على البيّنات التي قدمت أثناء المحاكمة، وتناقش فيها الخصوم بصورة علنية.).

وبناءً على ذلك، فإن على الشهود أن يدلوا بشهاداتهم أمام المحكمة بصورة شفهية، سواء أشهدوا أمام قاضي التحقيق أم لم يشهدوا، وعلى الخبراء أيضاً أن يشرحوا تقاريرهم بصورة شفهية أمام المحكمة، وعلى موظفي الضابطة العدلية أن يشهدوا أمام المحكمة إذا دُعوا إلى ذلك، ويشرحوا شفاهاً الظروف التي نظّموا فيها ضبوطهم. ومن ثم فلا يجوز الاكتفاء بتلاوة المحاضر التي تتضمن أقوال الشهود السابقة، إلاّ إذا تعذّر سماع هؤلاء الشهود أمام المحكمة[1]. وهذا ما استقر عليه اجتهاد محكمة النقض السورية حيث قالت: "يمكن الاكتفاء بتلاوة إفادات الشهود المدلى بها أمام المحقق القضائي، في حال عدم الاستدلال عليهم، أو تعذر سماعهم لأي سبب من الأسباب"[2].

**والباحث** لا يرى مانعاً من اللجوء إلى الشهادة الإلكترونية عبر الإنترنت في حال تعذر سماع الشاهد أمام المحكمة، كوجوده مثلاً خارج القطر، إذا توفرت الشروط التالية:

1- أن يتعذر حضور الشاهد مادياً أمام المحكمة.
2- أن تكون الشهادة على قدر من الأهمية.
3- أن يتم سماع الشهادة الإلكترونية بحضور خبير أو أكثر لضمان انغلاق الدارات الاتصالية مع الشهود.
4- أن يتم تبليغ الشاهد بأي وسيلة كانت قبل موعد الجلسة بمدة معقولة تقدرها المحكمة.

---

(1) د.عبد الوهاب حومد: أصول المحاكمات الجزائية,المرجع السابق، ص 824.

(2) الغرفة الجنحية أساس 225، قرار 372 تاريخ 1968/3/6، مجموعة القواعد القانونية، القاعدة 147، ص72.

وعلى ضوء ذلك، **فالباحث يقترح** على المشرع السوري أن يأخذ بأسلوب الشهادة الإلكترونية عبر الإنترنت ضمن الشروط المذكورة، لإثبات الجرائم الإلكترونية المنصوص عليها في مشروع قانون الجريمة الإلكترونية فقط، لأن الطبيعة العالمية لجرائم الإنترنت تثير في كثير من الأحيان مسألة سماع أقوال الشهود الموجودين خارج القطر. كما أن سماع الشاهد عبر الإنترنت بصورة سمعية ومرئية يساعد المحكمة على تقدير قيمة الشهادة، بصورة أفضل بكثير من الاكتفاء بتلاوة أقوال الشاهد السابقة –في حال وجودها– أمام هيئة المحكمة عندما يتعذر حضوره لأي سبب كان. وبهذا التطبيق الضيق يتم الحفاظ على إجراءات سماع الشهود المنصوص عليها في القواعد العامة.

# المطلب الثاني

# القرائــن

قبل التصدي لدور القرائن في إثبات جريمة الاحتيال عبر الإنترنت، لا بد لنا من التعرض للأحكام العامة للقرائن.

## أولاً- الأحكام العامة للقرائن:

سنتناول من خلال هذه الأحكام، تعريف القرائن، وأنواعها، وقوتها في الإثبات.

### أ-تعريف القرائن:

القرينة هي: "استنتاج الواقعة المطلوب إثباتها من واقعة أخرى قام عليها دليل إثبات"[1].

والقرائن تعدّ من طرق الإثبات غير المباشرة، باعتبارها لا ترد على الوقائع المطلوب إثباتها، في حين أن طرق الإثبات الأخرى كالشهادة أو الاعتراف مثلاً، هي أدلة مباشرة لأنها ترد على هذه الوقائع.

والقرائن لها أهمية خاصة في الإثبات، إذ إن بعض الوقائع يستحيل أن يرد عليها إثبات مباشر، فإذا اقتصر الإثبات على الأدلة المباشرة لما كان من الممكن الفصل في الدعاوى، فالقرائن تمكن من إثبات بعض الوقائع عن طريق وقائع أخرى ذات صلة سببية ومنطقية بها. ومثال القرائن في الدعوى الجزائية أن يُتهم شخص بسرقة من منزل، ولا يكون على هذه الجريمة شهود، وهو غير معترف بها، ولكن ترفع من باب المنزل بصمات تعود له، وتضبط المسروقات

---

(1) د.محمود نجيب حسني: شرح قانون الإجراءات الجنائية,المرجع السابق، الطبعة الثانية، ص487.

في حيازته، فتكون البصمات وضبط المسروقات لديه قرينتين على أنه هو الذي قام بالسرقة[1].

## ب-أنواع القرائن وقوتها بالإثبات:

لم يبحث قانون أصول المحاكمات الجزائية في القرائن، ولكن قانون البيّنات ذكر نوعين منها، هما:

### 1-القرائن القانونية:

وهي القرينة التي نصّ عليها القانون، وتغني من تقررت لمصلحته عن أية طريقة أخرى من طرق الإثبات[2]، ويلزم القاضي بالأخذ بها، لأنها افتراض قانوني يرتبه المشرع على واقعة معينة.

وتقسم القرائن القانونية بدورها إلى نوعين، هما:

**النوع الأول- القرينة القانونية القاطعة أو المطلقة[3]:**

وهي القرائن التي لا يجوز إثبات عكسها. ومثال ذلك ما نصت عليه المادة الثانية من قانون الأحداث رقم /18/ لعام 1974، والمعدل بالمرسوم التشريعي رقم /52/ لعام 2003 حيث قالت: (لا يلاحق جزائياً الحدث الذي لم يتم العاشرة من عمره حين ارتكاب الفعل). فعدم إتمام العاشرة من العمر يشكّل قرينة قانونية قاطعة على عدم التمييز، ومن غير الجائز إثبات عكسها، ولو أقام المضرور الأدلة على أن الحدث كان مميزاً ومدركاً لما يقوم به.

ولا يجوز أيضاً قبول دليل يناقض الحكم المبرم، لأن هذا الحكم هو عنوان الحقيقة، وله قوة القضية المقضية.

---

(1) د.محمود نجيب حسني: شرح قانون الإجراءات الجنائية,المرجع السابق، الطبعة الثانية، ص487-488.

(2) المادة /89/ من قانون البيّنات.

(3) د.عبد الوهاب حومد: أصول المحاكمات الجزائية,المرجع السابق، ص 630. د.حسن الجوخدار: المرجع السابق، الجزء الثاني، ص189.

**النوع الثاني- القرائن القانونية البسيطة أو المؤقتة[1]:**

وهي القرائن التي تقرر حالة قانونية بصورة مبدئية، ولكن يجوز للمضرور منها أن يقيم الدليل على عكس ما تضمنته. ومثال ذلك قرينة الدفاع الشرعي التي نصت عليها المادة (549) من قانون العقوبات، وهي حالة قتل صاحب المنزل للشخص الذي دخل إلى منزله ليلاً. فقد عدّ المشرع هذا الفعل من قبيل الدفاع الشرعي، لكنه سمح صراحة أن تزول دلالة هذه القرينة إذا ثبت أن الدخول كان لغرض آخر، أو أن صاحب البيت كان يعرف ذلك.

**2-القرائن القضائية أو الموضوعية[2]:**

وهي القرائن التي لم ينص عليها القانون، ويمكن للقاضي أن يستخلصها من ظروف الدعوى وأن يقتنع بأن لها دلالة معينة، ويعود أمر تقديرها للقاضي[3]. ومن أمثلة القرائن القضائية، الأسلحة والثياب والبصمات، وبقع الدم، والشعر، والسم... فكل ما يمكن أن يضبط مع الفاعل وله علاقة بالجريمة يعتبر قرينة على اقترافه الجريمة. ومظاهر الثراء المفاجئ على المدعى عليه قرينة على اختلاسه المال الذي اؤتمن عليه... وغير ذلك.

وقد أكّدت محكمة النقض على أن القناعة الوجدانية للقاضي من الممكن أن تتولّد عن القرائن التي يستخلصها، فقالت: "إن القناعة الوجدانية يمكن أن

---

(1) د.عبد الوهاب حومد: أصول المحاكمات الجزائية,المرجع السابق، ص 631. د.حسن الجوخدار: المرجع السابق، الجزء الثاني، ص 190 .

(2) د.عبد الوهاب حومد: أصول المحاكمات الجزائية,المرجع السابق، ص 633. د.حسن الجوخدار: المرجع السابق، الجزء الثاني، ص190.

(3) المادة /92/ من قانون البيّنات.

تتولّد عن شذرات متفرقة من الظروف والحوادث، بحيث تشكل بمجموعها سلسلة من القرائن الموجبة لقناعة قضاة الموضوع."[1]

## ثانياً– دور القرائن في إثبات جريمة الاحتيال عبر الإنترنت:

يعدّ الدليل الرقمي[2]من فئة القرائن القضائية التي يعود تقدير قيمتها إلى قاضي الموضوع. فمعرفة عنوان الإنترنت الرقمي مثلاً IP address يشير إلى الحاسوب الذي ارتكبت بواسطته الجريمة فقط، ولا يؤدي إلى معرفة الفاعل بدقة، وذلك بخلاف الدليل العلمي الناتج عن تحليل الحمض النووي DNA، أو بصمة الإصبع، وغيرها من الأدلة التي تشير إلى الفاعل الحقيقي بدقة متناهية.

ففي جريمة الاحتيال عبر الإنترنت، تشكل معرفة عنوان الإنترنت الرقمي قرينة قضائية على ارتكاب هذه الجريمة من قبل مالك الحاسوب، ولكن هذه القرينة لا تكفي لبناء منطق الإدانة القائم على اليقين والجزم، ما لم تتوفر أدلة أخرى تؤكّد ارتكاب مالك الحاسوب لهذه الجريمة.

ومن أمثلة الأدلة الرقمية التي يمكن أن يستنتج منها القاضي دلالة معينة، أن يكون للمحتال الذي قام بالاستيلاء على أموال بعض المؤسسات المالية عبر الإنترنت، أسلوبٌ خاصٌ به في بناء برمجيات الاختراق، فيتم القبض عليه لأن أسلوبه أضحى معروفاً من قبل جهات الضبط القضائي، ثم يجري التحقيق معه وتقديمه إلى القضاء على هذا الأساس[3].

---

(1) الغرفة الجنائية أساس 456، قرار 452 تاريخ 1955/6/14، مجموعة القواعد القانونية، القاعدة 41، ص23.

(2) **يقصد بالدليل الرقمي "المعلومات أو البيانات الرقمية المخزنة في الحاسوب أو المنقولة بواسطته، والتي يمكن استخدامها في إثبات أو نفي جريمة ما."**

(3) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت,المرجع السابق، ص 941.

كما أن تفتيش البريد الإلكتروني، أو السجلات الإلكترونية الموجودة في الحاسوب العائد للضحية أو المشتبه به، قد يؤدي إلى استخلاص بعض القرائن القضائية. ومثال ذلك أنه في قضية قتل المدعو "بروبرت دورال" لزوجته، تمّ إثبات عنصر العمد لديه، ومن ثم رفع مستوى الجريمة إلى القتل من الدرجة الأولى، بعد أن تبيّن بنتيجة تفتيش حاسوبه أنه كان يبحث في الإنترنت عن مصطلحات مثل: (قتل– حادث – وفيات– خنق) في وقت سابق على ارتكاب جريمته[1].

وفي قضية أخرى، فقد أثبت الخبير التقني للمحكمة أن الصور الخلاعية الموجودة على حاسوب المدعى عليه قد تمّ تحميلها من الإنترنت، استناداً إلى أن الوقت والتاريخ المبيّن على هذه الملفات يتزامن مع الفترات الزمنية التي دخل بها المدعى عليه إلى شبكة الإنترنت. وقد اقتنعت المحكمة بهذه القرينة وأدانت المدعى عليه[2].

وبناءً على ما تقدم، يمكن القول بأن نظام الإثبات الحر المتبع في قضائنا الجزائي يسمح للقاضي أن يختار ما يشاء من القرائن القضائية لإثبات جريمة الاحتيال عبر الإنترنت، ما دامت هذه القرائن تشكّل القناعة لديه على ارتكاب المدعى عليه لهذه الجريمة.

---

(1) Eoghan Casey, op-cit, P-19.

(2) Eoghan Casey, op-cit, P-104.

# المطلب الثالث

# الاعتـراف

سنتناول في هذا المطلب الأحكام العامة للاعتراف، ثم نشرع في تطبيقها على جريمة الاحتيال عبر الإنترنت.

## أولاً- الأحكام العامة للاعتراف:

تتضمن الأحكام العامة للاعتراف، تعريفه، وأنواعه، وشروطه، والقيمة القانونية له.

### أ-تعريف الاعتراف :

الاعتراف هو: "إقرار المدعى عليه على نفسه بصدور الواقعة الجرمية عنه."[1]

والأصل أن يكون للاعتراف دور حاسم في الدعوى الجزائية، عندما يصدر عن شخص عضّه الندم، فلم يجد سبيلاً أمامه إلاّ الاعتراف إلى العدالة بحقيقة ما اقترفت يداه، طلباً لراحة النفس، وتسكيناً لتأنيب الضمير.

إلاّ إن الاعتراف قد يكون كاذباً في بعض الأحيان لعدة اعتبارات: فقد يصدر الاعتراف إشباعاً لنزوات المدعى عليه، كمن يعترف بارتكابه جريمة خطيرة اهتم بها الرأي العام، كي تتحدث عنه وسائل الإعلام. وقد يصدر الاعتراف نتيجة وهم المدعى عليه، كمن يتوهم بأنه يتعاطى المخدرات، ثم يتبيّن بنتيجة التحليل أن المادة دوائية وليست من أنواع المخدرات. وقد يصدر

---

(1) د.محمود نجيب حسني: شرح قانون الإجراءات الجنائية,المرجع السابق، ص460- كما عرّفت المادة /93/ من قانون البيّنات الإقرار بأنه" هو إخبار الخصم أمام المحكمة بحق عليه لآخر".

الاعتراف دافع إنقاذ المجرم الحقيقي، كما لو اعترف الابن بارتكابه الجريمة كي ينقذ والده من العقوبة[1].

أما الوسيلة إلى الوصول للاعتراف، فهي حسب تشريعنا استجواب المدعى عليه. والقانون لم يحدّد أسلوباً خاصاً لإجراء الاستجواب، بل ترك الباب مفتوحاً أمام القضاة لاختيار الأسلوب الأفضل في إدارة الاستجواب. ونظراً لأهمية الاستجواب فقد منع القانون القضاة من إنابة الشرطة في استجواب المدعى عليه لخطورته[2].

## ب-أنواع الاعتراف:

قد يكون **الاعتراف قضائياً**، عندما يصدر عن المدعى عليه في مجلس القضاء أثناء النظر في الدعوى المتعلقة بالجريمة، وقد يكون **الاعتراف غير قضائي**، عندما يصدر عن المدعى عليه خارج مجلس القضاء، أو في مجلس القضاء ولكن في غير الدعوى المتعلقة بالجريمة[3]، كأن يعترف المشتبه به أمام الشرطة أو أمام شخص آخر بارتكاب الجريمة. أما فيما يتعلق بمدى قوته في الإثبات، فإن الاعتراف غير القضائي هو أضعف من الاعتراف القضائي.

## ج-شروط الاعتراف:

يشترط لصحة الاعتراف توفر الشروط التالية[4]:

---

(1) د.محمود نجيب حسني: شرح قانون الإجراءات الجنائية,المرجع السابق، ص464. د.عبد الوهاب حومد: أصول المحاكمات الجزائية,المرجع السابق، ص 551.

(2) المادتان /48 و 101/ من قانون أصول المحاكمات الجزائية. د.عبد الوهاب حومد: أصول المحاكمات الجزائية,المرجع السابق، ص 554.

(3) المادتان /94 و 95/ من قانون البيّنات.

(4) د.محمود نجيب حسني: شرح قانون الإجراءات الجنائية,المرجع السابق، ص464. د.حسن الجوخدار: المرجع السابق، الجزء الثاني، ص171-173.

1- أن يكون الاعتراف صادراً عن شخص يتمتع بالوعي أو الإدراك، فلا يصح الاعتراف الصادر عن المجنون أو المعتوه أو المنوّم مغناطيسياً.

2- أن يكون الاعتراف صادراً عن إرادة حرة، فلا يصح الاعتراف الصادر تحت وطأة الإكراه المادي، كالضرب والتعذيب، ولا يصح أيضاً الاعتراف الصادر تحت وطأة الإكراه المعنوي، كالضغط النفسي والخديعة والتهديد.

ويرى الفقه أن سبب عدم جواز تحليف المدعى عليه اليمين يرجع إلى أن اليمين تنطوي على شيء من التعذيب النفسي[1].

وقد أكّدت محكمة النقض على أن الاعتراف الصادر عن صاحبه تحت تأثير الإكراه المادي أو المعنوي يجب إهماله، لأن المعترف يكون هنا معيب الإرادة، مضطرب التفكير[2].

3-يجب أن يكون الاعتراف صريحاً، فالقانون لا يعتد بالاعتراف الضمني. فلا يعدّ اعترافاً ما يمكن استنتاجه من تصرفات المدعى عليه، فسكوته لا يعدّ إقراراً منه بما نُسب إليه، وكذلك فراره أو تصالحه مع المدعي. ومتى كان الاعتراف صريحاً، فلا فرق إذا كان خطياً أو شفهياً.

## د-القيمة القانونية للاعتراف:

الاعتراف الصحيح هو مجرد دليل إثبات في الدعوى الجزائية، ويخضع تقديره لقاضي الموضوع حسب قناعته الشخصية، فله أن يأخذ به، وله أن يهمله.

أما الإقرار في الدعوى المدنية، فهو حجة على المقر، ولا يصح مبدئياً الرجوع عنه، ولا تجزئته على صاحبه[3]. وهذا على عكس الإقرار في المسائل

---

(1) د.عبد الوهاب حومد: أصول المحاكمات الجزائية,المرجع السابق، ص 553.

(2) الغرفة الجنائية أساس 237، قرار 426 تاريخ 1968/5/23،مجموعة القواعد القانونية، القاعدة15، ص14.

الجزائية، إذ إنه يمكن للمعترف أن يرجع عنه، وللقاضي في هذه الحالة تقدير قيمة هذا الرجوع، فإذا تبيّن له أن رجوعه محق، أسقط الاعتراف، وإلاّ فإنه لا يعتد بهذا الرجوع، ويحكم حسب الاعتراف[1]. كما أن مبدأ عدم تجزئة الاعتراف لا يطبق في المسائل الجزائية، فللقاضي أن يأخذ من اعتراف المدعى عليه ما يقتنع به، ويترك ما يشك في صحته، وليس للمدعى عليه أن يحتج على ذلك بأن اعترافه وحدة متماسكة[2].

## ثانياً- الاعتراف في جريمة الاحتيال عبر الإنترنت:

لا تختلف أحكام الاعتراف في جريمة الاحتيال عبر الإنترنت عن الأحكام العامة المشار إليها للاعتراف في الجرائم التقليدية، فلا يكفي مجرد اعتراف المدعى عليه بارتكابه جريمة تحويل الأموال بطريقة غير مشروعة عن طريق اختراق النظام المعلوماتي العائد لأحد المصارف عبر الإنترنت، بل يجب أن يحدّد المعترف الكيفية التي تمّ بها الاختراق، ومن ثم يجب أن يتطابق هذا الاعتراف مع الأسلوب الحقيقي الذي تمّ فيه هذا الاختراق فعلاً والبرمجية التي استخدمت في ذلك. فإذا تبيّن أن المعترف ليس لديه أساساً أية معلومات عن طريقة استخدام الحاسوب والولوج إلى الإنترنت، فلا يمكن الاستناد إلى اعترافه وإدانته بهذا الجرم.

ولذلك يمكن لجهات التحقيق أن تلجأ إلى أسلوب تمثيل الجريمة، من أجل التأكد من تطابق أقوال المدعى عليه مع الكيفية الحقيقية التي ارتكبت بها

---

(3) المواد من 96 وحتى 102 من قانون البيّنات.

(1) الغرفة الجنائية أساس 1037، قرار 956 تاريخ 1982/10/23، مجموعة قانون أصول المحاكمات الجزائية، تجميع أديب استانبولي، الجزء الأول، الطبعة الثالثة، 1994، القاعدة 704، ص 752. د.عبد الوهاب حومد: أصول المحاكمات الجزائية,المرجع السابق، ص 570.

(2) الغرفة الجنائية أساس 1126، قرار 1131 تاريخ 1982/10/27، مجموعة قانون أصول المحاكمات الجزائية، الجزء الأول، القاعدة 701، ص 750.

الجريمة، حيث يقوم الجاني مثلاً بتعريف جهة التحقيق على الأسلوب الذي اتبعه في عملية الاختراق، والطريقة التي قام بها بتحويل الأموال، وهذا ما يعرف بـ (الاعتراف العملي)[1].

ومن أمثلة القضايا التي بدأت بالاعتراف، أن كلاً من "وليام غريس" و"برادنودن ويلسن"، اعترفا باختراق أنظمة المحكمة في ولاية كاليفورنيا بهدف تعديل سجلات هذه المحكمة. وقد تضمّن اعتراف المدعو "ويلسن" قيامه بتعديل السجلات المتعلقة بتهمه السابقة التي سجلت ضده (تعاطي المخدرات، وحيازة الأسلحة، والقيادة تحت تأثير الكحول وغيرها)، كما قام "ويلسن" بتعديل بعض سجلات المحكمة المتعلقة بأصدقائه وأفراد عائلته.

وقد أكّد "ويلسن" بأنه حصل على كلمة سر النظام عن طريق شريكه المدعو "غريس" الذي كان يعرف كلمة السر نتيجة عمله السابق كمستشار خارجي في قسم الشرطة المحلية.

وأشارت التحقيقات التي أجريت بعد اعترافهما واعتقالهما بأنهما تمكنا فعلاً من الوصول غير المصرح به إلى العديد من الحواسيب، وتغيير سجلات المحكمة، وتعديل قراراتها، واستعادة المذكرات، وقراءة البريد الإلكتروني العائد لأغلب الموظفين. وقد حكم على المذكورين بالسجن لمدة تسع سنوات[2].

وفي إحدى القضايا الحديثة في سورية التي استندت إلى الاعتراف، أن موظفة في أحد المصارف بدأت تتلقى اتصالات هاتفية من داخل القطر ومن خارجه، حيث كان المتصلون يوجهون لها الكلام المنافي للأخلاق، ويطلبون منها ممارسة الجنس معها مقابل المنفعة المادية. وعند سؤالها لأحد المتصلين عن كيفية الحصول على رقمها، أخبرها بأنه حصل عليه من أحد المواقع الإلكترونية التي تروّج للدعارة. ولدى قيام المجني عليها بالدخول إلى هذا

---

(1) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت,المرجع السابق، ص947.

(2) Eoghan Casey, op-cit, P-4.

الموقع، وجدت رقم جوالها عليه، وإلى جانبه الاسم المعروفة به في وظيفتها. وهنا حصرت شبهتها بزميل لها في المصرف، لأن رقم جوالها الموجود على الإنترنت هو رقم جديد لا يعرفه سوى هذا الزميل. وعندها قامت بتقديم شكوى إلى مدير المصرف.

ولدى قيام مدير المصرف بالتحقيق مع هذا الزميل، اعترف أمامه بارتكابه هذه الجريمة، لأنه سبق وأن تقدم لخطبتها فرفضت.

ثم تبيّن بنتيجة التحقيقات الأولية التي قامت بها الشرطة أن المشتبه به دخل إلى الإنترنت من حاسوب المصرف، ومن ثم قام بالدخول إلى موقع ترويج الدعارة، حيث وضع اسم زميلته ورقمها على هذا الموقع، باعتباره يعمل مهندساً في قسم المعلوماتية العائد لهذا المصرف[1].

ومما تقدم، نجد أن مجرد الاكتفاء بالاعتراف النظري في ارتكاب جرائم الإنترنت أمر يرفضه المنطق السليم، ما لم يقترن بالاعتراف العملي الذي يؤكد صحة ما جاء على لسان المدعى عليه.

---

(1) ضبط شرطة الحميدية رقم 1371 تاريخ 2008/10/12، مسجل بسجلات النيابة العامة بدمشق برقم موجوداً 18367/م تاريخ 2008/10/13.

# المطلب الرابع
# الدليل الكتابي

يشمل الإثبات بالدليل الكتابي في المسائل الجزائية، ثلاثة أنواع من الأدلة الكتابية، هي[1]:

1- الضبوط.

2- الأوراق التي تشكّل جسم الجريمة، كالأوراق المزورة أو العملة المزيفة أو الرسالة التي تحمل تهديداً للمجني عليه، وغيرها.

3- الأوراق الخاصة الصادرة عن المدعى عليه، والتي تتضمّن اعترافاً منه، كاعترافه بكيفية ارتكاب الجريمة أو التخطيط لها.

وسنقتصر في هذا المطلب على دراسة النوع الأول فقط، أي الضبوط، أما النوعين الثاني والثالث، فسوف نتناول البحث فيهما لاحقاً في إطار حجية الدليل الرقمي، لأنهما يعدّان من مستخرجات الحاسوب في مجال جريمة الاحتيال عبر الإنترنت.

## أولاً- تعريف الضبط أو المَحْضَر:

الضبط هو: "المحرر الذي يدوّنه الموظف المختص،لإثبات ارتكاب الجرائم أو الإجراءات التي اتخذت بشأنها، وذلك وفق الشروط والأشكال التي حدّدها القانون"[2].

## ثانياً- القيمة الإثباتية للضبوط:

فرّق قانون أصول المحاكمات الجزائية بين ثلاثة أنواع من الضبوط، من حيث قوتها في الإثبات، هي:

---

(1) د.عبد الوهاب حومد: أصول المحاكمات الجزائية,المرجع السابق، ص 638 وما بعدها. د.حسن الجوخدار: المرجع السابق، الجزء الثاني، ص187.

(2) د.محمود نجيب حسني: شرح قانون الإجراءات الجنائية, المرجع السابق، ص484.

**النوع الأول: الضبوط التي يعمل بها ما لم يثبت تزويرها.** وقد نصت المادة /182/من قانون أصول المحاكمات الجزائية على هذا النوع من الضبوط بقولها:

(لا يسوغ تحت طائلة البطلان إقامة البيّنة الشخصية على ما يخالف أو يجاوز مضمون المحاضر التي يوجب القانون اعتبارها والعمل بها حتى ثبوت تزويرها.).

وهذه الضبوط هي أقوى أنواع الضبوط من حيث الإثبات، لأن القاضي ملزم بالأخذ بها، إلاّ إذا استطاع المدعى عليه إثبات تزويرها. والعلة من إعطاء هذه الضبوط تلك القوة في الإثبات، هي أن هناك بعض الجرائم يتعذر إثباتها بغير هذه الوسيلة. ويدخل في هذا النوع، الضبوط التي ينظمها موظفو ضابطة الحراج[1]، والضبوط التي ينظمها موظفو الضابطة الجمركية[2]، وضبوط جلسات المحاكم ونصوص الأحكام[3].

**النوع الثاني: الضبوط التي يعمل بها حتى يثبت العكس.** وقد نصت المادة /178/ من قانون أصول المحاكمات الجزائية على هذا النوع من الضبوط بقولها:

(1-يعمل بالضبط الذي ينظّمه ضباط الضابطة العدلية ومساعدو النائب العام، في الجنح والمخالفات المكلفون باستثباتها، حتى يثبت العكس.

2-ويشترط في إثبات العكس أن تكون البيّنة كتابية أو بواسطة شهود.).

وهذه الضبوط تسهّل عمل القضاء في إثبات الجرائم الجنحية والمخالفات، ومن ثم فالضبوط التي يتم تنظيمها من قبل الضابطة العدلية لإثبات ارتكاب

---

(1) قانون الضابطة الحراجية رقم /41/ لعام 2006.

(2) قانون الجمارك رقم /38/ لعام 2006.

(3) الفقرة الأخيرة من المادة /342/ من قانون أصول المحاكمات الجزائية.

الجنح والمخالفات، يُعمل بها حتى يثبت العكس بالبيّنة الكتابية أو بواسطة الشهود. ويدخل في هذا النوع الضبوط التي تنظمها شرطة السير لإثبات المخالفات المرورية[1].

**النوع الثالث: الضبوط التي لا تعدو أن تكون معلومات عادية.** وقد نصت المادة /180/ من قانون أصول المحاكمات الجزائية على هذا النوع بقولها: (لا قيمة للضبوط الأخرى إلاّ كمعلومات عادية).

والقانون لم يحدد طبيعة هذا النوع، لذلك يمكن القول أن كل ضبط لا يدخل في النوعين الأول والثاني يدخل في هذه الزمرة، ومن أمثلة هذه الضبوط، الضبوط التي ينظّمها موظفو الضابطة العدلية في الجنايات، والضبوط التي ينظمها موظفو الضابطة العدلية في الجرائم التي لا تدخل في اختصاصاتهم. ويمكن تشبيه هذه الضبوط بأنها بمثابة إخبار عن ارتكاب الجرائم[2].

## ثالثاً- الشروط الشكلية للضبط:

حتى يكون للضبوط المذكورة قوة في الإثبات، يجب أن تتوفر فيها الشروط الشكلية المنصوص عليها في المادة /179/ من قانون أصول المحاكمات الجزائية، وهي:

أ- أن يكون الضبط قد نُظم ضمن حدود اختصاص الموظف، وأثناء قيامه بمهام وظيفته.

ب-أن يكون الموظف قد شهد الواقعة بنفسه أو سمعها شخصياً.

ج- أن يكون الضبط صحيحاً في الشكل، بأن يتضمن الضبط اسم من نظّمه وصفته، وأن يكون مؤرخاً وموقعاً منه.

## رابعاً- القيمة الإثباتية للضبوط في جريمة الاحتيال عبر الإنترنت:

---

(1) قانون السير رقم /31/ لعام 2004 والمعدل بالمرسوم التشريعي /11/ لعام 2008.

(2) د.عبد الوهاب حومد: أصول المحاكمات الجزائية,المرجع السابق، ص 639.

سبقت الإشارة إلى أن مشروع قانون الجريمة الإلكترونية نص على إحداث وحدات شرطية في وزارة الداخلية متخصصة بمكافحة الجرائم التي نص عليها هذا المشروع. وبناءً على ذلك، فالضبوط التي يمكن تنظيمها مستقبلاً من قبل هذه الضابطة لإثبات الجرائم المنصوص عليها في مشروع قانون الجريمة الإلكترونية، إما أن يعمل بها حتى ثبوت العكس عندما تكون الجريمة جنحية الوصف، وإما أن تكون على سبيل المعلومات عندما تكون الجريمة جنائية الوصف. وهذه القواعد هي الواجب إتباعها مستقبلاً بالنسبة للضبوط المتعلقة بجريمة الاحتيال عبر الإنترنت.

وهناك من يرى في الفقه أن تخصص رجل الضابطة العدلية في مجال تقنية المعلومات أمرٌ تفرضه طبيعة جرائم الإنترنت، فلذلك يجب أن يكون عمل رجل الضبط القضائي أقرب إلى الخبير التقني، بحيث يكون مستعداً دائماً للتعامل مع هذه الجرائم، ومدرباً على فن تنظيم المحاضر والضبوط المتعلقة بها[1].

(1) د.عمر بن يونس ,الجرائم الناشئة عن استخدام الإنترنت,المرجع السابق ,ص819.

# المطلب الخامس

# الخبـرة

لا بد لنا قبل التطرق للخبرة في جريمة الاحتيال عبر الإنترنت من أن نلقي الضوء على الأحكام العامة للخبرة.

**أولاً- الأحكام العامة للخبرة:**

سنتناول من خلال هذه الأحكام، تعريف الخبرة، وإجراءات تعيين الخبراء، والقوة الإثباتية للخبرة.

**أ-تعريف الخبرة:**

الخبرة هي: "إبداء رأي فني من شخص مختص فنياً، في شأن واقعة ذات أهمية في الدعوى الجزائية"[1].

والمشرع السوري لـمُ يفصّل قواعد الخبرة في قانون أصول المحاكمات الجزائية، وإنما اكتفى بالإشارة إليها في المواد 39 و40 و41، في معرض حديثه عن وظائف النيابة العامة في حالة الجرم المشهود، حيث نصت المادة /39/ على ما يلي:

(إذا توقف تمييز ماهية الجرم وأحواله على معرفة بعض الفنون والصنائع، فعلى النائب العام أن يصطحب واحداً أو أكثر من أرباب الفن والصنعة.).

أما المادة /40/، فقد تحدثت عن الاستعانة بالأطباء لمعرفة أسباب الوفاة عندما تكون هناك شبهة جرمية في الوفاة. كما فرضت المادة /41/ على الأطباء والخبراء أن يُقسموا قبل مباشرتهم العمل يميناً بأن يقوموا بالمهمة الموكلة إليهم بشرف وأمانة.

---

(1) د.محمود نجيب حسني: شرح قانون الإجراءات الجنائية,المرجع السابق، ص474.

وإذا كان المشرع لم ينص صراحة على ضرورة الاستعانة بالخبراء في جميع مراحل الدعوى الجزائية، إلاّ أنه يحق لقضاة التحقيق والإحالة والمحاكم اللجوء إلى الخبرة؛ تطبيقاً لمبدأ حرية الإثبات في المواد الجزائية[1].

والقانون لم يحدد القضايا التي يجوز للقاضي الاستعانة فيها بالخبرة، غير أنه يمكن اللجوء إلى الخبرة عندما يتوقف الفصل في الدعوى على معرفة أمور فنية، حيث يمكن للمحكمة أن تقرر إجراء الخبرة من تلقاء نفسها أو بناء على طلب الخصوم[2]. فالاستعانة بالخبرة أمر متروك لسلطة القاضي التقديرية، اللهم إلاّ إذا تعلّقت الدعوى بمسألة فنية وعلمية لا يكفي في معرفتها الاختصاص العام، فعندها يصبح اللجوء إلى الخبرة أمر لا مفر منه[3].

ومع ازدياد الجرائم التي تستخدم في ارتكابها العلوم والمعارف الحديثة، تقدمت الخبرة مع تقدم هذه العلوم والمعارف، حيث ظهرت الخبرات الكيميائية، كتحليل الدم، وفحص الحمض النووي DNA، والخبرات التي تتعلق برفع البصمات، ومضاهاة الخطوط، وفحص الأسلحة وغير ذلك.

## ب-الفرق بين الخبير والشاهد:

هناك عدة فوارق بين الخبراء والشهود، وهذه الفوارق، هي[4]:

1- إن الشاهد يقدم للقاضي معلومات حصل عليها بالملاحظة الحسية، أما الخبير فيقدم للقاضي آراء تتعلق بقواعد علمية وأصول فنية.

---

(1) د.عبد الوهاب حومد: أصول المحاكمات الجزائية,المرجع السابق، المرجع السابق، ص 655 د.حسن الجوخدار: المرجع السابق، الجزء الثاني، ص 151.

(2) المادة /138/ من قانون البيّنات.

(3) الغرفة الجنائية أساس 160، قرار 204 تاريخ 1965/3/31، مجموعة القواعد القانونية، القاعدة رقم 52، ص 31.

(4) د.عبد الوهاب حومد: أصول المحاكمات الجزائية، المرجع السابق، ص 656. د.محمود نجيب حسني: شرح قانون الإجراءات الجنائية,المرجع السابق، المرجع السابق، ص475.

2- إن صيغة اليمين التي يؤديها الخبراء قبل مباشرتهم العمل تختلف عن صيغة اليمين التي يقسمها الشهود قبل أداء الشهادة. والخبير يمكن أن يكون شاهداً في القضية إذا شهد بعض وقائع القضية، وعندها يجب عليه أن يقسم الصيغة المتعلقة بالشهود.

3- إذا ثبت كذب الشاهد فإنه يعاقب بمقتضى نصوص قانون العقوبات المتعلقة بشهادة الزور /المواد 397 وما بعدها/، أما إذا جزم الخبير بأمر ينافي الحقيقة، فإنه يتعرض للعقوبة المنصوص عليها بالمادة /402/ من قانون العقوبات[1].

## ج-إجراءات تعيين الخبراء:

ذكرنا أن قانون أصول المحاكمات الجزائية لم يفصل في مسألة الخبرة. والسؤال الذي يطرح نفسه هنا هو: **هل يجب على القاضي الجزائي أن يطبق أحكام الخبرة المنصوص عليها في قانون البيّنات رقم /359/ لعام 1947؟**

أجابت محكمة النقض عن هذا السؤال بقولها: "إن الأصول المبينة في الباب السابع من قانون البيّنات ذي الرقم /359/ الصادر في 1947/6/10، والباحثة عن كيفية انتخاب الخبراء أو تعيينهم، وكيفية دعوة الطرفين، يجب مراعاتها في القضايا المدنية والتجارية فقط، كما هو واضح من مذكرته الإيضاحية، ومن تسمية هذا القانون باسم قانون البيّنات في المواد المدنية والتجارية. وإن اقتصار قانون أصول المحاكمات الجزائية في البحث عن وجوب الاستعانة بأرباب الفن والصنعة، عندما يتوقف تمييز ماهية الجرم وأحواله على

---

(1) تنص المادة 402 من قانون العقوبات على ما يلي :( 1- إن الخبير الذي تعينه السلطة القضائية ويجزم بأمر مناف للحقيقة أو يؤوله تأويلاً غير صحيح على علمه بحقيقته, يعاقب بالحبس ثلاثة أشهر على الأقل وبغرامة لا تنقص عن مائة ليرة, ويمنع فضلاً عن ذلك أن يكون أبداً خبيراً. 2- ويقضى بالأشغال الشاقة إذا كانت مهمة الخبير تتعلق بقضية جنائية.)

معرفة بعض الفنون والصنائع، ووجوب تحليفهم اليمين على ما ورد في المواد /39 و40 و41/ أصول جزائية، يدل على عدم رغبة واضع القانون في تقييد القضاة الجزائيين بأمور شكلية مادام أمر الثبوت وعدمه في الأصل متروكاً لضمائرهم وقناعتهم."[1].

وعلى ضوء ذلك، فقد استقر الاجتهاد القضائي على أن للمحاكم الجزائية تعيين الخبراء من غير المسميين في جدول الخبراء الذي تصدره وزارة العدل وفقاً لقانون الخبراء الصادر بالمرسوم التشريعي رقم 42 لعام 1979. فالمحاكم الجزائية غير مقيدة بالأمور الشكلية عند اختيار الخبراء، من حيث عددهم، وطريقة اختيارهم، وكيفية دعوتهم، فلم يتطلب قانون أصول المحاكمات الجزائية من الخبير سوى أن يقسم اليمين المنصوص عليها بالمادة /41/ من قانون أصول المحاكمات الجزائية[2] قبل مباشرته العمل[3].

وللخبير أن يلجأ إلى استخدام كل ما ينور له طريقه كي يكون تقريره واضحاً ومتكاملاً، فله استدعاء المدعى عليه، وله طلب أدوات الجريمة، وزيارة مكانها، ويجب أن يقدم تقريره مكتوباً وموقعاً منه، في المدة التي حدّدها له القاضي[4].

## د-القوة الإثباتية للخبرة:

---

(1) الغرفة الجنحية أساس 2140، قرار 2117 تاريخ 1968/12/31، مجموعة القواعد القانونية، القاعدة رقم 60، ص 34.

(2) تنص المادة41 من قانون أصول المحاكمات الجزائية على ما يلي : (على الأطباء والخبراء المشار إليهم في المادتين 39 و 40 أن يقسموا قبل مباشرتهم العمل يميناً بأن يقوموا بالمهمة الموكلة إليهم بشرف وأمانة.).

(3) الغرفة الجنحية أساس 3551، قرار 3782 تاريخ 1968/12/31، مجموعة القواعد القانونية، القاعدة رقم 62، ص 34.

(4) د.عبد الوهاب حومد: أصول المحاكمات الجزائية,المرجع السابق، ص 653.

لاُ يلـزم تقريـر الخبـرة القاضـي الجزائـي؛ لأنـه يحكـم بحسـب قناعتـه الشخصية. فالمحكمة هي التي تقدر قيمة النتائج التي توصل إليها الخبير في تقريره، فلها أن تأخذ به كله، أو أن تجزّئه، فتأخذ منه بالقدر الذي تقتنع به، كما لها أن تهمله مع بيان الأسباب[1].

ومما لا شكّ فيه بأن الخبرة الجارية في مرحلة التحقيق الابتدائي ومرحلة المحاكمة تعدّ من قبيل الأدلة القضائية، أما الخبرة الجارية في مرحلة التحقيق الأولي، فلا تعتبر دليلاً قضائياً يمكن الاستناد إليه في إصدار الأحكام، وإنما تعدّ بمثابة معلومات عادية[2].

والواقع أن القاضي غالباً ما يسلّم بما خلص إليه الخبير في تقريره ويبني حكمه على أساسه. ويرى الفقه أن تصرف القاضي هنا لا يخرج عن حدود المنطق، لأن رأي الخبير ورد في موضوع فني لا اختصاص للقاضي به، وليس من شأن ثقافته القانونية أو خبرته القضائية أن تتيح له الفصل فيه، ناهيك عن أن القاضي هو الذي انتدب الخبير وراقب مهمته[3].

## ثانياً- الخبرة التقنية في جريمة الاحتيال عبر الإنترنت:

تعدّ الخبرة التقنية في جريمة الاحتيال عبر الإنترنت من أكثر طرق الإثبات أهمية، إذ إنها تؤدي دوراً لا يستهان به في إثبات هذه الجريمة. فالاستعانة بالخبرة التقنية في التحقيق الأولي أو الابتدائي أو النهائي، من أقوى مظاهر التعامل مع هذه الجريمة.

---

(1) الغرفة الجنحية أساس 2177، قرار 2224 تاريخ 1968/9/26. الغرفة الجنحية أساس 3483، قرار 3147 تاريخ 1966/12/12، مجموعة القواعد القانونية، القواعد 68، 69، 71 ص 37-38.

(2) د.حسن الجوخدار: المرجع السابق، الجزء الثاني، ص150.

(3) د.محمود نجيب حسني: شرح قانون الإجراءات الجنائية,المرجع السابق، ص482.

والواقع أن هذا النوع المتميز من الخبرة بدأ يتخذ لنفسه حيزاً في مجال إثبات جرائم العالم الافتراضي، حتى أصبح يعرف في الفقه المقارن بمصطلح Computer Forensic أو Digital Forensic، أي المعلوماتية الشرعية[1].

ويمكن تعريف **المعلوماتية الشرعية** بأنها: "استخدام الطرق العملية لجمع وتعريف وتحليل وتفسير الدليل الرقمي المأخوذ من مصادر رقمية، والاحتفاظ به وتوثيقه، على نحو يسهل بناء الحوادث التي تؤدي إلى اكتشاف الجريمة."[2]. أو هو: "جمع وحفظ وتحليل وتقديم الدليل المتعلق بالحاسوب."[3].

فالمعلوماتية الشرعية هي عملية البحث التي يقوم بها الخبير المعلوماتي من أجل الحصول على الدليل الرقمي، بغية إعادة بناء مجريات القضية وتوضيحها للمحكمة. وهذه العملية تشبه تشريح الجثة في الطب الشرعي.

## أ-كيفية اختيار الخبير المعلوماتي:

أطلق المشرع يد القاضي الجزائي في الاستعانة بالخبرة لتكوين قناعته الشخصية، فله مطلق الصلاحية في اختيار الخبير المعلوماتي، الذي من الممكن أن يكون شخصاً طبيعياً أو اعتبارياً، كالشركات المختصة في تكنولوجيا المعلومات.

ويرى جانب من الفقه أنه يمكن للقاضي الجزائي أن يختار الخبير المعلوماتي من إحدى الفئات التالية[4]:

---

(1) يمكن هنا استخدام مصطلح "المعلوماتية الشرعية" نسبة إلى الطب الشرعي.

(2) Robin Bryant, op-cit, p.173.

(3) John R.vacca, Computer Forensics: Computer Crime scene Investigation, published by Charles River media, 2002, chapter, 1 m p-4 .

(4) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت,المرجع السابق، ص 1035.

**1-الجهات الخاصة:**

إلى جانب الخبرة الفردية، يمكن للقاضي الجزائي أن يلجأ إلى الشركات المختصة في مجال تكنولوجيا المعلومات، التي تضم في الغالب خبراء على مستوى عالٍ من الكفاءة. فهذه الشركات كثيراً ما تسعى إلى التعاقد مع أشخاص لهم شهرتهم في هذا المجال، ولو لم يكونوا من أصحاب الدراسات الأكاديمية؛ فلقد أثبتت التجربة العملية أن هناك أشخاصاً يتمتعون بمهارات فائقة في التعامل مع الحاسوب والإنترنت، دون أن يتجاوز تحصيلهم العلمي السنوات الجامعية الأولى. مثل "بيل كيتس" Bill Gates، صاحب شركة مايكروسوفت، وهذا الأمر ينطبق أيضاً على عتاة الهكرة ومخترقي الأنظمة ، الذين لم يتجاوز تعليمهم الثانوية العامة[1].

**2-المؤسسات التعليمية:**

قام العديد من المؤسسات التعليمية بإعداد قاعدة قوية في مجال دراسات الحاسوب والإنترنت، مثل جامعة "ستانفورد"، ومعهد التكنولوجيا في ولاية "ماساشوستس"، الذي قدم للبشرية خبراء على درجة عالية من التميز. ويمكن للقاضي الاستعانة بمثل هذه المؤسسات التعليمية المختصة لاختيار الخبير المعلوماتي[2].

**3-جهات الضبط القضائي:**

اتجهت معظم الدول المتقدمة إلى إحداث أجهزة مختصة في المعلوماتية الشرعية، فقد أسّست الولايات المتحدة الأمريكية مؤخراً فرعاً تابعاً لمكتب التحقيقات الفيدرالي FBI أُطلق عليه (المخبر الإقليمي الشرعي للحاسوب)،

---

(1) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت,المرجع السابق، ص 1023 و 1035.

(2) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت,المرجع السابق، ص 1037.

مقره "سان دييجو"، لكي يكون بيت الخبرة الحكومي، حيث يتم فيه إعداد الباحثين في المجال المعلوماتي على مستوى عالٍ من الكفاءة[1].

**4-التعاون الدولي:**

يمكن للقاضي الجزائي أن يلجأ إلى الخبراء الأجانب من أجل القيام بالخبرة التقنية، غير أن هذا الأمر يتوقف على مدى نشاط المشرع في كل دولة لإبرام اتفاقيات تعاون في هذا المضمار[2].

وفي سورية يمكن للقاضي الجزائي أن يستعين بعدة جهات مماثلة للجهات المذكورة ، لمساعدته في اختيار الخبير المعلوماتي، كالجمعية العلمية السورية للمعلوماتية، أو كلية الهندسة المعلوماتية، أو الشركات الخاصة التي تعمل في مجال تكنولوجيا المعلومات، أو الهيئة الوطنية لخدمات الشبكة، حيث جعل قانون التوقيع الإلكتروني وخدمات الشبكة رقم /4/ تاريخ 2009/2/19 من مهام الهيئة الوطنية لخدمات الشبكة، مهمة اقتراح الخبراء التقنيين للجهات القضائية في مجال التوقيع الإلكتروني[3].

## ب-آلية عمل الخبير المعلوماتي:

يقوم الخبير المعلوماتي بفحص الأجهزة الرقمية المتعلقة بالجريمة، سواء أكانت حواسيب شخصية أم مُخدّمات لدى مزود خدمة الإنترنت. ولذلك فإن الفقه الإجرائي يرى بأنه يجب على الخبير المعلوماتي أن يكون قادر على القيام بالمهام التالية[4]:

---

(1) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت,المرجع السابق، ص 1038.

(2) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت,المرجع السابق، ص 1039.

(3) المادة /15/ من قانون التوقيع الإلكتروني وخدمات الشبكة رقم /4/ لعام 2009.

(4) John R.vacca, op-cit, chapter 1, p- 5 .

Eoghan Casey, op-cit, chapter 1, p-97 to 111. And Robin Bryant, op-cit, P-59 to 63.

- حجز البيانات.
- حفظ البيانات.
- استعادة البيانات.
- تحليل البيانات.
- إعادة بناء القضية.
- كتابة التقرير.

وسنلقي الضوء على هذه الإجراءات باختصار.

**1-حجز البيانات:**

هناك مبدأ شهير في مجال المعلوماتية الشرعية، يعرف باسم "مبدأ لوكارد التبادلي"، ويقصد به أن أي شخص يدخل إلى مسرح الجريمة، يجب أن يأخذ منه شيئاً، وأن يترك خلفه شيئاً ما.

فمثلاً، إذا أرسل شخص رسالة إلكترونية تحمل مضموناً احتيالياً إلى أحد الأشخاص، فإن هذه الرسالة سوف تخزن على المُخدّمات الموجودة لدى مزود خدمة الإنترنت مع التاريخ والوقت، إضافةً إلى مسار الرسالة وعنوان رقم النفاذ.

لذلك يجب على الخبير المعلوماتي أن يقوم في بادئ الأمر بعملية حجز للبيانات المتعلقة بالجريمة الموجودة لدى مزود الخدمة، إضافةً إلى حجز الأجهزة التي تحوي هذه البيانات، والتي تكون بحيازة المشتبه به أو في مسرح الجريمة[1].

**2-حفظ البيانات:**

يقوم الخبير المعلوماتي في هذه المرحلة بنسخ البيانات التي تمّ حجزها، بحيث يصبح لديه منها نسختان: الأولى يتم تخزينها في الأجهزة الرقمية التي تمّ

---

(1) Eoghan Casey, op-cit, , p-101. And John R.vacca, op-cit,chapter 1, p- 6.

حجزها، بحيث تبقى محفوظة بشكل جيد، والثانية عبارة عن نسخة طبق الأصل، يتم إجراء عملية الاختبار أو الفحص عليها[1].

**3-استعادة البيانات:**

يجب على الخبير المعلوماتي أن يستعيد البيانات المحذوفة، وهو أمر ضروري من أجل إعادة بناء القضية. فمثلاً يمكن للخبير أن يستعيد جميع الرسائل التي قام الجاني بحذفها عن طريق تتبع الأثر الذي تتركه هذه الرسائل على جهاز التخزين[2].

**4-تحليل البيانات:**

في هذه المرحلة، يقوم الخبير المعلوماتي بعملية تقييم محتوى البيانات الرقمية، بحيث يفحصها بدقة من أجل تحديد وسائل الجريمة ودوافعها والغرض منها[3].

**5-إعادة بناء القضية:**

ويقصد بإعادة بناء القضية، العملية التي يقوم بها الخبير، بعد تجميع وتحليل البيانات والمعلومات التي تمّ الحصول عليها بنتيجة البحث، من أجل توضيح ما حصل بين المجرم والضحية أثناء ارتكاب الجريمة. فالدليل الرقمي الذي تمّ الحصول عليه يحتوي على آثار سلوكية للمجرم، مثل الكلمات التي استخدمها المجرم في تصفح الإنترنت، والمواقع التي قام بتصفحها على الشبكة، وغرف الدردشة التي قام بزيارتها، وغير ذلك... فالربط بين هذه

---

(1) Eoghan Casey, op-cit, p-109. And John R.vacca, op-cit, chapter 1, p- 6.

(2) Eoghan Casey, op-cit, p-109. And John R.vacca, op-cit, chapter 1, p- 6.

(3) Eoghan Casey, op-cit, p-111.

السلوكيات يؤدي إلى معرفة وقت ومكان ارتكاب الجريمة، والطريقة التي تمت بها، وكيفية وصول الجاني إلى ضحيته[1].

**6-كتابة التقرير:**

يتضمن تقرير الخبرة بين دفتيه النتائج التي توصل إليها الخبير من خلال عملية البحث. أما النقاط التي يجب أن يتضمنها التقرير، فهي[2]:

- مواصفات مسرح الجريمة الافتراضية.
- ملخص عن عملية الفحص التي تمّ القيام بها.
- إعادة رواية أحداث القضية.
- ملخص النتائج.
- اقتراحات الخبير المعلوماتي.

وينصح أن يكون التقرير متسلسلاً من حيث بناء الأحداث، وأن يكون مختصراً من الناحية التقنية، ومكتوباً بأسلوب بسيط وواضح، حتى تتمكن المحكمة من فهمه بسهولة.

وإذا رأت المحكمة نقصاً في تقرير الخبرة، أو كان فيه مسائل معينة تحتاج إلى إيضاح من الخبير، فيمكن أن تقرر من تلقاء نفسها، أو بناء على طلب أحد الخصوم، دعوة الخبير المعلوماتي لحضور الجلسة، وتوجيه الأسئلة له، لتكملة هذا النقص أو إيضاح المسائل الغامضة[3].

## ج- مدى تأثير الخبرة التقنية على قناعة القاضي:

يرى جانب من الفقه بأن الخبير المعلوماتي هو القاضي الحقيقي للدعوى، فكل ما يبديه الخبير المعلوماتي يعدّ من الحقائق التي تجبر القاضي على

---

(1) Eoghan Casey, op-cit, p-116.

(2) Eoghan Casey, op-cit, p-131.

(3) المادة /155/ من قانون البيّنات.

الأخذ بها، فالدور الجوهري للخبير في تحديد الأدلة الرقمية لا يترك مجالاً واسعاً للقاضي لتحديد مسار الدعوى. ولذلك يصبح الخبير الملهم الأساسي في القضية[1].

ويستشهد أصحاب هذا الرأي بقضية شهيرة، تتلخص وقائعها بأنه في عام 2000، قام اتحاد الطلبة اليهود في فرنسا برفع دعوى ضد شركة "ياهو" Yahoo الفرنسية و"ياهو" الأمريكية، بسبب وجود مزاد علني يتعلق بالنازية على إحدى الصفحات المجانية التي تبث من خلال "ياهو" على الإنترنت. ولقد تضمّن المزاد عرض مجموعة من صور الزعيم النازي "أدولف هتلر" ومجموعة شعارات وصور وأعلام تتعلق بالحزب النازي.

وقد رفعت الدعوى أمام محكمة باريس الابتدائية، بناءً على أن شركة "ياهو" قامت بالتقليل من كارثة "الهولوكوست" عندما سمحت بإجراء مثل هذا المزاد على الإنترنت، وهو الأمر الذي يشكّل جريمة وفق القانون الفرنسي الذي يكافح النازية.

وقد أصدر القاضي حكمه على شركة "ياهو" بإلزامها بمنع المستخدمين من الدخول إلى هذه المزادات، واعتمد القاضي في حكمه على تقرير الخبرة التقنية الذي أكّد قدرة شركة "ياهو" على منع مستخدمي الإنترنت من الدخول إلى هذه المزادات، رغم إصرار شركة "ياهو" على عدم قدراتها على ذلك.

ويرى الفقه في هذه القضية أن المحكمة اعتمدت على تقرير الخبرة التقنية دون أن تقوم بمناقشته بشكل جيد؛ فقرار المحكمة صدر بعد أيام قليلة من إيداع لجنة الخبراء لتقريرها[2].

---

(1) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت,المرجع السابق، ص 967.

(2) نشرت هذه القضية على موقع www.juriscom.net ومشار إليها عند د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت,المرجع السابق، ص 1003 و 1028.

و**يرى الباحث** أن اعتماد المحكمة على تقرير الخبير المعلوماتي لا يعد مساساً بمبدأ قناعة القاضي الشخصية، ولا يجعل من الخبير القاضي الحقيقي للدعوى. فدور الخبير التقني ليس سوى أحد الأدوار التي تساعد القاضي على فهم القضية، وهذا الدور ليس بجديد على الساحة القضائية؛ فالقضاء كثيراً ما كان يستند في أحكامه إلى الخبرة التي تجري على البصمات، أو على الحمض النووي DNA، أو على التحاليل النفسية وغيرها. كما أن بناء الحكم على أساس تقرير الخبرة لا يختلف عن الأخذ بأقوال الشهود وبناء الحكم بالبراءة أو الإدانة على أساس هذه الأقوال. فمحكمة الموضوع هي صاحبة القول الفصل في تقرير الخبرة الذي قد تقتنع به أو لا تقتنع.

# المبحث الثاني
# طرق الإثبات المستحدثة (الدليل الرقمي)

لم تَسلَم طرق الإثبات من تأثيرات ثورة المعلومات والتكنولوجيا، فالتناغم المطلوب تحقيقه دائماً بين طبيعة الدليل وطبيعة الجريمة التي يولد منها، أفرز إلى حيز الوجود نوعاً جديداً من الأدلة يتماشى مع طبيعة جرائم الإنترنت، وهو ما يعرف بالدليل الرقمي، أي الدليل الناتج عن فحص المكونات المعنوية أو البرمجية للحواسيب وشبكة الإنترنت.

فإذا كان فحص السلاح الناري والذخيرة هو المولد للدليل في جريمة القتل، وفحص المحرر هو المولد للدليل في جريمة التزوير؛ فإن جريمة الاحتيال عبر الإنترنت لا تخرج عن هذا الإطار، فإثبات هذه الجريمة يحتاج إلى طرق تقنية تتناسب مع طبيعتها، بحيث يمكن ترجمة النبضات والذبذبات الإلكترونية إلى أدلة إثبات أو نفي على ارتكاب هذه الجريمة.

وقد ساهم القضاء المقارن في رسم معالم الدليل الرقمي، سواء من حيث فائدته أم من حيث قيمته القانونية، حيث اعتّدت به المحاكم، بناء على نص تشريعي تارة، وعلى الاجتهاد تارة أخرى.

وبناءً على تسلسل هذه الأفكار، سنقسم هذا المبحث إلى المطلبين التاليين:

المطلب الأول: ماهية الدليل الرقمي.

المطلب الثاني: حجية الدليل الرقمي.

# المطلب الأول
# ماهية الدليل الرقمي

يتطلب منا البحث في ماهية الدليل الرقمي التعرض لتعريفه، ثم التعرف على مزايا ومساوئ هذا الدليل، وتحديد مصادره الرقمية، وبيان الدور الذي يلعبه الدليل الرقمي في التحقيقات الجرمية، وذلك عن طريق عرض بعض القضايا الواقعية المتعلقة بجريمة الاحتيال عبر الإنترنت. وهذا ما سنبحثه على التتالي:

## أولاً– تعريف الدليل الرقمي:

هناك عدة تعريفات للدليل الرقمي، نذكر منها:

– هو:"أية بيانات مخزنة أو منقولة بواسطة الحاسوب، تدعم أو تدحض أية نظرية حول كيفية ارتكاب الجريمة، وتتعلق بعناصر هامة في الجريمة."[1].

–كما عرفت المنظمة الدولية للدليل الرقمي هذا الدليل بأنه: "معلومات مخزنة أو منقولة بشكل يمكن قبوله في المحكمة"[2].

– أما مجموعة العمل العلمية حول الدليل الرقمي SWGDE، فقد عرفته بأنه: "أية معلومات ذات قيمة مخزنة أو منقولة بشكل رقمي."[3].

---

(1) Eoghan Casey: op-cit, P-21 .

(2) وهي منظمة تزود الجهات الدولية القانونية بكيفية تبادل المعلومات المتصلة بتحقيقات جرائم الحاسوب ومسائل ذات صلة بالبحث المعلوماتي. وسنلقي الضوء بشكل أوسع على هذه المنظمة لاحقاً. متوفر على الموقع www.ioci.org.

(3) ===Scientific Working Croup on Digital Evidence.

– وهـو: "المعلومـات والبيانـات ذات القيمـة الاستقصـائية، والمخزنـة أو المنقولة عبر جهاز إلكتروني."[1].

– وهو: "برامج الحاسوب وبياناته التي تستخدم للإجابة عن الأسئلة الهامة حول الحادثة الأمنية"[2].

– وبتعريـف آخـر هـو: "معلومـات ذات قيمـة برهانيـة أو اسـتدلالية تـمّ تخزينها أو نقلها بشكل رقمي"[3].

– وهو أيضاً: "الدليل الذي يجد له أساساً في العالم الافتراضي ويقود إلى الجريمة"[4].

ومن خلال استقراء هذه التعاريف، يمكن تحديد خاصتين للدليل الرقمي هما:

**الخاصة الأولى:** إن الدليل الرقمي عبارة عن معلومات أو بيانات رقمية مخزنة في الحاسوب أو منقولة بواسطته، أيّاً كان شكل هذا الحاسوب، بحيث يستوي أن يتخذ شكل الحاسوب الشخصي، أو مُخدّم الإنترنت، أو أن يكون ضمن الهاتف الجوال، أو ساعة اليد، أو الكاميرات الرقمية وغيرها.

**الخاصة الثانية:** القيمة الاستدلالية أو البرهانية لهذه المعلومات في إثبات أو نفي الجرائم.

---

=== تأسست هذه المجموعة في شباط عام 1998 من خلال التعاون مع مدراء مختبرات الجريمة الفيدرالية , ومقرها الولايات المتحدة، ومهمتها توحيد المقاييس الدولية للدليل الرقمي, وتطوير معايير حفظ وفحص الدليل الرقمي. متوفر على الموقع www.swegde.org.

(1) Panagiotis kanellis and others, Digital Crime and Forensic Science in Cyberspace, Published by Idea group inc, 2006, P-272.

(2) Micheal G.Solomon and others, Computer Forensics jump start, published by Wiley- Default, 2005, chapter- 3, P-4 .

(3) Alpert.J.Marcella: op-cit, P-132 .

(4) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت,المرجع السابق، ص969.

وبناءً على ما تقدم، يمكن تعريف الدليل الرقمي بأنه: "**المعلومات أو البيانات الرقمية المخزنة في الحاسوب أو المنقولة بواسطته، والتي يمكن استخدامها في إثبات أو نفي جريمة ما.**"

ولا بدّ من الإشارة بأن ما يهمنا في هذه الدراسة هو دور الدليل الرقمي في إثبات جرائم الإنترنت عموماً والاحتيال خصوصاً فقط، لأن هذا الدليل يمكن استخدامه في إثبات أو نفي الجرائم التقليدية أيضاً، كما لو كانت هناك رسالة إلكترونية تحمل اعترافاً للجاني بارتكابه جريمة القتل أو الاغتصاب أو الاحتيال العادي.

## ثانياً- مزايا الدليل الرقمي:

يتمتع الدليل الرقمي بعدة مزايا، وهي:

**أ-إمكانية النسخ:**

يمكن نسخ الدليل الرقمي نسخة مطابقة للأصل تماماً ، بحيث يمكن إجراء الفحص المعلوماتي على هذه النسخة لتفادي خطر إتلاف النسخة الأصلية أثناء عملية الفحص، وهذه الميزة لا تتوفر في الأدلة التقليدية[1].

**ب-إمكانية كشف التعديل:**

قد يتعرض الدليل الرقمي للتعديل المقصود من قبل الجاني، أو التعديل غير المقصود من قبل المحقق أو الخبير المعلوماتي أثناء عملية جمع الدليل، وفي كلتا الحالتين يمكن معرفة ما إذا كان الدليل الرقمي قد تعرض للتعديل أم لا، وذلك باستخدام برمجيات تقنية معينة تستخدم في هذا الخصوص، إضافةً إلى إمكانية إجراء المقارنة مع النسخة الأصلية إن وجدت[2].

---

(1) Eoghan Casey: op-cit, P-25 .

(2) Eoghan Casey: op-cit, P-25 .

**جـ- صعوبة التخلص من الدليل الرقمي:**

وهذه الميزة من أهم مزايا الدليل الرقمي على الإطلاق، بل يمكن القول بأنها الميزة التي يتمتع بها الدليل الرقمي دون غيره من الأدلة التقليدية، وهو بذلك يشبه الدليل العلمي المتعلق بالحمض النووي DNA، إذ إن كليهما يصعب التخلص منهما.

ففي مجال الأدلة التقليدية، كثيراً ما كانت أجهزة العدالة تعاني من مسألة التخلص من الأدلة المادية، إذ يمكن التخلص من بصمات الأصابع بمسحها من موضعها، ويمكن التخلص من الأوراق التي تحمل إقرارات معينة بتمزقها وحرقها، كما يمكن التخلص من الشهود بقتلهم أو تهديدهم بعدم الإدلاء بشهاداتهم. وفي جميع هذه الحالات يكون من الصعب إن لم يكن مستحيلاً استرجاع أو استرداد هذه الأدلة.

أما في حالة الدليل الرقمي فالأمر يختلف تماماً. فمسألة التخلص من الملفات الإلكترونية عن طريق تعليمات Delete أو Erase أو حتى في حالة إعادة تهيئة القرص الصلب Format وغيرها، لا تشكّل عائقاً يحول دون استرجاع هذه الملفات(كلياً أو جزئياً) التي تمّ إلغاؤها أو إزالتها من الحاسوب[1].

ومن القضايا التي أبرزت هذه الميزة، أنه أثناء التحقيق مع الكولونيل "أوليفر نورد" في قضية إيران عام 1986، تمّ استعادة جميع الرسائل الإلكترونية المتعلقة بالجريمة، بعد أن قام هذا الكولونيل بحذفها من حاسوبه، إذ لم يكن هذا الأخير يعلم بأن هذه الرسائل يمكن استعادتها عن طريق النسخ المحفوظة في النظام[2].

## ثالثاً- مساوئ الدليل الرقمي:

---

(1) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت,المرجع السابق، ص 981, 982, 983.

(2) Eoghan Casey: op-cit, P-26 .

للدليل الرقمي عدة مساوئ، وهي:

**أ-الدليل الرقمي دليل غير مرئي:**

ليس للدليل الرقمي طبيعة مادية ملموسة كما هو الحال في الأدلة التقليدية، فالأجهزة التقنية لا تفرز سكيناً عليها بصمات القاتل، أو مالاً يمكن ضبطه مع السارق في جريمة السرقة وغير ذلك، فكل ما تنتجه التقنية هو عبارة عن نبضات إلكترونية يمكن أن تدل في مجموعها على أنماط السلوك الإنساني.

والواقع أن هذه الطبيعة غير المرئية للدليل الرقمي تلقي بظلالها على أجهزة الضبط القضائي التي تتعامل مع هذه الجرائم المستحدثة، لأن غياب الدليل المرئي يشكّل عقبة كبيرة أمام كشفها[1].

**ب-الحجم الكبير للبيانات التي يوجد فيها الدليل الرقمي:**

يحتوي القرص الصلب مثلاً على حجم كبير من البيانات والمعلومات غير المرتبة، ولكن ما يتعلق بالجريمة قد يشكل جزأً صغيراً فقط من هذه المعلومات. ويمكن تشبيه حجم المعلومات هذا بموجات الراديو الموجودة في الهواء والتي تحتوي على بيانات متشابكة، الأمر الذي يجعل من الصعوبة بمكان معرفة الإشارة المطلوبة وترجمتها إلى بيانات مفهومة. فالوصول إلى الدليل الرقمي المطلوب يشكّل تحدياً أمام الخبير المعلوماتي[2].

**جـ- الدليل الرقمي دليل ظرفي:**

---

(1) د.جميل عبد الباقي الصغير: الجوانب الإجرائية للجرائم المتعلقة بالإنترنت, المرجع السابق، ص4. د.علي محمود علي حمودة: المرجع السابق، ص16. متوفر على الموقع www.arblawinfo.com.

(2) Eoghan Casey: op-cit, P-25 .

الدليل الرقمي هو عادة دليل ظرفي، فمعرفة عنوان الإنترنت IP مثلاً يشير إلى الحاسوب الذي ارتكبت الجريمة بواسطته فقط، دون أن يحدّد مرتكب الجريمة بالذات، الأمر الذي يجعل من الصعوبة بمكان، نسبة النشاط الجرمي إلى شخص ما، ما لم يتم القيام بالعديد من التحقيقات للتأكد من ذلك.

ففي إحدى القضايا التي عرضت على المحاكم الأمريكية، نازع المدعى عليه في جميع الأدلة التي وجدت على حاسوبه، لأن المحققين لم يستطيعوا إثبات أنه هو الشخص الذي قام بالنشاطات غير الشرعية على الإنترنت[1].

وتجدر الملاحظة في هذا المجال إلى أن المساوئ المشار إليها، والتي تقف في وجه الدليل الرقمي في هذه الأيام، قد لا يكون لها أثر في القريب العاجل، لأن التطور المتسارع للبرمجيات في عصر الثورة الرقمية قادر على إزالة معظم الصعوبات التي تقف حائلاً دون نمو هذا الدليل المستحدث.

## رابعاً- مصادر الدليل الرقمي ودور الإنترنت في التحقيقات الجرمية:

يمكن الوصول إلى الدليل الرقمي المتعلق بجرائم الإنترنت عن طريق البحث في المصدرين التاليين:

### أ-أنظمة الحاسوب وملحقاتها:

تعدّ الحواسيب مصدراً غنياً بالأدلة الرقمية، وخاصة تلك الحواسيب الشخصية التي تعدّ بمثابة أرشفة سلوكية للأفراد. فهذه الحواسيب تحتوي على الكثير من المعلومات المتعلقة بنشاطات الأفراد ورغباتهم.

فالملفات الشخصية أو ملفات النظام وغيرها من أنواع الملفات، التي تكون مخزنة عادة في الأقراص الصلبة أو الأقراص الليزرية CD أو الذواكر

(1) Eoghan Casey: op-cit, P-26 .

المعروفة بـ Flash Memory[1] كثيراً ما تحتوي على معلومات تتعلق بالجريمة وتفيد في عملية التحقيق[2].

وعملية حجز الحاسوب أو ضبطه بقصد تفحصه، تعدّ نقطة البداية في الكشف عن خفايا جريمة الإنترنت، لأن الحاسوب هو وسيلة النفاذ إلى هذه الشبكة، أيّاً كان شكل هذا الحاسوب. ويجب أن تشمل عملية الفحص جميع البرمجيات المخزنة في المكونات الصلبة أو الذواكر الملحقة بالحاسوب، وجميع البرمجيات التي تمّ إلغاؤها من ذي قبل، كما يجب التأكد من أن المكونات الصلبة والبرمجيات تعمل بشكل سليم ومنتظم، وأن الحاسوب غير مصاب بفيروس يؤثر على نظامه أو على ملفات التشغيل أو التنفيذ، لأن ذلك يمكن أن ينال من صحة الدليل الرقمي المستخلص عند عرضه على القضاء[3].

**ب-أنظمة الاتصال بالإنترنت:**

تشمل عملية فحص أنظمة الاتصال بالإنترنت، فحص حركة التنزيل والتحميل ودرجة الاستيعاب، والشبكات المحلية، والنظام الأمني المحاط بالإنترنت...الخ. فعملية الفحص هذه قد تؤدي إلى الحصول على دليل رقمي يفيد في كشف الحقيقة[4].

ولعلّ أهم المسائل المثارة في صدد فحص أنظمة الاتصال بالإنترنت هي مسألة تحديد مكان الجريمة، أو الحاسوب الذي ارتكب بواسطته النشاط الجرمي، حيث يمكن معرفة هذا الحاسوب عن طريق تتبع الحركة العكسية

---

(1) ذاكرة سريعة بحجم القلم، ذات سعة كبيرة ومحمولة، يمكن ربطها بالحاسوب الشخصي وتسجيل ملفات ذات حجم كبير. د.عبد الحسن الحسيني: المرجع السابق، ص526.

(2) Eoghan Casey: op-cit, P-21. and also Albert.J.Marcella, op-cit, p-94, 95. and also Robin Bryant, op-cit, p-50 .

(3) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت,المرجع السابق، ص 1008- 1009.

(4) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت,المرجع السابق، ص 333- 997.

لمسار الإنترنت[1]، ويستخدم في عملية التتبع هذه نظام فحص إلكتروني يطلق عليه **علم البصمات المعاصر أو علم بصمات القرن الواحد والعشرين**، وهو منهج تم استخدامه في العديد من الجرائم، مثل تتبع مبتكر فيروس "ميليسا"، وكذلك في التوصل إلى الشخص الذي ابتكر موقع خدمات "بلومبرمج" لأخبار المال، وهو موقع احتيالي يرفع أسعار الأسهم بطريقة الخداع.[2]

ومن الملاحظ أن ما يتم التوصل إليه بفضل تتبع الحركة العكسية لمسار الإنترنت هو عنوان رقمي فقط IP adress ، وهذا الدليل الرقمي لا يكفي لنسبة الجريمة إلى مالك الحاسوب، إذ من الممكن ألاّ يكون هو مرتكب الجريمة، كما لو كان حاسوبه مسروقاً، أو مؤجراً في أحد مقاهي الإنترنت، أو أن يكون عنوانه الرقمي الخاص مسروقاً، أو أن يكون هناك من يستخدم حاسوبه احتيالاً، أو أن المشتبه به لا يعرف أي شيء عن الإنترنت...الخ. الأمر الذي يتطلب من جهات التحقيق توفير الدليل المادي كالاعتراف أو الشهادة أو الخبرة...الخ إلى جانب الدليل الرقمي، حتى يمكن أن تنسب الجريمة إلى مرتكبها[3].

أما مُخدّمات شبكة الإنترنت، فهي تحتوي على الكثير من المعلومات حول أنماط سلوك الأفراد في وقت محدد، فيمكن عن طريق فحص هذه المُخدّمات معرفة الرسائل الإلكترونية التي قام الجاني أو المجني عليه بإرسالها أو استقبالها، والمواقع الإلكترونية التي سبقت زيارتها، وغرف الدردشة التي تمّ

---

(1) يقصد **بمسار الإنترنت**، الحركة التراسلية للنشاط الممارس من خلال الإنترنت، فالحاسوب بمجرد أن يتعرف على المسار، يقوم تلقائياً باختيار البروتوكول التراسلي الذي من خلاله يقوم باستدعاء البيانات، وهذه هي الحركة التي أشار إليها علماء الإنترنت بأنها تتشابه مع شبكة العنكبوت من حيث عدم انتظام شكل المسار الاتصالي والتواصلي عبرها. د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت,المرجع السابق، ص 998.

(2) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت,المرجع السابق، ص 998.

(3) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت,المرجع السابق، ص 999.

الدخول إليها، حيث يستطيع المحقق أو الخبير المعلوماتي بعد أن يصل إلى هذه المعلومات، أن يتصل بجميع الأفراد الذين كانوا على اتصال مع الجاني أو المجني عليه قبل ارتكاب الجريمة، وذلك عن طريق إرسال الرسائل الإلكترونية إليهم، وسؤالهم عن أي معلومات تتعلق بالجريمة[1].

وعلى المحقق أو الخبير المعلوماتي أن يوثق جميع مراحل عملية البحث، بحيث يشير إلى زمان البحث ومكان المعلومة وكيفية الحصول عليها، وأن يستخدم البرمجيات التي تحافظ على مواقع الوبّ التي عمل بها؛ لأنه من المعروف أن المعلومات تتغير على الإنترنت من لحظة إلى أخرى[2].

وقد يتخذ الدليل الرقمي المستمد من الحاسوب أو الإنترنت شكل المخرجات الورقية التي يتم الحصول عليها عن طريق الطابعات أو الراسمات، كما يمكن أن يتخذ الشكل الإلكتروني كالأشرطة والأقراص الليزرية وغيرها من الأشكال الإلكترونية. وإلى جانب ذلك يوجد مخْرَج ثالث وهو عرض المعلومات والبيانات المتعلقة بالدليل الرقمي عن طريق شاشة الحاسوب. ويطلق على جميع هذه الأشكال مصطلح **مخرجات الحاسوب**[3].

ومن أمثلة القضايا التي تظهر دور الإنترنت في عملية التحقيق، قضية تتعلق بالاحتيال عبر الإنترنت، تتلخص وقائعها بقيام شخص يدعى "كوري ستيل" Cory Steele من ولاية "مينسوتا" الأمريكية، وهو صاحب شركة لتجارة الأدوية اسمها Advanced Express System، بإنشاء موقع لصيدلية غير شرعية على الإنترنت باسم Swift RX.com، حيث كان يقوم بالاحتيال على

---

(1) Eoghan Casey: op-cit, P-451.

(2) Eoghan Casey: op-cit, P-452.

(3) د.هلالي عبد اللاه أحمد: حجية المخرجات الكمبيوترية في المواد الجنائية، النسر الذهبي للطباعة– القاهرة، 2002، ص15–16.

الناس عبر هذا الموقع، عن طريق عرض الأدوية للبيع بدون وصفات طبية، وتلقي الثمن عبر الإنترنت من خلال بطاقات الائتمان، وعدم إرسال هذه الأدوية إلى المشترين.

وقد بدأت مجريات هذه القضية عندما لاحظ أحد المستأجرين في البناء الذي يوجد فيه مقر شركة المدعو "كوري" مظاهر الثراء الفاحش على هذا الأخير، الذي كان يملك عدة سيارات فخمة مثل Lamborghini ، Mercedes ،Ferrari، فقام هذا الجار بالبحث عن اسم الشركة عبر الإنترنت، حيث تبين له أن لهذه الشركة عدة مواقع إلكترونية، وأن هناك الكثير من الأشخاص الذين كانوا يشتكون من احتيالات هذه الشركة. عندها اتصل بمكتب التحقيقات الفيدرالي FBI وأعلمهم بهذه المعلومات.

وبعد تلقي هذا الإخبار، بدأ أحد المحققين في مكتب التحقيقات الفيدرالي بجمع معلومات إضافية عن المدعو"كوري" وذلك عن طريق محركات البحث مثل google و whois، حيث تبين بأن الموقع الإلكتروني للصيدلية Swift RX.com كان مسجلاً على مزود خدمة إنترنت في سويسرا، وله عنوان تجاري في المملكة المتحدة، وكان ذلك بهدف عرقلة عملية التعقب من قبل المحققين، كما تبين بأن هناك العديد من مواقع الصيدليات غير الشرعية على الإنترنت التي تعود لشركة المدعو "كوري"، وهذه المواقع مسجلة تحت أسماء وعناوين مختلفة في الولايات المتحدة الأمريكية، ومستضافة من قبل مزودي خدمة الإنترنت في تكساس، وأوهايو، ومينيسوتا.

كما توصل المحقق المسؤول عن هذه القضية إلى معلومات تفيد بأن المدعو "كوري" كان يستخدم مبرمجة حاسوب لاختراق المواقع الإلكترونية للصيدليات المنافسة عبر الإنترنت، وذلك بهدف سرقة المعلومات المتعلقة بالزبائن، إضافةً إلى أن "كوري" كان يتعامل مع مجموعة من الأفراد القادرين

على سرقة عناوين الإنترنت، حيث كانت هذه العناوين المسروقة تستخدم في إرسال الإعلانات الدوائية الوهمية إلى الزبائن.

وبعد جمع هذه المعلومات من قبل المحقق، قام بإرسال تقريره إلى معاونة المحامي العام في أمريكا، التي قامت بتشكيل فريق لمتابعة التحقيق والبحث عن معلومات إضافية تتعلق بالمدعو "كوري"، وقررت على الفور إغلاق مواقع الصيدليات غير الشرعية على الإنترنت، وأصدرت عدة مذكرات تفتيش لمقر الشركة، حيث قام فريق التحقيق بمصادرة مجموعة من الحواسيب من هذا المقر.

وقد تمّ مراجعة وتدقيق جميع الأدلة الحاسوبية والوثائقية، كما تمّ ضبط جميع الرسائل الإلكترونية بين المشتبه به وشركائه، حيث أعطت هذه الرسائل الصورة الحقيقية لأعمال المدعو "كوري" والتاريخ الكامل لهذه الأعمال، كما تمّ سماع ما يقرب من مئة شاهد في هذه القضية. وقد تبيّن بأن مبيعات الصيدليات غير الشرعية كانت تصل إلى /28/ مليون دولار شهرياً من خلال استخدام/17/ موقعاً إلكترونياً.

أما المدعو "كوري"، فقد تمّ إلقاء القبض عليه في المطار بعد عودته من الخارج، حيث كان يقوم بالبحث عن أماكن ليؤسس فيها أعماله في الخارج، وقد حُكم عليه بالسجن لمدة /20/ عاماً، وبمصادرة ما يعادل خمسة ملايين دولار من ممتلكاته[1].

وفي قضية احتيال أخرى تظهر دور الإنترنت في التحقيقات، تتلخص وقائعها بأن مكتب النائب العام في مقاطعة Harris التابعة لولاية New Jersey الأمريكية، تلقى عدة شكاوى تتعلق بعمليات احتيال عبر الإنترنت، حيث كان هناك أشخاص يقومون بسرقة هوية الغير، ويستخدمون البيانات

(1) Joseph T.Wells, op-cit, P-1 to 10.

الشخصية العائدة للغير في طلبات شراء عبر الإنترنت من مواقع بعض الشركات التي تبيع الأجهزة الإلكترونية كالحواسيب والكاميرات وغيرها، وكانوا يستخدمون بيانات بطاقات الائتمان المسروقة في عملية الدفع عبر الإنترنت. وبعد أن قامت الشركة بإرسال الأجهزة المطلوبة إلى عناوين المشترين، تبين لها بأن أصحاب هذه البطاقات لم يكونوا على علم بطلبات الشراء هذه.

ومن أكثر الشركات التي وقعت ضحية لعمليات الاحتيال هذه، شركة Hewart Package وهي شركة كبيرة لتصنيع الحواسيب، وشركة photo street co. وهي شركة تبيع الأجهزة الإلكترونية بالتجزئة.

وقد انطلقت عملية التحقيق التي قام بها مكتب التحقيقات الفيدرالي FBI من مراجعة السجلات المتعلقة بشحن البضائع في إحدى الشركات التي تعرضت للاحتيال، حيث أظهرت هذه السجلات أن البضائع كانت تشحن عن طريق شركة للشحن تسمى National courier transport company، وأن جميع البضائع المختلسة كانت تسلم عن طريق سائق شحن يعمل في هذه الشركة يدعى "روجر" Roger. وبناءً على ذلك تمّ وضع هذا السائق تحت المراقبة، التي أظهرت فيما بعد أن البضائع المختلسة كانت تسلم إلى أشخاص يقيمون في منطقة مليئة بموزعي المخدرات والأحداث الجانحين.

وفي نفس الوقت قام مكتب التحقيقات الفيدرالي FBI، بتعقب عنوان الإنترنت العائد لأحد طلبات الشراء الإلكترونية المريبة، حيث تبيّن بأن الطلب أُرسل عن طريق حاسوب موجود في منزل شخص يدعى "جيري" Jerry. وعلى أثر ذلك حصل مكتب التحقيقات الفيدرالي على إذن بتفتيش حاسوب المدعو "جيري" الموجود في منزله، وبعد إجراء التفتيش والتحقيق معه، اعترف "جيري" أمام المحققين بأن جاره المدعو "كيث" Keith كان يستعمل الحاسوب الموجود في منزله من أجل إجراء طلبات الشراء الاحتيالية عبر الإنترنت.

وقد تضمن الاعتراف أسلوب الاحتيال الذي تمّ استخدامه، إذ إن أسماء الضحايا وأرقام بطاقاتهم الائتمانية كان يتم الحصول عليها عن طريق فواتير الزبائن في أحد متاجر بيع الألبسة، حيث كان أحد العاملين في هذا المتجر يقوم بتزويدهم بها، ثم تجري عملية البحث عبر الإنترنت للربط بين الأسماء التي تمّ الحصول عليها والعناوين الأصلية لتلك الأسماء، إضافةً إلى أرقام الهواتف، وبعد ذلك تستخدم هذه الأسماء وأرقام بطاقات الائتمان في عمليات الشراء من المواقع الإلكترونية للشركات المستهدفة، وكانت البضائع تسلّم إلى عناوين أشخاص آخرين من أفراد العصابة ليوقعوا على استلامها.

وقد لعبت الأدلة الرقمية دوراً هاماً في هذه القضية، فقد تمّ العثور على ما يزيد عن /900/ صفحة من الأدلة الرقمية في الحاسوب الذي استخدم في عمليات الاحتيال، تضمنت المواقع الإلكترونية التي كان "جيري" يقوم بزيارتها للبحث عن عناوين الضحايا.

وبعد أن تمّ إلقاء القبض على جميع أفراد العصابة، حُكم على الأشخاص الذين كانوا يتسلمون البضاعة، بالحرية المراقبة لضآلة دورهم، كما حُكم على السائق "روجر" بوضعه أيضاً تحت الحرية المراقبة، وذلك بسبب حسن تعاونه في التحقيق ولعدم وجود أسبقيات له. أما "كيث" فقد حُكم عليه بالسجن ثلاث سنوات. وحُكم على "جيري" بالسجن لمدة عشر سنوات؛ لأنه كان يقوم أيضاً بتوزيع المخدرات إضافة إلى أعماله الاحتيالية[1].

**ومن الملاحظ** بعد استعراض هاتين القضيتين بأن الدليل الرقمي يتمتع بأهمية بالغة في عملية التحقيق بجريمة الاحتيال عبر الإنترنت، إلاّ أنه لا بدّ من أن يكون هناك دائماً أدلة مادية (كالاعتراف مثلاً) يتم الاستناد إليها إلى

---

(1) Joseph T.Wells, op-cit, P-219 to 228.

جانب الدليل الرقمي، حتى تكتمل صورة الجريمة، فالقضاء كما رأينا لم يقم بإدانة المدعى عليهم إلاّ بعد أن توفرت مثل هذه الأدلة.

# المطلب الثاني
# حجية الدليل الرقمي

لا تقف الصعوبات التي تواجه الدليل الرقمي عند حد كيفية الحصول عليه وإجراءات حفظه، بل تمتد إلى مدى القوة الثبوتية التي يتمتع بها هذا الدليل، ومدى حرية قاضي الموضوع بالاقتناع به؛ لبناء الحكم على أساسه بالبراءة أو الإدانة. لذلك حاول المشرع والقضاء والفقه المقارن التصدي لهذه المسألة، وذلك بتحديد الشروط التي يجب توفرها في الدليل الرقمي أو في مخرجات الحاسوب، حتى يمكن قبوله من قبل القاضي الجزائي.

وبناء على ما تقدم، سنتناول حجية الدليل الرقمي في الولايات المتحدة الأمريكية وإنكلترا وفرنسا، والمنظمة الدولية لدليل الحاسوب والفقه العربي.

## أولاً- الولايات المتحدة الأمريكية:

تبنّى قانون الإثبات الفيدرالي في المادة /1002/ منه قاعدة **الدليل الأفضل**، ويقصد بهذه القاعدة أنه عند إثبات مضمون كتابات أو سجلات أو صور، فإن أصل هذه الكتابات أو السجلات أو الصور يجب أن يكون متوفراً، أي يجب تقديمه إلى المحكمة[1].

---

(1) The Federal Rules of Evidence.

يتضمن هذا القانون القواعد المقبولة في الإثبات أمام المحاكم الاتحادية في الولايات المتحدة الأمريكية، في حين أن محاكم الولايات تتبع قواعدها الخاصة مثل "كاليفورنيا" و"واشنطن". وقد وُضِعَ هذا القانون بناء على اقتراح المحكمة العليا في الولايات المتحدة الأمريكية أول مرة عام 1975، وجرى تعديله عدة مرات، وهو متوفر على الإنترنت مع تعديلاته حتى 2008/12/1 على الموقع www.wikipedia.org أو www.lawsource.com ومشار إليه عند د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت,المرجع السابق، ص988.

وقاعدة الدليل الأفضل التي تعبر عن أصالة الدليل تقف حائلاً أمام الدليل الرقمي، لأن ما يتم تقديمه إلى المحكمة ليس الملفات الإلكترونية المخزنة في الحاسوب، وإنما نسخ عن هذه الملفات. ولذلك فقد حسم المشرع الأمريكي هذه المسألة لصالح الدليل الرقمي في المادة 1001/3 من قانون الإثبات الأمريكي والتي نصت على ما يلي:

(إذا كانت البيانات مخزنة في حاسوب أو آلة مشابهة، فإن أي مخرجات مطبوعة منها أو مخرجات يمكن قراءتها بالنظر إليها وتعكس دقّة البيانات، تعدّ بيانات أصلية) [1].

ووفقا لهذه المادة، فإن البيانات أو المعلومات التي تمّ الحصول عليها من الإنترنت، والتي تمّ استخراجها بواسطة الطابعة، تعدّ دليلاً أصلياً كاملاً، ولا حاجة لجلب الحاسوب إلى قاعة المحكمة.

أما فيما يخص القوة الإثباتية للسجلات الإلكترونية، فإن المرشد الفيدرالي الأمريكي لتفتيش وضبط الحواسيب الصادر في عام 2002 يميز بين نوعين من السجلات، وهما:

**النوع الأول– السجلات المخزنة في الحاسوب:**

وهي الوثائق الإلكترونية التي تحتوي على كتابات عائدة لشخص ما، ومن أمثلتها رسائل البريد الإلكتروني، وملفات الورد Word ، ورسائل غرف الدردشة

---

(1) Albert .J. Mercella, op-cit, 26.

وأيضاً د.عمر بن يونس: الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي,المرجع السابق، ص 441.

على الإنترنت. وهذه الوثائق تتضمن إفادات بشرية، وتعدّ كالشهادة على السماع في مجال الإثبات[1].

**النوع الثاني– السجلات المأخوذة من الحاسوب:**

وهي عبارة عن نتائج برامج الحاسوب التي لا تمسها الأيدي البشرية، ومن أمثلتها سجلات الدخول إلى الإنترنت، وسجلات الهاتف، وإيصالات الصراف الآلي وغيرها. فهذه السجلات لا تتضمن إفادات بشرية، وإنما هي عبارة عن نتائج البرامج الحاسوبية. فالصراف الآلي مثلاً يمكن أن يعطي إيصالاً يتضمن أن /100/ دولار أمريكي قد تم إيداعها في الحساب عند الساعة 2.25 مساءً، وهذا النوع من السجلات يمكن للمحاكم أن تأخذ به، إذا كان برنامج الحاسوب يؤدي عمله على نحو جيد وسليم[2].

وبناءً على هذه القواعد، فإن الفقه في أمريكا يرى بأنه حتى يكون الدليل الرقمي مقبولاً أمام المحكمة، يجب أن يتوفر فيه الشروط التالية[3]:

- أن لا يطرأ على محتويات السجل الإلكتروني أي تغيير، أي أن يكون الدليل المقدم إلى المحكمة هو نفس الدليل الذي تمّ جمعه، ويمكن

---

(1) الشهادة على السماع وفق قواعد الإثبات الفيدرالية تقبل على سبيل الاستثناء في المجالات التالية: الأعمال، المذاكرات اليومية، التقارير، السجلات، الأحداث، الشروط، الآراء، التشخيص. فإذا تمّ حفظ هذه الأشكال في الحاسوب بالأسلوب المعتاد ووفق نظام العمل السائد، فإنها تعد كالشهادة على السماع.
Albert .J. Mercella, op-cit, 22.
وأيضاً د.عمر بن يونس: الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي, المرجع السابق، ص420–421.

(2) Albert .J. Mercella, op-cit, 23.
وأيضاً د.عمر بن يونس: الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي, المرجع السابق، ص420–421.

(3) Eoghan casey,op-cit,p.78 .

للشخص الذي قام بجمع الدليل أن يشهد بذلك أمام المحكمة، وهذا ما يطلق عليه مفهوم "**سلسلة الرعاية**" Chain of Custody، ويقصد بذلك أن الدليل الرقمي منذ لحظة جمعه وحتى لحظة تقديمه إلى المحكمة لم يطرأ عليه أي تغيير، ولا يوجد أي احتمال للعبث به، وأنه تمّت مراعاة سلامته حتى يبقى بنفس الحالة التي وجد عليها[1].

- أن تكون المعلومات الموجودة في السجل، قد صدرت فعلاً عن المصدر المزعوم، سواء كان هذا المصدر الإنسان أم الآلة.
- أن تكون المعلومات الموجودة في السجل، والمتعلقة بالوقت والتاريخ، معلومات دقيقة.

أما القضاء الأمريكي فقد تعرض في العديد من القضايا إلى مسألتي الأصالة والصحة. ففي إحدى القضايا، قررت المحكمة: "إن عضو مكتب التحقيقات الفيدرالي FBI الذي كان حاضراً عندما تمّ ضبط الحاسوب الخاص بالمتهم، يمكن أن يقرر صحة الملفات المضبوطة."[2]. وفي قضية أخرى قبلت المحكمة سجلات الهاتف بعد أن أكّدت موظفة الفواتير في الشركة أصالة هذه السجلات[3]. كما قبلت إحدى المحاكم الدليل الرقمي رغم الدفوع المتعلقة بالعبث بهذا الدليل، لأن هذه الدفوع جاءت على شكل تخمين، دون أن يوجد

---

(1) Dr. Henry B. wolfe, Forensics and the emerging importance of electronic Evidence gathering, OTAGO university, 2001, P-4, available on line. www.e-evidence.info.
Albert .J. Mercella, op-cit, 343.

(2) Witaker, 127 F.3d 595, 601 (7th cir. 1997).
مشار إليه عند د.عمر بن يونس: الإجراءات الجنائية في القانون الأمريكي، المرجع السابق، ص 425.

(3) Eoghan casey,op-cit,p.170.

أي دليل يدعمها[1]. وفي إحدى القضايا قررت المحكمة: "إن حقيقة وجود احتمال بتعديل البيانات الموجودة في الحاسوب غير كافية للقول بعدم جدارة الدليل."[2] كما ذكرت وزارة العدل الأمريكية في المرشد الفيدرالي لتفتيش وضبط الحواسيب، وصولاً إلى الدليل الإلكتروني في التحقيقات الجنائية: "إن غياب دليل واضح على حدوث العبث في الدليل، لا يؤثر على أصالة ودقة سجلات الحاسوب"[3].

## ثانياً– إنكلترا:

في عام 1948 صدر في إنكلترا قانون الشرطة والإثبات الجنائي (Pace)[4]. وقد حدد هذا القانون الصلاحيات لشرطة "إنكلترا" و"ويلز"، وهو قانون يهدف إلى إقامة التوازن بين قوى الشرطة البريطانية وحقوق الأفراد، ويتناول آلية تفتيش الأماكن، وكيفية معاملة المشتبه بهم، والاعتقال وغير ذلك. وقد تم تعديل هذا القانون في 14 تشرين الأول عام 2002.

كما ركّز هذا القانون بصفة أساسية على قبول مخرجات الحاسوب كدليل في الإثبات، حيث حدد المشرع الإنكليزي في المادة 69 من هذا القانون الشروط الواجب توفرها في المستند الناتج عن الحاسوب، حتى يُقبل كدليل في الإثبات. وهذه الشروط هي[5]:

---

(1) Witaker, 127 F.3d at 602, Eoghan casey,op-cit,p.170.

(2) Bouallo, 858 F.2d 1427, 1436 (9th cir.1988). Eoghan casey, op-cit, p.170.

(3) Eoghan casey,op-cit,p.170.

(4) وهو اختصار The Police Criminal Evidence Act ومتوفر على الإنترنت على موقع القوانين البريطانية www.briTishlaw.org.uk.

(5) فهد سلطان محمد أحمد بن سليمان: المرجع السابق، ص146. د. هلالي عبد اللاه أحمد: المرجع السابق، ص53. د. عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت,المرجع السابق، ص993.

- عدم وجود أسس معقولة للاعتقاد بأن البيان يفقد الدقة بسبب الاستخدام غير المناسب أو الخاطئ للحاسوب.
- أن الحاسوب كان يعمل في جميع الأحوال بصورة سليمة، وإذا لم يكن كذلك، فإن أي جزء لم يكن يعمل فيه بصورة سليمة، أو كان معطلاً عن العمل، لم يكن ليؤثر في إخراج المستند أو دقة محتوياته.

وقد علق مجلس اللوردات على المادة 69 المشار إليها، بأنه: "يمكن للشهادة الشخصية الصادرة عن شخص على علم بطريقة تشغيل الحاسوب، أن تعطي الثقة بالدليل، وليس بالضروري أن يكون هذا الشخص خبيراً بالحاسوب"[1]. وبناءً على ذلك قبلت المحاكم الإنكليزية –فيما يتعلق بسلامة نظام الحاسوب– بشهادة أشخاص لديهم علم بطريقة عمل نظام الحاسوب[2].

## ثالثاً– فرنسا:

يتناول الفقه في فرنسا حجية مخرجات الحاسوب في المواد الجنائية، في إطار مسألة أوسع وأعم، هي مسألة قبول الأدلة الناشئة عن الآلة أو الأدلة العلمية، مثل الرادارات، وأجهزة التصوير، وأشرطة التسجيل، وأجهزة التنصت.

أما القضاء فقد قبل هذه الأدلة إذا توفرت فيها مجموعة من الشروط، من أهمها أن يتم الحصول عليها بطريقة شرعية ونزيهة، وأن يتم مناقشتها حضورياً من قبل الأطراف. وقد قضت محكمة النقض الفرنسية بأن أشرطة التسجيل الممغنطة، التي يكون لها قيمة دلائل الإثبات، يمكن أن تكون صالحة للتقديم أمام القضاء الجنائي[3].

---

(1) Eoghan casey,op-cit,p.170

(2) .R.V Shephard. 1933, Eoghan casey,op-cit,p.170

(3) Cass. Criw. 28 avr. 1987, Bull. Criw.no.173

أما بالنسبة إلى قناعة القاضي الجزائي، فإن الأدلة الإلكترونية تخضع لحرية القاضي في الاقتناع الذاتي، بحيث يمكن أن يطرح مثل هذه الأدلة – رغم قطعيتها من الناحية العلمية– عندما يجد أن الدليل الإلكتروني لا يتسق منطقياً مع ظروف الواقعة وملابساتها[1].

## رابعاً– المنظمة الدولية لدليل الحاسوب:

تأسست المنظمة الدولية لدليل الحاسوب IOCE[2]في عام 1995، وتتكون من الجهات الحكومية المسؤولة عن تطبيق القانون، أو من الهيئات الحكومية التي تزاول التحقيق في مجال الحاسوب. وتهدف هذه المنظمة إلى تزويد الجهات الدولية القانونية بكيفية تبادل المعلومات بتحقيقات جرائم الحاسوب والمسائل ذات الصلة بالمعلوماتية الشرعية. كما تقوم بتنظيم عملية الاتصال بين أعضائها، وتقدم التوصيات اللازمة في هذا المجال، وتقيم المؤتمرات المتعلقة بنشاطاتها.

وإضافةً إلى ذلك فإن المنظمة وضعت المعايير المطلوبة في دليل الحاسوب، وقد تمت المصادقة على هذه المعايير خلال المؤتمر الدولي للبحث المعلوماتي والجريمة التقنية، المنعقد في تشرين الأول عام 1999 (IHCFC)[3]، وهذه المعايير هي[4]:

- عدم تغير الدليل أثناء ضبطه.
- أن تتم عملية الضبط من قبل شخص مؤهلٍ في المعلوماتية الشرعية.

---

مشار إليه عند: د. هلالي عبد اللاه أحمد: المرجع السابق، ص43. د. علاء عبد الباسط خلاف: المرجع السابق، ص450.

(1) علي حسن محمد الطوالبة: المرجع السابق، ص191.

(2) وهو اختصار لـInternational Organization on computer Evidence.

(3) وهو اختصار لـInternational Hi- tech crime and Forensics conference.

(4) ALBERT. J.Marcella, op- cit, p.141. And available on www. Ioce.org.

- جميع النشاطات المتعلقة بالضبط والوصول والتخزين ونقل الدليل الرقمي، يجب أن تكون موثقة ومحفوظة بغرض التدقيق.
- أن يكون الشخص الذي بحوزته الدليل الرقمي مسؤولاً عن جميع الإجراءات المتعلقة بهذا الدليل.
- أن تكون الجهات المسؤولة عن ضبط وتخزين ونقل الدليل الرقمي والوصول إليه مسؤولة عن تطبيق هذه المبادئ.

## خامساً- الفقه العربي:

يرى جانب من الفقه العربي أن للقاضي الجزائي مطلق الحرية في أن يصل إلى الحقيقة من أي دليل قانوني مهما كان نوعه، بما في ذلك الدليل الرقمي الذي يعد من قبيل القرائن. إلا أنه يشترط في هذا الدليل أن يتوفر فيه ما يلي[1]:

- الانسجام مع أحكام القانون، أي الحصول على الدليل الرقمي بوسيلة مشروعة.
- إمكانية مناقشة الدليل الرقمي.
- أن يكون الدليل الرقمي غير قابل للشك فيه.

كما يرى الفقه بأن مخرجات الحاسوب ليست إلا نوعاً من أنواع الأدلة العلمية (كالبصمة الوراثية، والرادارات وغيرها)، وفي إطار قناعة القاضي يميز هذا الفقه بين أمرين، هما[2]:

الأمر الأول: القيمة العلمية القاطعة للدليل.

---

(1) د.علي جبار الحسيناوي: المرجع السابق، ص142. علي حسن محمد الطوالبة: المرجع السابق، ص178. د. علاء عبد الباسط خلاف: المرجع السابق، ص451.

(2) د.هلالي عبد اللاه أحمد: المرجع السابق، ص46. د. جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، المرجع السابق، ص22.

الأمر الثاني: الظروف والملابسات التي وجد فيها هذا الدليل.

فتقدير القاضي لا يتناول القيمة العلمية القاطعة للدليل، ذلك لأن قيمة الدليل تقوم على أسس علمية دقيقة، ولا حرية للقاضي في مناقشة الحقائق العلمية الثابتة. أما ما يتعلق بالظروف والملابسات التي وجد فيها هذا الدليل، فإنها تدخل في نطاق تقديره الشخصي لأنها من طبيعة عمله، ومن ثم فللقاضي الجزائي أن يطرح الدليل المستخرج من الحاسوب عندما يجد أن وجوده لا يتفق منطقياً مع ظروف الواقعة. فمجرد توفر الدليل العلمي لا يعني أن يحكم القاضي مباشرة، دون البحث بالظروف والملابسات[1].

## رأي الباحث في مسألة الدليل الرقمي:

يستمد القاضي الجزائي قناعته من أي دليل يطمئن إليه من الأدلة التي تقدم في الدعوى دون التقيد بدليل معين، ما لم ينص القانون على غير ذلك؛ فلا يوجد أدلة يحظر القانون عليه قبولها. فالقانون أمدّ القاضي الجزائي بسلطة واسعة وحرية كاملة في مجال الإثبات، فله أن يأخذ من الأدلة ما تطمئن له عقيدته، ويطرح ما لا يرتاح إليه. وهذا ما نصت عليه الفقرة الأولى من المادة 175 من قانون أصول المحاكمات الجزائية بقولها:

(تقام البينة في الجنايات والجنح والمخالفات بجميع طرق الإثبات، ويحكم القاضي حسب قناعته الشخصية).

و**يرى الباحث** أن الدليل الرقمي يندرج تحت طائفة القرائن القضائية، ويمكن للقاضي الجزائي الأخذ به، سواء في إطار الإدانة أم البراءة، إذا توفرت في هذا الدليل الشروط التالية:

1- **المشروعية:** أي أن يتم الحصول على الدليل الرقمي بصورة قانونية.

---

(1) د. هلالي عبد اللاه أحمد: المرجع السابق، ص47.

2- **الصحة والمطابقة:** أي أن يكون الدليل الرقمي المقدم إلى المحكمة هو نفس الدليل الذي تم جمعه، وأن لا يطرأ على هذا الدليل أي تغيير خلال فترة حفظه.

3- **الدقة:** أي أن نظام الحاسوب الذي استخرج منه الدليل يعمل على نحو دقيق وسليم، بحيث لا يتطرق الشك في دقته.

أما بالنسبة إلى **الدفوع** المتعلقة بهذه الشروط، وخاصة شرطي الصحة والدقة، فإن هذه الدفوع يجب أن لا تنال من قيمة الدليل الرقمي، إذا جاءت على شكل تخمين، دون أن يوجد دليل يدعمها. وهذا ما سارت عليه المحاكم الأمريكية كما رأينا.

وفيما يتعلق **بكيفية تقدير قيمة الدليل الرقمي**، فإن **الباحث يؤيد** ما ذهب إليه الفقه العربي من ضرورة التمييز بين أمرين، هما:

الأمر الأول: القيمة العلمية القاطعة للدليل.

الأمر الثاني: الظروف والملابسات التي وجد فيها الدليل.

فالقاضي ليس له أن ينازع فيما استقرت عليه تكنولوجيا المعلومات والعلوم التقنية من الناحية العلمية، وإنما له أن يقدر الظروف والملابسات التي أحاطت بهذا الدليل، ويساعده في هذا التقدير الأدلة التقليدية (الاعتراف والشهادة وغيرها) التي توجد عادة إلى جانب الدليل الرقمي، فله أن يرفض الدليل الرقمي إذا لم يقتنع بظروف الواقعة وملابساتها.

والواقع ليست هي المرة الأولى التي يواجه فيها القضاء السوري الأدلة العلمية، فالمحاكم قبلت الدليل المستمد من آلات التصوير في مجال مخالفات

السير، كما هو الحال في كاميرات المراقبة التي توضع على الطرق السريعة[1]، كما قبلت الدليل المستمد من البصمة الوراثية DNA سواء في إدانة المتهم أم تبرئته[2]. فجميع هذه الأدلة العلمية عرضت على القضاء على أنها من القرائن القضائية وخضعت لتقدير المحاكم.

وفي مجال تقدير الدليل الرقمي، لابد لنا أن نتساءل عن حجية التوقيع الإلكتروني المصادق عليه في المسائل الجزائية، وخاصة بعد أن صدر في سورية قانون التوقيع الإلكتروني رقم 4 لعام 2009[3]. فعلى سبيل المثال، **إذا كانت هناك رسالة إلكترونية تحمل مضموناً احتيالياً، وموقعة توقيعاً إلكترونياً مصادقاً، فهل يملك القاضي الجزائي حرية تقدير الدليل الرقمي المستمد من هذه الرسالة؟**

---

(1) تنص الفقرة ب من المادة 205 من قانون السير رقم 31 لعام 2004 والمعدل بالمرسوم التشريعي رقم 11 لعام 2008 على ما يلي: (تعتبر الوثائق الصادرة باستخدام أجهزة الرقابة الآلية لضبط مخالفات السير بما في ذلك أجهزة التصوير التي تعمل بصورة يدوية أو آلية، بينة فنية مقبولة في كل إجراء قضائي، إذا احتوت الصورة أثناء التقاطها رقم لوحة المركبة، ومكان وجودها، وتاريخ ووقت ارتكاب المخالفة). وقد كانت محاكم السير قبل هذا التعديل تأخذ بالصور الناتجة عن الرادارات على الطرق السريعة.

(2) قررت محكمة الجنايات الثانية بريف دمشق في قرار حديث لها، إدانة المتهم بجناية القتل, بعد أن تم أخذ عينات من بقع الدم الموجودة على ملابسه، حيث تم تحليل الحمض النووي لهذه العينات، فتبين بأنها تعود إلى الضحية. الدعوى أساس 608 لعام 2008، قرار رقم 461 تاريخ 2008/10/30.

(3) تنص المادة 3 من قانون التوقيع الإلكتروني على ما يلي: (يعد التوقيع الإلكتروني المصدق، المدرج على وثيقة إلكترونية، مستجمعاً للشروط المطلوبة للحجية في الإثبات, وهي:

1- ارتباط التوقيع بالموقع وحده دون غيره، وكفايته للتعريف بشخص الموقع.===

==2- سيطرة الموقع وحده دون غيره على منظومة إنشاء التوقيع الإلكتروني المستخدمة.

3- ارتباط التوقيع الإلكتروني بالوثيقة الإلكترونية ارتباطاً لا يمكن بعده إحداث أي تعديل أو تبديل على الوثيقة دون ظهور أثر قابل للتدقيق والكشف).

يرى بعض الفقهاء أن حجية التوقيع الإلكتروني تختلف في الإثبات المدني عن الإثبات في الأمور الجزائية، لأن الإثبات المدني- حسب هذا الرأي- يخضع لقواعد شكلية، أما الإثبات الجزائي فيخضع تقديره لمطلق سلطة قاضي الموضوع واقتناعه بصحته وقوته الإثباتية[1].

**والباحث يؤيد** ما ذهب إليه هذا الرأي الفقهي، لأن قانون التوقيع الإلكتروني لم يعط أية حجية للتوقيع الإلكتروني في المسائل الجزائية، وهذا مستمد من الفقرة أ من المادة الثانية من هذا القانون التي تنص على ما يلي: (للتوقيع الإلكتروني المصدق، المدرج على وثيقة إلكترونية، في نطاق المعاملات المدنية والتجارية والإدارية، ذات الحجية المقررة للأدلة الكتابية في أحكام قانون البينات، إذا روعي في إنشائه وإتمامه الأحكام المنصوص عليها في هذا القانون، والنواظم والضوابط التي يصدرها الوزير، بناء على قرار مجلس إدارة الهيئة المنصوص على إحداثها في الفصل الثالث من هذا القانون).

وكما هو واضح من نص هذه المادة ، فإن حجية التوقيع الإلكتروني المصدق تقتصر على المسائل المدنية والتجارية والإدارية، دون المسائل الجزائية، وعليه فإن الوثيقة الإلكترونية أو الرسالة الإلكترونية، الموقعة توقيعاً إلكترونياً مصادقاً، تعد كباقي الأدلة الرقمية التي من الممكن أن تعرض على القاضي الجزائي، والتي تخضع لتقديره من ناحية الظروف والملابسات التي وجدت فيها هذه الوثيقة أو الرسالة الإلكترونية.

وبناءً على ما تقدم، فإن **الباحث يقترح** على المشرع السوري في مشروع قانون الجريمة الإلكترونية، أن يترك مسألة تقدير الدليل الرقمي إلى قناعة القاضي الجزائي أسوة بالقواعد العامة، وذلك إذا توفرت في هذا الدليل الشروط

---

(1) علي حسن محمد الطوالبة: المرجع السابق، ص195. فهد سلطان محمد أحمد بن سليمان، المرجع السابق، ص154.

التي سبقت الإشارة لها، بحيث تعد هذه الشروط متوفرة في الدليل ما لم يثبت عكس ذلك. و**نقترح** أن يكون النص على الشكل التالي :

( تقدر المحكمة قيمة الدليل الرقمي، بشرط أن يكون نظام الحاسوب المستمد منه الدليل يعمل على نحو سليم، وألا يطرأ على الدليل المقدم إلى المحكمة أي تغيير خلال فترة حفظه. ويعد الدليل المقدم إلى المحكمة مستجمعاً لهذين الشرطين ما لم يثبت عكس ذلك .)

أما بالنسبة إلى شرط المشروعية، فلا داعي إلى الإشارة له؛ لأن القواعد العامة تكفل وجوده .

وبعد أن بّين الباحث رؤيته الموضوعية والإجرائية لجريمة الاحتيال عبر الإنترنت، سيتناول ما توصل إليه من نتائج ومقترحات من خلال خاتمة الرسالة.

## الخاتمــة

قدمنا في هذه الأطروحة دراسة متواضعة لجريمة الاحتيال عبر الإنترنت، تناولنا فيها جزئيات هذه الجريمة ضمن رؤية موضوعية وإجرائية وفق ما تقتضيه أساليب الدراسة التحليلية التأصيلية.

ولعله من الواجب علينا في نهاية هذه الدراسة، أن نضع ضمن إطار واحد النتائج التي توصل إليها الباحث في مختلف جوانب الرسالة. **وهذه النتائج هي :**

1- يمكن تعريف جريمة الاحتيال عبر الإنترنت بأنها: **(الاستيلاء على مال الغير بالخداع عبر تقنية الإنترنت).** ويرى **الباحث** أنه من الأفضل عدم ذكر وسائل الاحتيال وصوره عند تعريف هذه الجريمة، نظراً إلى طبيعة وسائل الاحتيال عبر الإنترنت التي يمكن أن تتخذ صوراً لا حصر لها.

2- **فيما يتعلق بتطبيق النصوص التقليدية لجريمة الاحتيال، على الاحتيال عبر الإنترنت، فالباحث** يرى إمكانية تطبيق هذه النصوص التقليدية للأسباب التالية:

أ- إن البرامج والمعلومات يجب معاملتها على أنها من **الأموال المادية**، لأن الفقه الحديث -كما رأينا- يعترف للمعلومات بصفة المال استناداً إلى قيمتها الاقتصادية، فهي تصلح لأن تكون محلاً للملكية الفكرية، وهي ملك لمن ابتكرها، إضافةً إلى أن المعلومات أو البرامج تشغل حيزاً مادياً في ذاكرة الحاسوب، يمكن قياسه بمقياس معين هو البايت (BYTE)، فهذه المعلومات بطبيعتها عبارة عن إشارات إلكترونية تشبه إلى حد بعيد

الإشارات الكهربائية التي جعلها المشرع السوري من القوى المحرزة التي تنزل منزلة الأشياء المنقولة في تطبيق القوانين الجزائية (المادة 621 من قانون العقوبات). ومن ثم يمكننا أن نعدّ المعلومات مفهوماً يندرج تحت مصطلح القوى المحرزة التي يحميها القانون الجزائي.

ب- إن النشاط الجرمي للاحتيال المتمثل بفعل **الخداع** يمكن أن يقع على أنظمة الحاسوب، لأن الحاسوب مجرد وسيط، وهو يعبر عن إرادة المجني عليه، فهذا الأخير هو من يقوم ببرمجته وفقاً لمتطلباته، ولا يوجد ما يمنع قانوناً من أن يمارس الخداع على أنظمة الحاسوب، وقد رأينا أن جانباً من الفقه الفرنسي سار في هذا الاتجاه.

ج- إن وسيلة **استعمال الدسائس** الواردة في المادة /641/ من قانون العقوبات لها مفهوم واسع بحيث تشمل جميع الوسائل التقنية التي يمكن بها ارتكاب الاحتيال عبر الإنترنت؛ إضافة إلى أن بقية الوسائل الاحتيالية الواردة في المادة /641/ من قانون العقوبات لا يوجد ما يمنع قانوناً من تطبيقها على الاحتيال عبر الإنترنت.

د- وفي مجال **التسليم**، فإن النقود الكتابية أو الإلكترونية يتحقق بها التسليم المطلوب في جريمة الاحتيال، لأنها تعادل تسليم الأموال العادية؛ وهذا ما يعرف بنظرية "التسليم المعادل" التي ابتدعها القضاء الفرنسي، وأيدها جانب من الفقه المصري.

**وغني عن البيان**، أن بعض النصوص المتعلقة بالجرائم التقليدية -كالاحتيال- قد تسعف القضاء في الوقت الراهن لمواجهة هذه الجرائم في حال ارتكابها عبر الإنترنت، مع الأخذ بالحسبان بأن هذه النتيجة لا يمكن تعميمها على جميع الجرائم التقليدية التي يمكن أن ترتكب عبر هذه الشبكة؛ فلا يمكن

مثلاً تطبيق النص المتعلق بخرق حرمة المنزل على الدخول غير المشروع إلى موقع إلكتروني، ولا يمكن تطبيق النص المتعلق بالسرقة على الحصول على معلومات الغير بطريقة غير مشروعة، ولا يمكن أيضاً تطبيق النص المتعلق بتزوير المحرر على تزوير المعلومات أو البيانات.

3- **وفيما يخص صور الاحتيال عبر الإنترنت**، فإن أساليب هذا النوع من الإجرام متنوعة ومتجددة وهي تساير التقدم التكنولوجي. ومع ذلك يمكن أن نميز بين **سبع صور عامة للاحتيال عبر الإنترنت**، وهي : الاستيلاء على أموال المصارف، والاحتيال التجاري، والاحتيال عن طريق الأوراق المالية، وانتحال الشخصية، والاحتيال عن طريق البريد الإلكتروني، والاحتيال المهني، واحتيال الاتصالات. وإن معظم هذه الصور تندرج تحت وسيلة استعمال الدسائس، أو استعمال الاسم المستعار أو الصفة الكاذبة، المنصوص عليهما في المادة /641/ من قانون العقوبات.

أما **الصورة الخاصة المتعلقة بالاحتيال عن طريق بطاقات الائتمان**، فقد رأينا أن الفقه والقضاء المقارن قد أضفى وصف الاحتيال على أغلب الأفعال غير المشروعة المتعلقة ببطاقات الائتمان، كاستخدام بطاقة الائتمان المسروقة أو المزورة في سحب النقود أو الوفاء لدى التجار.

4- وبالنسبة إلى **مسألة الاختصاص**، فإن الاتجاه الغالب في العالم اليوم لحل مشكلة الاختصاص القضائي عبر الإنترنت، هو تطبيق ذات المبادئ المعمول بها لحل مشكلة الاختصاص الجزائي الدولي في الجرائم التقليدية، وهذه المبادئ هي : مبدأ الإقليمية والعينية والشخصية والعالمية.

وتماشياً مع هذا الاتجاه؛ فإن **الباحث** لا يجد ما يمنع قانوناً من تطبيق الصلاحيات الإقليمية والذاتية والشخصية والشاملة المنصوص عليها في قانون العقوبات السوري على جريمة الاحتيال عبر الإنترنت. فمن الثابت فقهاً أن القواعد الإجرائية الجزائية يمكن أن تفسر تفسيراً واسعاً، إضافةً إلى إمكانية اللجوء إلى القياس عند فقدان النص الإجرائي، وذلك بخلاف القواعد الموضوعية . كما يرى **الباحث** ضرورة اعتبار **النطاق العلوي السوري** على الإنترنت (المنتهي بـ sy.) الذي يخضع لإدارة الحكومة السورية جزءاً من الإقليم السوري أو بحكم الأرض السورية، لأن المبررات المتعلقة بسيادة الدولة على إقليمها، التي دفعت المشرع الجزائي إلى اعتبار الطائرة أو السفينة السورية بحكم الأرض السورية، متوفرة في ذلك النطاق العلوي السوري على الإنترنت، فهذا النطاق يحمل العلم السوري أو الجنسية السورية، وبالتالي فإن اعتباره بحكم الأرض السورية يتفق مع فلسفة المشرع السوري.

5- ضرورة إنشاء **جهاز متخصص بمكافحة جرائم الإنترنت** في سورية. وقد سبقت الإشارة إلى أن مشروع قانون الجريمة الإلكترونية السوري نص على إحداث وحدات شرطية متخصصة لمكافحة هذه الجرائم في وزارة الداخلية.

6- يمكن القيام **بالمراقبة الإلكترونية** قياساً على ما ورد في المادة /96/ من قانون أصول المحاكمات الجزائية، التي تسمح لقاضي التحقيق أن يضبط لدى مكاتب البريد كافة الخطابات والرسائل والجرائد والمطبوعات والطرود، ولدى مكاتب البرق كافة الرسائل البرقية، كما يجوز له مراقبة المحادثات الهاتفية، متى كان لذلك فائدة في ظهور الحقيقة.

فإذا كانت العلة من قيام قاضي التحقيق بضبط الرسائل والخطابات والرسائل البرقية والمحادثات الهاتفية تكمن في إظهار الحقيقة، فإن هذه العلة متوفرة

أيضاً في المراقبة الإلكترونية، بما في ذلك مراقبة البريد الإلكتروني. ومن ثم يمكن قياس المراقبة الإلكترونية على مراقبة الرسائل والخطابات والمحادثات الهاتفية، لاتحادهما في العلة، وهي إظهار الحقيقة. وبالتالي يمكن لموظف الضابطة العدلية القيام بالمراقبة الإلكترونية في ظل التشريع السوري بعد أن يحصل على إنابة من قبل قاضي التحقيق المختص.

7- فيما يتعلق **بالمعاينة**، يمكن لموظف الضابطة العدلية القيام بمعاينة مسرح الجريمة الافتراضية في ظل التشريع السوري، كأن يقوم مثلاً بمعاينة الموقع الإلكتروني المستخدم في الاحتيال عبر الإنترنت، ثم يقوم بتجميد الشاشة أو تصويرها للمحافظة على صفحة الوبّ المتعلقة بهذا الموقع من أجل تقديمها للقضاء في وقت لاحق.

8- إن تقديم **الإخبار أو الشكوى عبر الإنترنت** يسهل عملية إعلام السلطات المختصة بوقوع الجريمة، كما يؤمن الحماية لمقدم الإخبار الذي يظلّ مجهولاً في أغلب الأحيان. لذلك **نقترح** على أجهزة العدالة السورية أن تنشأ مواقع إلكترونية متخصصة في تلقي الإخبارات والشكاوى المتعلقة بجرائم الإنترنت.

9- إن نظام **الإرشاد الجنائي عبر الإنترنت** هو من أهم وسائل تحري واستقصاء جريمة الاحتيال عبر الإنترنت، وهو نظام لا بدّ من الأخذ به في سورية للحدّ من هذه الجريمة.

10- أما بالنسبة إلى **تفتيش المكونات المعنوية أو البرمجية للحاسوب، فيرى الباحث** أن النصوص الحالية المتعلقة بالتفتيش في قانون أصول المحاكمات الجزائية[1] تسمح بتفتيش المكونات المعنوية للحاسوب، لأن هذه النصوص سمحت بالتفتيش للبحث عن **الأشياء التي تساعد على إظهار الحقيقة**. ويدخل

(1) المواد 32 و33 و89 و90 من قانون أصول المحاكمات الجزائية.

في مفهوم الأشياء المعلومات أو البرامج، فالمعلومات أو البرامج وإن لم يكن لها كيان مادي محسوس، إلاّ أنها تشغل **حيزاً مادياً** في ذاكرة الحاسوب أو وسائط التخزين، يمكن قياسه بمقياس معين، وهو "البايت" (byte)، وبالتالي فإن البرامج يمكن أن تدخل في نطاق الأشياء المادية. إضافةً إلى أن المكونات المعنوية أو البرمجية للحاسوب تعدّ أثراً من آثار الجريمة عندما تتضمن أدلة تساعد في كشف الحقيقة. ولا يوجد ما يمنع من التوسع في تفسير القواعد الأصولية، بحيث تشمل تفتيش هذه المكونات المعنوية.

**أما فيما يتعلق بتفتيش الحاسوب أو المُخدّم المرتبط بحاسوب المتهم، فيرى الباحث** أن تفتيش الحاسوب الآخر أمر تفرضه أهداف التفتيش والضرورات العملية، إذ إن عدم القيام بتفتيش هذه الأجهزة يفقد التفتيش هدفه الرئيسي، وهو الحصول على الأدلة الرقمية الضرورية لإظهار الحقيقة. **كما أن امتداد التفتيش إلى حاسوب أو مُخدّم موجود في دولة أخرى** لا يعد انتهاكاً لسيادة هذه الدولة، لأن الطبيعة العالمية للإنترنت تسمح بمثل هذا الإجراء، فمتطلبات السرعة في إجراء عملية التفتيش تقتضي عدم انتظار إذن الدولة التي يوجد فيها الحاسوب أو المُخدّم الآخر، مع ضرورة إعلام هذه الدولة في وقت لاحق. **أما بالنسبة إلى مسألة مدى اعتبار الحاسوب جزءاً من المكان المطلوب تفتيشه،** فقد رأينا بأن الواقع العملي في سورية يشير إلى أن إذن التفتيش المتعلق بالمكان الخاص يشمل جميع الحواسيب الموجودة في هذا المكان. و**الباحث يؤيد** هذا التوجه العملي مادام تفتيش أجهزة الحاسوب الموجودة في المكان المطلوب تفتيشه تفيد في إظهار الحقيقة.

11- إن عملية **الضبط** يجب أن تراعى فيها طبيعة الأشياء المضبوطة، ومن ثم فإن ضبط الأدلة الرقمية يجب أن يتناسب مع ماهيتها، بحيث ينصبّ على

جميـع الأجهـزة والأدوات التـي جـرى تخـزين المعلومـات فيهـا؛ لأن ضـبط المعلومات والبيانات لا يمكن أن يتم بمعزل عن وسائط التخزين.

12- وفيما يخص **الشهادة الإلكترونية عبر الإنترنت**، فإن **الباحث** لا يرى مانعاً من اللجوء إليها لإثبات الجرائم الإلكترونية المنصوص عليها في مشروع قانون الجريمة الإلكترونية فقط، لأن الطبيعة العالمية لجرائم الإنترنت تثير في كثير من الأحيان مسألة سماع أقوال الشهود الموجودين خارج القطر، كما إن سماع الشاهد عبر الإنترنت بصورة سمعية ومرئية يساعد المحكمة على تقدير قيمة الشهادة بصورة أفضل بكثير من الاكتفاء بتلاوة أقوال الشاهد السابقة –في حال وجودها– أمام هيئة المحكمة عندما يتعذر حضوره لأي سبب كان. **ويشترط في الشهادة الإلكترونية توفر الشروط التالية:**

أ- أن يتعذر حضور الشاهد مادياً أمام المحكمة، كوجوده مثلاً خارج القطر.

ب- أن تكون الشهادة على قدر من الأهمية.

ج- أن يتم سماع الشهادة الإلكترونية بحضور خبير أو أكثر لضمان انغلاق الدارات الاتصالية مع الشهود.

د- أن يتم تبليغ الشاهد بأي وسيلة كانت قبل موعد الجلسة بمدة معقولة تقدرها المحكمة.

وبهذا التطبيق الضيق يتم الحفاظ على إجراءات سماع الشهود المنصوص عليها في القواعد العامة.

13- يمكن للقاضي أن يختار ما يشاء من **القرائن القضائية** لإثبات جريمة الاحتيال عبر الإنترنت، ما دامت هذه القرائن تشكّل القناعة لديه على ارتكاب المدعى عليه لهذه الجريمة. فنظام الإثبات الحر المتبع في قضائنا الجزائي يسمح له بذلك.

14- لا تختلف أحكام **الاعتراف** في جريمة الاحتيال عبر الإنترنت عن الأحكام العامة للاعتراف في الجرائم التقليدية، فلا يكفي مثلاً مجرد اعتراف المدعى عليه بارتكابه جريمة تحويل الأموال بطريقة غير مشروعة عن طريق اختراق النظام المعلوماتي العائد لأحد المصارف عبر الإنترنت، بل يجب أن يحدّد المعترف الكيفية التي تمّ بها الاختراق، ومن ثم يجب أن يتطابق هذا الاعتراف مع الأسلوب الحقيقي الذي تمّ فيه هذا الاختراق فعلاً والبرمجية التي استخدمت في ذلك. فإذا تبيّن أن المعترف ليس لديه أساساً أية معلومات عن طريقة استخدام الحاسوب والولوج إلى الإنترنت، فلا يمكن الاستناد إلى اعترافه وإدانته بهذا الجرم. ولذلك يمكن لجهات التحقيق أن تلجأ إلى أسلوب تمثيل الجريمة، من أجل التأكد من تطابق أقوال المدعى عليه مع الكيفية الحقيقية التي ارتكبت بها الجريمة، حيث يقوم الجاني -مثلاً- بتعريف جهة التحقيق على الأسلوب الذي اتبعه في عملية الاختراق، والطريقة التي قام بها بتحويل الأموال، وهذا ما يعرف بـ **الاعتراف العملي**. فمجرد الاكتفاء بالاعتراف النظري في ارتكاب جرائم الإنترنت أمر يرفضه المنطق السليم، ما لم يقترن بالاعتراف العملي الذي يؤكد صحة ما جاء على لسان المدعى عليه.

15- وفيما يخص **الخبرة**، يمكن للقاضي الجزائي أن يستعين بعدة جهات لمساعدته في اختيار الخبير المعلوماتي، كالجمعية العلمية السورية للمعلوماتية، أو كلية الهندسة المعلوماتية، أو الشركات الخاصة التي تعمل في مجال تكنولوجيا المعلومات، أو الهيئة الوطنية لخدمات الشبكة، حيث جعل

قانون التوقيع الإلكتروني وخدمات الشبكة رقم /4/ تاريخ 2009/2/19 من مهام الهيئة الوطنية لخدمات الشبكة، مهمة اقتراح الخبراء التقنيين للجهات القضائية في مجال التوقيع الإلكتروني.

و**يرى الباحث** أن اعتماد المحكمة على تقرير الخبير المعلوماتي لا يعد مساساً بمبدأ قناعة القاضي الشخصية، ولا يجعل من الخبير القاضي الحقيقي للدعوى. فدور الخبير التقني ليس سوى أحد الأدوار التي تساعد القاضي على فهم القضية، وهذا الدور ليس بجديد على الساحة القضائية؛ فالقضاء كثيراً ما كان يستند في أحكامه إلى الخبرة التي تجري على البصمات، أو على الحمض النووي DNA، أو على التحاليل النفسية وغيرها، كما أن بناء الحكم على أساس تقرير الخبرة لا يختلف عن الأخذ بأقوال الشهود، وبناء الحكم بالبراءة أو الإدانة على أساس هذه الأقوال. فمحكمة الموضوع هي صاحبة القول الفصل في تقرير الخبرة الذي قد تقتنع به أو لا تقتنع.

16- أما بالنسبة إلى **الدليل الرقمي، فيرى الباحث** أن هذا الدليل يندرج تحت طائفة القرائن القضائية، ويمكن للقاضي الجزائي الأخذ به سواء في إطار الإدانة أم البراءة، إذا توفرت فيه الشروط التالية:

**أ- المشروعية:** أي أن يتم الحصول على الدليل الرقمي بصورة قانونية.

**ب- الصحة والمطابقة:** أي أن يكون الدليل الرقمي المقدم إلى المحكمة هو نفس الدليل الذي تم جمعه، وأن لا يطرأ على هذا الدليل أي تغيير خلال فترة حفظه.

**ج- الدقة:** أي أن نظام الحاسوب الذي استخرج منه الدليل يعمل على نحو دقيق وسليم، بحيث لا يتطرق الشك في دقته.

أما بالنسبة إلى **الدفوع** المتعلقة بهذه الشروط، وخاصة شرطي الصحة والدقة، فإن هذه الدفوع يجب ألا تنال من قيمة الدليل الرقمي إذا جاءت على شكل تخمين دون أن يوجد دليل يدعمها. وهذا ما سارت عليه المحاكم الأمريكية كما رأينا.

وفيما يتعلق **بكيفية تقدير قيمة الدليل الرقمي**، فإن **الباحث** يرى ضرورة التمييز بين أمرين، هما:

الأمر الأول: القيمة العلمية القاطعة للدليل.

الأمر الثاني: الظروف والملابسات التي وجد فيها الدليل.

فالقاضي ليس له أن ينازع فيما استقرت عليه تكنولوجيا المعلومات والعلوم التقنية من الناحية العلمية، وإنما له أن يقدر الظروف والملابسات التي أحاطت بهذا الدليل، ويساعده في هذا التقدير الأدلة التقليدية (الاعتراف والشهادة وغيرها) التي توجد عادة إلى جانب الدليل الرقمي، وله أن يرفض الدليل الرقمي إذا لم يقتنع بظروف الواقعة وملابساتها.

أما بالنسبة إلى **حجية التوقيع الإلكتروني المصدق** في المسائل الجزائية، فإن قانون التوقيع الإلكتروني السوري رقم 4 لعام 2009 لم يعطِ أية حجية للتوقيع الإلكتروني في المسائل الجزائية، فحجيته تقتصر على المسائل المدنية والتجارية والإدارية دون المسائل الجزائية. وعليه فإن الوثيقة الإلكترونية أو الرسالة الإلكترونية الموقعة توقيعاً إلكترونياً مصادقاً تعد كباقي الأدلة الرقمية التي من الممكن أن تعرض على القاضي الجزائي، والتي تخضع لتقديره من ناحية الظروف والملابسات التي وجدت فيها هذه الوثيقة أو الرسالة الإلكترونية.

**وعلى ضوء الآراء والحلول التي ذكرناها؛ فإن الباحث يقترح على المشرع في مشروع قانون الجريمة الإلكترونية المقترحات التالية :**

**أولاً**– على الرغم من **قناعة الباحث** بإمكانية تطبيق النصوص التقليدية لجريمة الاحتيال على الاحتيال عبر الإنترنت، إلا أننا نوصي المشرع السوري بأن يسرع في التدخل لتجريم مختلف جرائم الإنترنت التقليدية منها والمستحدثة. لأن الأمر سيبقى محل خلاف وجدال بين الفقهاء، ولن يُحسم إلا بنص صريح من لدنّ المشرع حتى يحكم فيما كانوا فيه يختلفون. لذلك **فالباحث يقترح** أن يكون النص على الشكل التالي:

( 1– كل من استولى لنفسه عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسوب، على مال منقول أو غير منقول أو معلومات أو برامج أو على سندٍ يتضمن تعهداً أو إبراءً أو أي امتياز مالي آخر، وذلك عن طريق خداع المجني عليه، أو خداع الحاسوب أو الآلة الخاضعة لسيطرة المجني عليه، بأية وسيلة كانت، يعاقب بالحبس من سنة إلى ثلاث سنوات، وبالغرامة ثلاثمائة ألف ليرة سورية.

2– إضافةً إلى الغرامة المذكورة في الفقرة الأولى، تكون العقوبة الأشغال الشاقة المؤقتة إذا وقعت الجريمة على ثلاثة أشخاص فأكثر، أو إذا تجاوز مبلغ الاحتيال مليون ليرة سورية.).

**ثانياً**– أما فيما يتعلق **بالاستخدام غير المشروع لبطاقات الائتمان**، فإن **الباحث يقترح** أن يكون النص على الشكل التالي:

( يعاقب بالحبس من سنة إلى ثلاث سنوات، وبالغرامة ثلاثمائة ألف ليرة سورية على ما يلي:

1-كل من استخدم الشبكة المعلوماتية أو أحد أجهزة الحاسوب، للوصول دون وجه حق إلى بيانات أو أرقام بطاقة ائتمانية أو إلكترونية، وذلك بقصد الحصول على أموال الغير أو ما تتيحه من خدمات.

2-كل من قام بتزوير بطاقة ائتمانية أو إلكترونية بقصد الحصول على أموال الغير أو ما تتيحه من خدمات، أو كل من استعمل بطاقة ائتمانية أو إلكترونية مزورة في سحب النقود أو الوفاء.

3-كل من استعمل بطاقة ائتمانية أو إلكترونية مسروقة أو مفقودة في سحب النقود أو الوفاء.).

**ثالثاً**- بالنسبة إلى **الاختصاص**، فإن الباحث **يقترح** أن يكون النص على الشكل التالي:

(1-تطبق القواعد المتعلقة بالصلاحيات الإقليمية والذاتية والشخصية والشاملة المنصوص عليها في قانون العقوبات على الجرائم الإلكترونية.

2-يعتبر بحكم الأرض السورية، النطاق العلوي السوري على الإنترنت المنتهي بـ sy.).

كما **نقترح** على المشرع أن يرتفع بالعقوبات الجنحية في الجرائم الإلكترونية إلى الحبس ثلاث سنوات، كي يتجنب الشرط المتعلق بتجريم القانون الأجنبي عند تطبيق مبدأ الشخصية.

**رابعاً**- وفيما يخص **المراقبة الإلكترونية، فالباحث** يقترح على المشرع أن يسمح لموظفي الضابطة العدلية القيام بالمراقبة الإلكترونية، بشرط الحصول على إنابة من قبل قاضي التحقيق المختص، أو بناءً على إذن من النيابة

العامة، حتى يتمكن هؤلاء الموظفون من القيام بالمراقبة الإلكترونية على وجه السرعة، تماشياً مع طبيعة جرائم الإنترنت. و**نقترح** أن يكون النص على الشكل التالي:

( يجوز للضابطة العدلية القيام بالمراقبة الإلكترونية بناءً على إذن من النيابة العامة، أو على إنابة من قبل قاضي التحقيق المختص. )

**خامساً**- ومع إيمان **الباحث** بأن النصوص الإجرائية الحالية تسمح **بتفتيش** المكونات المعنوية أو البرمجية للحاسوب وشبكة الإنترنت، إلاّ أننا **نقترح** على المشرع أن ينص صراحةً على جواز تفتيش المكونات المعنوية لحاسوب المشتبه به والحواسيب المتصلة به أيضاً، أيّاً كان مكان وجودها، ما دام في ذلك فائدة في إظهار الحقيقة. **ونقترح** أن يكون النص على الشكل التالي:

(1- تعتبر المكونات المعنوية للحاسوب أو البرمجيات من الأشياء المادية التي يجوز تفتيشها وضبطها وفق القواعد المنصوص عليها في قانون أصول المحاكمات الجزائية.

2- يجوز تفتيش الحواسيب المتصلة بحاسوب المشتبه به أيّاً كان مكان وجودها، ما دام في ذلك فائدة في إظهار الحقيقة.)

**سادساً**- وفيما يتعلق **بالدليل الرقمي**، فإن **الباحث** يقترح على المشرع أن يترك مسألة تقدير الدليل الرقمي لقناعة القاضي الجزائي، أسوة بالقواعد العامة. و**نقترح** أن يكون النص على الشكل التالي :

( تقدر المحكمة قيمة الدليل الرقمي، بشرط أن يكون نظام الحاسوب المستمد منه الدليل يعمل على نحو سليم، وألا يطرأ على الدليل المقدم إلى

المحكمة أي تغيير خلال فترة حفظه. ويعد الدليل المقدم إلى المحكمة مستجمعاً لهذين الشرطين ما لم يثبت عكس ذلك .).

**ولا بد من الإشارة هنا** بأن جميع هذه التوصيات قد تم الأخذ بها من قبل اللجنة المكلفة بوضع مشروع قانون الجريمة الإلكترونية السوري.

**وأخيـــراً** أرجـو أن أكـون قـد عرضـت الموضـوع عرضـاً شـاملاً وافيـاً بالغرض، وأن أكون قد وفقت في وضع الحلول الملائمة له، فإن أصبت فلله المنّة والفضل، وإن أخطأت فالعصمة من شأن الرسل.

# (( المـــــــــراجع ))

## أولاً  المراجع باللغة العربية:

### أ- المراجع العامة :


– **د.أسامة عبدالله قايد:** شرح قانون العقوبات – القسم الخاص، جرائم الأموال، دار النهضة العربية،القاهرة، 1989.

– **د.جاك الحكيم و د.رياض الخاني:** شرح قانون العقوبات، القسم الخاص، مطبعة الداودي، دمشق، 1982.

– **د.حسن الجوخدار:** أصول المحاكمات الجزائية، الطبعة الخامسة، منشورات جامعة دمشق، 1991.

– **د.رؤوف عبيد:** جرائم الاعتداء على الأشخاص والأموال، الطبعة الثامنة، دار الفكر العربي، القاهرة، 1985.

– **العلامة رينيه غارو:** موسوعة قانون العقوبات العام والخاص، عشر مجلدات، منشورات الحلبي الحقوقية، بيروت،ترجمة المحامية لين صلاح مطر، 2003.

– **د.عبد الفتاح مصطفى الصيفي:** قانون العقوبات اللبناني، جرائم الاعتداء على أمن الدولة وعلى الأموال، دار النهضة العربية، بيروت، 1972.

– **د.عبد الوهاب حومد:**

- أصول المحاكمات الجزائية ، الطبعة الرابعة (منقحة ومزيدة)، المطبعة الجديدة، دمشق، 1987.
- المفصّل في شرح قانون العقوبات، القسم العام، المطبعة الجديدة، دمشق، 1990.

– **د.عبود السراج،** شرح قانون العقوبات، القسم العام، منشورات جامعة دمشق، 2007 .

– **د.علي عبد القادر القهوجي:** قانون العقوبات – القسم الخاص، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2001.

– **د.محمود محمود مصطفى:** شرح قانون العقوبات ، القسم الخاص، الطبعة الثامنة، مطبعة جامعة القاهرة، 1984 .

– **د.محمود نجيب حسني:**

- شرح قانون العقوبات اللبناني، القسم العام (جزأن) طبعة ثالثة جديدة (معدلة و منقحة)، منشورات الحلبي الحقوقية، بيروت، 1998.
- شرح الجرائم الواقعة على الأموال في قانون العقوبات اللبناني (جزأن)، طبعة ثالثة جديدة ( معدلة و منقحة)، منشورات الحلبي الحقوقية، بيروت، 1998 .
- جرائم الاعتداء على الأموال في قانون العقوبات اللبناني، دراسة مقارنة، دار النهضة العربية، بيروت، 1984.
- شرح قانون الإجراءات الجنائية، الطبعة الثانية، دار النهضة العربية، القاهرة، 1988.

– **د.وحيد الدين سوار:** الحقوق العينية الأصلية، منشورات جامعة دمشق، 1993.

**ب  المراجع المتخصصة :**

- **د. الشحات إبراهيم محمد منصور** ، الجرائم الالكترونية في الشريعة الإسلامية و القوانين الوضعية ، دار النهضة العربية ، القاهرة، 2002 .
- **القاضي الدكتور إيهاب السنباطي:** موسوعة الإطار القانوني للتجارة الالكترونية، دار النهضة العربية، القاهرة، 2007.
- **بشار محمود دودين:** الإطار القانوني للعقد المبرم عبر شبكة الإنترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2006.
- **د.جميل عبد الباقي الصغير:**
  - الإنترنت و القانون الجنائي، دار النهضة العربية، القاهرة، 2002.
  - أدلة الإثبات الجنائي و التكنولوجيا الحديثة، دار النهضة العربية، القاهرة، 2002 .
  - الحماية الجنائية والمدنية لبطاقات الائتمان، دار النهضة العربية، القاهرة، 2003 .
  - الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، 2002 .
- **د.حسين بن سعيد الغافري**، السياسة الجنائية في مواجهة جرائم الإنترنت(دراسة مقارنة)، دار النهضة العربية، القاهرة،2009.
- **د.سليمان أحمد فضل:** المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، دار النهضة العربية، القاهرة، 2007.
- **شمسان ناجي صالح الخيلي:** الجرائم المستخدمة بطرق غير مشروعة لشبكة الإنترنت(دراسة مقارنة)، دار النهضة العربية،القاهرة،2009.
- **د.طوني ميشال عيسى:** التنظيم القانوني لشبكة الإنترنت، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2001.

- **عبد الله عبد الكريم عبد الله:** جرائم المعلوماتية والإنترنت، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2007.
- **د.عبد الفتاح بيومي حجازي:**
  - التجارة الالكترونية وحمايتها القانونية، دار الفكر الجامعي، الإسكندرية، 2004.
  - مبادئ الإجراءات الجنائية، في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، المحلة الكبرى، القاهرة ، 2007.
- **د.عبد الفتاح مراد:** شرح جرائم الكمبيوتر والإنترنت، بلا دار نشر، بلا عام.
- **عفيفي كامل عفيفي:** جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، منشورات الحلبي الحقوقية، بيروت، 2003.

- **د.علاء عبد الباسط خلاف:** الحماية الجنائية لوسائل الاتصال الحديثة، دار النهضة العربية، القاهرة، 2002.
- **د.علي جبار الحسيناوي:** جرائم الحاسوب والإنترنت، الطبعة العربية، دار اليازوري العلمية للنشر والتوزيع، عمان، 2009.
- **د.عمر محمد أبو بكر بن يونس :**
  - الجرائم الناشئة عن استخدام الإنترنت، الطبعة الأولى، دار النهضة العربية، القاهرة، 2004 .
  - الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي، الطبعة الأولى، بدون اسم الناشر، القاهرة، 2005 .
  - الاتفاقية الأوربية حول الجريمة الافتراضية (المذكرة التفسيرية)، الطبعة الثانية، مؤسسة آدم للنشر والتوزيع، مالطا، 2008.

-**القاضي الدكتور غسان رباح:** الوجيز في قضايا حماية الملكية الفكرية والفنية مع دراسة مقارنة حول جرائم المعلوماتية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2008.

- **المحامي محمد أمين الشوابكة:** جرائم الحاسوب والإنترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2006.
- **د.محمد الشناوي:** جرائم النصب المستحدثة، دار الكتب القانونية، المحلة الكبرى، القاهرة، 2008.
- **د. مصطفى محمد موسى:** دليل التحري عبر شبكة الإنترنت، دار الكتب القانونية، القاهرة، 2005.
- **المحاميان منير محمد الجنبيهى وممدوح محمد الجنبيهى:**جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، 2005.
- **د.نائلة عادل محمد فريد قورة:** جرائم الحاسوب الآلي الاقتصادية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2005.
- **نبيلة هبة هروال** ،الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات ، الطبعة الأولى ،دار الفكر الجامعي ، الإسكندرية، 2007 .
- **د.هدى حامد قشقوش:** جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، بلا عام.
- **د. هلالي عبد اللاه أحمد** : حجية المخرجات الكومبيوترية في المواد الجنائية، النسر الذهبي للطباعة، القاهرة ، 2002 .
- **وائل الدبيسي:** البطاقة المصرفية، مطبعة صادر، بيروت، 2004.

**ج- رسائل الماجستير والدكتوراه :**

- **أحمد حسام طه تمام:** الجرائم الناشئة عن استخدام الحاسب الآلي، دراسة مقارنة، رسالة دكتوراه مقدمة لجامعة طنطا، 2000.
- **علي حسن محمد طوالبة:** التفتيش الجنائي على نظم الحاسوب والإنترنت، رسالة لنيل درجة الدكتوراه مقدمة إلى جامعة عمان العربية للدراسات العليا، 2003.
- **فهد سلطان محمد أحمد بن سليمان** ، مواجهة جرائم الإنترنت، رسالة حاصلة على درجة الماجستير في القانون الجنائي بجامعة القاهرة 2002.
- **د.محمد سعيد أحمد إسماعيل:** أساليب الحماية القانونية لمعاملات التجارة الإلكترونية، رسالة دكتوراه مقدمة من جامعة عين شمس، القاهرة، 2005.
- **محمد عبيد الكعبي:** الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، رسالة حاصلة على درجة الماجستير في القانون الجنائي بجامعة القاهرة، 2004 .

**د- الأبحاث:**

- **د.علي محمود علي حمودة:** الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية المنعقد في دبي من 26 – 28 نيسان، 2003. متوفر على الموقع www.arablawinfo.com.
- **المحامي يونس عرب:** جرائم الكمبيوتر والإنترنت، بحث منشور على الموقع www.arablaw.com.

**هـ – الدوريات:**

- **د. مصطفى محمد موسى:** المراقبة الإلكترونية عبر شبكة الإنترنت، دراسة مقارنة، سلسلة اللواء الأمنية في مكافحة الجريمة الإلكترونية، العدد الخامس، مطابع الشرطة للطباعة والنشر والتوزيع، القاهرة، 2003.

**و- القواميس التقنية:**

- **د.عبد الحسن الحسيني:** القاموس الموسوعي في المعلومات والاتصالات والمعلوماتية القانونية، الطبعة الأولى، مكتبة صادر، بيروت، 2004.

**ز- مجموعات الاجتهادات القضائية:**

- مجموعة قانون أصول المحاكمات الجزائية (جزأن)، تجميع أديب استانبولي، الطبعة الثالثة، 1994.
- المجموعة الجزائية لقرارات محكمة النقض السورية، تجميع أديب استانبولي والمحامي ياسين دركزلي، الطبعة الثانية، 1992.
- مجموعة القواعد القانونية في القضايا الجزائية من عام 1949 وحتى 1968، المكتب الفني في محكمة النقض، بإشراف القاضي أنس الكيلاني، الطبعة الأولى، 1969.
- مجموعة أحكام النقض في قانون العقوبات والقوانين المتممة من عام 1988 حتى 2001، إعداد عبد القادر جار الله، الطبعة الأولى، المكتبة القانونية، دمشق، 2001.

**المدقق اللغوي:**

الأستاذ زياد رزق.

## ثانياً – المراجع باللغة الأجنبية :


1) **Adam D Thierer**، Clyed wayne crews، Who rules the net?، published by cat to institute، 2003، ISBN: 9781930865433 .

2) **ALBERT .J . Marcella ، Robert .s. Green Field**، Cyber Forensics، Field Manual for collecting Examining and Preserving Evidence of computer crimes، published by CRC Press، 2002، ISBN:9780849309557.

3) **Allen Hammond**، Santa Clara University، The 2001 Council Of Europe Convention On Cyber- Crime An efficient Tool To Fight Crime On Cyber- space، 2001.

4) **Anthony Reys and others**، Cyber Crime Investigations، Bridging The Gaps Between Security Professional Law، Enforcement and Prosecutors. Published by Elsevier Since and Technology، 2007، ISBN: 9781597491334.

5) **Charles Doyle**: Cyber Crime: An Overview Of The Fraud Computer Fraud and Abuse Statute، 2008.

6) **Eoghn Casey**: Digital Evidence And Computer Crime، second edition، A cadimic Press، 2004. ISBN، 0121631044.

7) **Dr. Henry B. wolfe**، Forensics and the emerging importance of electronic Evidence gathering، OTAGO university، 2001، available on line. www.e-evidence.info.

8) **John R.vacca**، Computer Forensics: Computer Crime scene Investigation، published by Charles River media، 2002، ISBN: 1584500182.

9) **Joseph W.Koletar**: Fraud Exposed، What you don't know could cost your company millions، John Wiley & Sons، in 2003.

10) **Joseph T. wells**: Computer Fraud Casebook، Published by John Wiely @sons. Inc، Hoboken، New Jersey، 2009، ISBN: 9780470278147.

11) **Micheal Hirst**، Jurisdiction and the Ambit of the criminal law، published by oxford university، 2003، ISBN: 9780199245390.

12) **Micheal G.Solomon and others**: Computer Forensics jump start، published by Wiley- Default، 2005، ISBN: 9780782143751.

13) **Micheal Kunz and Patrick Wilson**: computer crime and computer fraud، University of Mayland، 2004.

14) On line fraud and crime: Are consumers safe? Hearing before the subcommittee on commerce trade and consumer protection، 2001.

15) **Panagiotis kanellis and others**، Digital Crime and Forensic Science in Cyberspace، Published by Idea group inc، 2006، ISBN: 9781591408727.

16) **Richard Hillman**: securities fraud، The internet poses challenges to Regulateres and Investors، United States General Accounting Office، 1999.

17) **Robin Bryant**: Investigating Digital Crime، John Wile& Sons، ltd، 2008، ISBN: 9780470516003 .

18) **Report**: internet crime compliment center، 2007. Available on www.ic3.gov

# الفهرس