ROLACC
مجلة مركز حكم القانون ومكافحة الفساد
RULE OF LAW AND ANTI-CORRUPTION CENTER JOURNAL

RESEARCH ARTICLE

مدى استيعاب النصوص التقليدية للسرقة الإلكترونية- دراسة مقارنة

د. حابس يوسف زيدات*

استاذ القانون الجنائي المساعد
جامعة القدس و الكلية العصرية الجامعية
فلسطين

Habes Zedat
Al-Quds University & Modern University College
Palestine
*Email: habes.zedat@yahoo.com

مُلخَّص

أن التطور التكنولوجي وتقنية المعلومات والكثير من الوسائل الالكترونية الحديثة جعل المجال مفتوحاً لأن تتدخل الى جانب الفائده كثير من السلبيات، فاذا كان البعض يستخدم الوسائل الحديثه في صالح البشرية، إلا أن هنالك من يرتكبون من خلال نفس تلك الوسائل الجرائم .

ومنها جريمة السرقة التى تفترض قيام الجاني باختلاس الشئ من المالك الأصلي وإدخاله إلى حيازة مرتكب الاعتداء والظهور عليه بمظهر المالك، فهذه التطورات الحديثة سمحت للأفراد والمؤسسات الى الولوج من خلال تلك الوسائل الى البنوك والمؤسسات المصرفيه وقواعد المعلومات وحتى الاجهزة الشخصية للافراد ، مما ساهم بظهور أشكال جديدة وأساليب جديدة يمكن من خلالها ارتكاب مثل تلك الجرائم التقليدية التى جرمتها نصوص قانون العقوبات في كل دول العالم.

وبات التساؤل هل تخضع تلك الجرائم الى النصوص التقليدية التى نص عليه قانون العقوبات أم هي بحاجه الى تشريع جديد يواكب ما رافق تلك الجرائم التقليدية «ومنها السرقة» من وسائل حديثة تسمى بالجرائم الالكترونية؟ رتب ذلك ضرورة التفكير في دراسة مدى كفاية النصوص التقليدية لمحاربة جرائم الاختلاس الإلكتروني، ومدى الحاجة الى وضع تشريعات قانونية حديثة لمكافحة الجرائم الإلكترونية .

الكلمات المفتاحية: المال المعلوماتي، النماذج التقليدية، المنظومة الالكترونية، القرصنة، التكييف القانوني، تبديل الحيازة .

Title: Latitude of punitive terminology interpretation for electronic theft

ABSTRACT

A natural course of world development benefits, harness and service the mankind, through means of technological development and various modern electronic means, it nevertheless created a platform for significant negative consequences , where some deploy the same modern means to commit illegal criminal actions.

Conventional crimes were and are still being committed in traditional ways, including theft, which assumes that the perpetrator steals the object and transmute its possession from its owner. In majority of countries around the world the provisions of the Penal Code in all countries of the world criminalize banking and information databases, which contributed to the emergence of new forms and new methods through which to conventional crimes are committed.

While crimes are committed through these modern means, the key question is whether these crimes are subject to the conventional provisions of the Penal Code, or a new legislation shall be passed to retain the pace associated with conventional crimes with modern twists i.e. cybercrime?

This leads to first; considering the adequacy of the conventional provisions combating cyber-crime, second; the need for developing a modern legal framework to combat cybercrime in which terminologies grasp all dimensions and negative effects of the criminal phenomenon. This will inspire nations to look for modern Legislations regulating and combating these conventional crimes committed through means of technology.

Keywords: Conventional prototypes, electronic ecosystem, hacking, legal adaptation, transmutation of possession

Submitted : 16 October 2019
Accepted : 13 November 2019
Published: 31 December 2019
https://doi.org/10.5339/rolacc.2019.9

© 2019 The Author(s), licensee HBKU Press. This is an open access article distributed under the terms of the Creative Commons Attribution license CC BY 4.0, which permits unrestricted use, distribution and reproduction in any medium, provided the original work is properly cited.

Cite this article as: : Zedat H. مدى استيعاب النصوص التقليدية للسرقة الإلكترونية – دراسة مقارنة, Rule of Law and Anti-Corruption Center Journal 2019:2.9. https://doi.org/10.5339/rolacc.2019.9

كيوسايننس
QSCIENCE
دار جامعة حمد بن خليفة للنشر
HAMAD BIN KHALIFA UNIVERSITY PRESS

1-0 المقدمة

لقد كان الهدف الأساسي من إيجاد أجهزة الكمبيوتر هو تسخيرها لخدمة الإنسان في مجال الأعمال والمعاملات، وكان لظهور تلك الأجهزة وتطورها بسرعة من مجرد أجهزة تقوم بعمليات حسابية إلى مخازن قادرة على تجميع واستيعاب كم ضخم من المعلومات والبيانات، وقادرة على استرجاعها بسرعة وبدقة، إلا أنها أحدثت مشكلة خطيرة تؤرق الكثيرين حول كيفية حماية تلك المعلومات بعد أن أصبحت في متناول اليد وبأقل مجهود وأبسط حركة، فلم يعد المجرم بحاجة إلى أدوات وآلات تقليدية لارتكاب جريمته، نتج عن ذلك علاقات قانونية جديدة بحاجة إلى الحماية حال التعدي عليها سواء في مجال فروع القانون المختلفة أو بقانون خاص بها .

إن التقدم العلمي والتطورات الحديثة ساهمت في إحداث وظهور أشكال وأساليب جديدة من صور الجرائم الإلكترونية، بحيث أصبح مفهوم الجريمة الإلكترونية،[1] يرتبط ارتباطاً وثيقاً بالتطور التكنولوجي **وتقنية** المعلومات، ومن الطبيعي أنه كلما تطور واتسع نطاق التجريم، أحدث ذلك تغيرات مستمرة ومتسرعة ومضطردة في أشكالها وصورها التي تختلف عن النماذج التقليدية للجرائم العادية، فالجرائم الإلكترونية ترتكب عبر الوسائط والوسائل الإلكترونية المختلفة، فتلك الجرائم تقع بأشكال مختلفة ومستحدثه لم تكن معروفه أو ظاهره إلا من قريب، وهي مرتبطة إلى حد ما بما يشهده العالم من تطور تكنولوجي وعلمي في جميع المجالات دون استثناء.

إن ظاهرة الإجرام المعلوماتي المتطورة تحمل جانباً مظلماً يتجسد بعدم قدرة القواعد القانونية أن تتطور بقدر مساوٍ لتلك الظاهرة حتى تستطيع الحد من تلك التعديات والجرائم التي تتم باستخدام شبكات الاتصالات الحديثة، مثل: الإنترنت والحاسوب والهواتف النقالة والبريد الإلكتروني، واعتراض المعلومات السرية أو الكشف عنها وغيرها من الجرائم العابرة للحدود.[2]

ونظراً لحداثة ظهور هذه الجرائم، وفي نفس الوقت حداثة تنبه المجتمع الدولي لخطرها، حيث يرجع أصل شبكة المعلومات والاتصالات الدولية (Internet) إلى شبكة من أجهزة الحاسب الآلي، أنشأتها الولايات المتحدة الأمريكية –أنشأت هذه الشبكة في وزارة الدفاع الأمريكية – في الستينيات من القرن الماضي لخدمة التأهب السريع للقوات المسلحة في حال نشوب حرب نووية أو استخدام الأسلحة الأخرى المحرمة أو أي هجوم عسكري عليها، وقد شهدت العقود الأخيرة من القرن العشرين، ثورة في عالم الاتصال ونقل المعلومات والتكنولوجيا على مختلف الأصعدة، مما سمح للأفراد والمؤسسات الولوج إلى البنوك والمؤسسات وقواعد المعلومات لمحلياً ودولياً، مما ألف مصدراً غنياً بالمعلومات لمراكز اتخاذ القرار، رافق ذلك ظهور الكمبيوتر والإنترنت، مما خلق إشكاليات خطيرة على اقتصادياً وقانونياً وما رافق ذلك من تنوع الاعتداءات على تلك المعلومات والبيانات والبرامج، فهذا التطور الشامل للمنظومة الإلكترونية، وما تبعه من نشاط متواصل ما بين أكثر من مائتي دولة جعلها على اتصال دائم من خلال تبادل البيانات والمعلومات التي يتم إدخالها وتحميلها على الشبكة الالكترونية في أقل من دقيقة مما جعله متاحاً لأي مستخدم في تلك الدول.[3]

ولم تعرف الدول العربية الحاسب الآلي إلا في مطلع السبعينات من القرن العشرين، حيث أدخلته شركات البترول في بعض الدول، مثل: السعودية والكويت وليبيا، ودخل إلى لبنان من خلال البنوك الأجنبية والمحلية، وأدخلته بعض الدوائر الحكومية إلى القطاع الحكومي في مصر والعراق، وإزاء هذا التطور ودخول الحاسب الآلي إلى مختلف الدول، فإن العديد من الجرائم الاقتصادية سوف تظهر في البيئة الإلكترونية والناتجة عن اتساع استخدام الحاسوب والإنترنت؛ لأنه ما دام البشر موجودين فالخير موجود والشر موجود والجريمة وموجودة، مما دفع صوب إيجاد تشريعات تنظم وتحارب تلك الجرائم، فكانت القواعد التقليدية في قانون العقوبات التي تطبق على تلك الجرائم، ونظراً لانتشار تلك الجرائم كان لا بد من البحث عن تشريعات جديدة وحديثة لمواجه الجرائم الإلكترونية، والتي يمتد تأثيرها على الأشخاص والأموال، مما حذا بالدول لوضع تشريعات لمواجهة ذلك وكانت بداية انفتاحها على القانون الجنائي والذي يرسخ بداية هذه الفكرة قانون جرائم المعلوماتية الفرنسي الصادر سنة 1988م ويحمل الرقم 19 وما تبعه من قوانين أخرى ذات صلة، ومنها التشريع الفرنسي الصادر في 4 أغسطس 1994م، المسمى بقانون Toubon، ومن ثم توالت الدول في سن القوانين،[4] والتشريعات، ومن الدول العربية التي اجتهدت في ذلك قانون الجرائم الإلكترونية الأردني رقم 27 لسنة 2015م، والقانون الاتحادي لدول الإمارات رقم 2 لعام 2006م بشأن مكافحة جرائم تقنية المعلومات، والنظام السعودي لمكافحة جرائم المعلوماتية الصادر 2007م، كما نظم المشرع الفلسطيني بموجب القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية.[5]

1-1 أهمية الدراسة

يكتسب موضوع الدراسة أهمية كبيرة بسبب جسامة الأخطار وحجم الخسائر الناجمة عن الجرائم الإلكترونية بأنواعه المختلفة، التي لم تعد عواقبها قاصرة فقط على الأفراد فحسب، وإنما امتدت آثارها لتهدد الدول، حيث تقوم الدراسة هنا على التركيز على التوعية بخطورة الجرائم الإلكترونية، وتحديد الطبيعة القانونية التي تتسم بها المعلومات والبيانات الإلكترونية والجدل الدائر حول مدى اعتبارها أموال تصلح للاختلاس وترتيباً على ذلك، كان لابد من ضرورة التفكير في دراسة مدى كفاية النصوص التقليدية لمحاربة الاختلاس الإلكتروني، ومدى ضرورة وضع تشريعات قانونية الحديثة لمكافحة الجرائم الإلكترونية قادرة على حماية التطور التكنولوجي بعيداً عن القواعد العامة التقليدية التي ذكرت في قانون العقوبات خاصة جرائم الحاسوب والإنترنت والتي تتعرض للكثير من الانتهاكات على أن تكون تلك النصوص قادرة على مواجهة الظواهر الإجرامية بكل أبعادها وآثارها السلبية، كعمليات النسخ والحذف والإتلاف ونقل المعلومات والبيانات الالكترونية أو القرصنة وغيرها من الجرائم الإلكترونية بكافة أنواعها المستحدثة، وإلى جانب القواعد الموضوعية، لابد من وضع النصوص الإجرائية التي تتناسب مع طبيعة تلك الجرائم سريعة الحدوث والاختفاء؛ نظراً لصعوبة التحري والقبض على مرتكبيها، وكذلك التفتيش عن الأدلة الإلكترونية وضبطها، ناهيك عن وجود صعوبة في اكتشافها وإثباتها.

1-2 إشكالية البحث

نظراً لما تتمتع بها خدمات الحاسب الالي والتطور التكنولوجي من أهمية كبرى في مختلف المجالات وفي كثير من الدول، رافق تلك الأهمية العديد من التغيرات والاشكاليات القانونية حول مقدرة وكيفية تعامل النصوص العقابية التقليدية لنشاط الوسائل الالكترونية المستحدثة، وما يستتبع ذلك من صعوبات تتعلق بتحديد الطبيعة القانونية لهذا التطور وما ينتج عنه من جرائم تنصب على المعلومات المخزنة في الحاسوب كجريمة السرقة مثلاً والتى تطرح مجموعة من الإشكاليات القانونية فيما يخص تحديد الطبيعة القانونية خاصة ما يتعلق بمحل الاعتداء باعتباره أهم العناصر المكونة لها، بالإضافة إلى النشاط الإجرامي، وما يطرح حول مدى انطباق عناصر جريمة الاختلاس العادية على سرقة المعلومات والبيانات

---

1 ولسنا هنا بصدد التعريفات المتعددة لبرامج الكمبيوتر سواء بالمعنى الضيق لها أو بالمعنى الواسع؛ لأن المجال لا يسمح باستعراض كل أو معظم التعريفات الواردة في هذا الشأن لذا نكتفي ببعض التعريفات، فهنالك تعريفات انطلقت من الوسيلة المستخدمة في ارتكاب الجريمة وهي التي تتحقق من خلال استخدام الحاسب والكمبيوتر وسيلة لارتكاب الجريمة، حيث عرفت بأنها: «الجريمة التي يتم ارتكابها إذا قام شخص باستخدام معرفته بالحاسب الآلي بعمل غير قانوني»، وعرفها مكتب تقييم التقنية بالولايات المتحدة الأمريكية أنها الجريمة التي تلعب فيها البيانات الكمبيوترية والبرامج والمعلوماتية دورا رئيسا»، كما عرفها القرار الوزاري السعودي رقم 79 المؤرخ في 1428/03/07ه، المتضمن الموافقة على نظام مكافحة جرائم المعلوماتية بأنها:» كل فعل يرتكب متضمنا استخدام الحاسب الآلي أو الشبكة المعلوماتية، بالمخالفة لأحكام هذا التنظيم"وعرفت من حيث العلم بها والمعرفة التقنية، كما يظهر ذلك من التعريف الذي تبنته وزارة العدل الأمريكية من دراسة وضعها معهد ستانفورد للأبحاث، والذي جاء فيه :»أنها أية جريمة لفاعلها معرفة فنية بالحاسبات تمكنه من ارتكابها".

2 Halder, D.,and Jaishankar,K. 2011 Cyber crime and the Victimization of Women :Laws,Rights,and Regulations. Hershey, PA, USA:IGI Global.ISBN 9789-830-60960-1-.

3 Feral Schull (C) Lemonde informatique, 2 fevier 1996.p.25..

4 للمزيد القانون الإسرائيلي المسمى « قانون جرائم الحاسوب – رقم 5755 لسنة 1995والذي يشمل العبث ببرامج الكمبيوتر ونقل المعلومات غير صحية وغيرها من الجرائم.

5 أصدرت فلسطين بعض القوانين الخاصة التي أشارت من خلالها إلى بعض الجرائم الإلكترونية ضمن نصوص بسيطة يقف على رأس هذه القوانين القرار بقانون رقم (15) لسنة 2009م بشأن الهيئة الفلسطينية لتنظيم قطاع الاتصالات، والقانون رقم (3) لسنة 1996م بشأن الاتصالات السلكية واللاسلكية.

المخزنة في جهاز الحاسوب، وما يطبق عليها من إجراءات التفتيش والضبط المتبعة في القوانين الإجرائية.

1-3 خطة البحث

سوف نتعرض بالدراسة إلى الاختلاس في الجرائم الإلكترونية من خلال البحث في التكييف القانوني لاختلاس المعلومات والبيانات الإلكترونية في ضوء أحكام جريمة السرقة وما ينطبق عليه من إجراءات ضبط وتفتيش، وبناء عليه: على التقسيم التالي: المبحث الأول: التكييف القانوني لاختلاس المعلومات والبيانات الإلكترونية في ضوء أحكام جريمة السرقة. المبحث الثاني: إجراءات التفتيش والضبط في الجرائم الإلكترونية.

2-0 المبحث الأول- تطبيق أحكام جريمة السرقة على البيانات والمعلومات

إن الجرائم الإلكترونية من الصعوبة بمكان حصرها فهي متجددة بين الحين والأخر؛ كونها من الجرائم المستحدثة سريعة التطور،ولقد تخيرنا في هذا المطلب أكثر الجرائم شيوعا وأهمية، وهي جريمة السرقة كجرائم أموال في الجرائم الإلكترونية، فجميع القوانين الجنائية نصت على حماية الأموال من الاعتداء سواء في نصوص قانون العقوبات أو من خلال القوانين الخاصة بالجرائم الإلكترونية وحقوق المؤلف وغيرها، والتي أخضعت جميع الأموال المادية أو المعنوية للحماية الجنائية، فالمعلومات والبيانات الإلكترونية تتمتع بالحماية، بحيث نتناول طبيعية المكونات الإلكترونية المادية منها والمعنوية والنقاش حول إمكانية تطبيق نصوص القوانين التقليدية على تلك المعلومات والبيانات وبرامج الكمبيوتر الأخرى بكافة معطياتها، ومدى انطباق نصوص السرقة التقليدية عليها، وما دار حول أصباغ صفة المال على المكونات المعنوية وما نتج عن ذلك من جدال بين الفقهاء، مرجع ذلك أن النصوص القانونية التقليدية لا تتواءم بسهولة مع طبيعة تلك المعلومات والبيانات الإلكترونية الأمر الذي يسبب إزعاجاً متزايداً للفقه المهتم بتلك المعلومات والبيانات ومدى توفير الحماية الجنائية الكافية لها، مما حذا بهم السعي إلى إدراج تلك الأموال المعنوية للحماية الجنائية في مختلف التقسيمات القانونية. ونتناول هذه الدراسة المطالب التالية:

المطلب الأول: مفهوم جريمة السرقة (الاختلاس) وأركانه.

المطلب الثاني: العقبات القانونية التي تعترض تطبيق نصوص الاختلاس على البيانات الإلكترونية.

2-1 المطلب الأول: مفهوم جريمة السرقة وأركانه

2-1-1 مفهوم ومحل جريمة السرقة

عرف المشرع الأردني السرقة في المادة (399) من قانون العقوبات النافذ، حيث نص في الفقرة 1 منها على أنها: «أخذ مال الغير المنقول دون رضاه، ونص في الفقرة 2 على أنها: «إزالة تصرف المالك فيه برفعه من مكانه ونقله، وإذا كان متصلا بغير منقول فبفصله عنه فصلا تاما ونقله»، وقرر في الفقرة 3 أن لفظ المال يشتمل على القوى المحرزة، فالمشرع بين أن موضوع السرقة هو الشيء المادي وهو في نفس الوقت الشيء الذي يتقبل السلطات المادية التي تنطوي عليها الملكية والحيازة، ونصت المادة (311) من قانون العقوبات المصري على أن السرقة: «كل من اختلس منقولا مملوكا لغيره فهو سارق»، ونص في المادة (1/311) من قانون العقوبات الفرنسي على أن السرقة هي: «اختلاس الشيء المملوك للغير»، كما عرفت السرقة بأنها: «اعتداء على ملكية منقول وحيازته بنية تملكه».[6] فاعتبار السرقة جريمة اعتداء على ملكية المنقولات فإنه يتعين أن يكون لموضوعها صفة المال المنقول، وهو ما يتم نقله من مكان إلى آخر دون تلف، وهي كذلك اعتداء على الحيازة من أجل استطاعة الاعتداء على **الملكية**، وهذا التعريف وما سبق من تعريف لدى المشرع الأردني يمثل – في غالبية مضمونه – ذات المفهوم المقرر في مختلف التشريعات العربية منها وغير العربية، كما هو واضح من نص المادة 635 من قانون العقوبات اللبناني، والمادة 621 سوري، وكذلك الأمر في تشريعات فرنسا وايطاليا، بحيث يتطلب فعل الاختلاس في السرقة أن يرد على شيء مادي أو مال مادي، وتعرف سرقة المعلومات والبيانات بأنها: الاستيلاء عليها دون علم وإرادة صاحبها أو حائزها القانوني سواء أكانت مخزنة على أشرطة ممغنطة (ديسكات) أو إسطوانات (سي دي) بقصد التصرف بها على غير رضا صاحبها .

محل جريمة السرقة (الاختلاس): تصنف جريمة السرقة على أنها من جرائم الاعتداء على الأموال؛ كون فعل الاختلاس لا يقع إلا على مال، والعلة من وراء تجريم السرقة؛ كونها تشكل اعتداء على ملكية هذا المال، والملكية في حقيقة الأمر هي أحد الحقوق التي أولاها المشرع أهمية، ويتطلب في محل السرقة أن تتوفر الصفة المادية في المحل، وأن يكون مالاً (كل شيء يصلح محلا لحق عيني)؛ لأن الحيازة التي تنالها السرقة بالاعتداء، يراد منها الحيازة المادية، فلفظ الشيء التي جاء بها المشرع الفرنسي تقابل لفظ المال المنقول التي جاء بها القانونيين الأردني والمصري، حيث إن الصفة المادية للشيء هي إمكانية السيطرة المادية عليه، وصلاحيته لأن تستخلص منه مباشرة المزايا المادية التي تشكل السرقة اعتداء عليها، ولعل تفسير كلمة شيء لا يجب أن تفسر بمعزل عن صلته بفعل الاختلاس، وهو ما اعتدت به محكمة استئناف Anvers البلجيكية حين اعتبرت في حكم لها صادر بتاريخ 13ديسمبر 1984م أن قيام المتهم بنسخ ثلاثة برامج تحتوي معلومات وبيانات خاصة للمؤسسة التي يعمل لديها قاصداً في ذلك تحقيق منفعته الخاصة، يشكل جريمة سرقة، وقد بينت المحكمة أساس حكمها على «أن كلمة شيء (chose) التي وردت في الفقرة الأولى من المادة 461 من قانون العقوبات البلجيكي، والتي نصت «على أن كل من يختلس شيئا مملوكا للغير يعد مرتكباً لجريمة السرقة، إنما يجب أن ينظر إليها في إطار المعنى الشائع والمألوف للكلمة بحيث يكون هذا المعنى متوافقا مع مفهوم اختلاس هذا الشيء، وهو ما يتحقق حالة نسخ البرامج والمعلومات والتي تعد من عناصر الذمة المالية للشركة التي تمتلكها، فهذه البرامج والمعلومات لا تعد – كما يدعي المتهم – مجرد مجموعة من التعليمات ذات طبيعة غير مادية ولا تصلح بالتالي أن تكون محلاً للاختلاس، وإنما هي على العكس من ذلك أشياء قابلة للنقل وإعادة الإنتاج، كما أن لها أهمية اقتصادية، ومن ثم تصلح محلاً للسرقة.[7]

وإذا كانت القواعد العامة لجريمة السرقة لا تدخل الأموال المعنوية ضمن الاعتداد في نصوص جريمة السرقة؛ لما تتطلبه تلك النصوص من كون المال يقع على كيان مادي، وعلى الرغم من ذلك، إلا أنه إذا أمكن حيازته داخل إطار معين للاستئثار به، فإنه يقع تحت طائلة السرقة وان كانت طبيعة المعلومات والبيانات المخزنة والمتبادلة عبر شبكة الإنترنت مما يصعب حيازته ما لم تثبت على وسيلة لنقل أو نسخ المعلومات بحيث تصلح محلاً للسرقة،[8] لأن كيانها المادي يتمثل بالشريط الممغنط أو الملف التي يحفظ تلك المعلومات، والذي يعد عندها اختلاس محتوى المعلومة، تأسيساً على أن سرقة المعلومات والبيانات تختفي خلف سرقة الشريط الممغنط أو الملف، وأن سرقة هذا الأخير دليل على سرقة الأول من معلومات وبيانات.[9]

هذا وقد أوضحت التعريفات السابقة أن محل السرقة منقول، والذي يفترض قيام الجاني باختلاس الشيء، أي نزع حيازته من المالك الأصلي وإدخاله إلى حيازة الجاني مرتكب الاعتداء، بحيث يمكن القول أن المعلومة شيء منقول، ذلك وفق ما أوضح وعرف المشرع الفرنسي المعلومات في القانون رقم (652/82)الصادر بتاريخ 26 يوليو 1982م، هي عبارة عن «أصوات وصور ووثائق ومعطيات أو رسائل أياً كانت طبيعتها»، وقد أوضحت محكمة النقض الفرنسية في حكم لها أنه منذ انفصال الشيء عن الأصل الذي كان ملتصقاً به فإنه يعد منقولاً قابلاً للسرقة.[10]

---

6 د.فوزية عبد الستار –شرح قانون العقوبات – القسم الخاص – سنة 1982 –دار النهضة العربية – القاهرة – ص666.

7 مشار إليه في :د. نائلة عادل محمد فريد ، المصدر سابق ، ص 135 ؛ وينظر: عفيفي كامل عفيفي ، جرائم الكومبيوتر ، دراسة مقارنة ، منشورات الحلبي الحقوقية ، ط2 ، 2007 ، ص 151.

8 The No Electronic Theft (NET) Act, enacted in 1997 by the U.S. Congress, amended titles 17 and 18, United States Code, to provide greater protection for copyright owners by amending criminal copyright infringement provisions, and for other purposes.

9 د. أحمد حسام طه تمام – الجرائم الناشئة عن استخدام الحاسب – دار النهضة العربية – القاهرة – سنة 2000م–ص496.

10 مشار إليه د. أحمد طه تمام – المرجع السابق – ص .492 وما يليها. مشار إليه د. الدكتور عمر الفاروق الحسيني – المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية– ط2 سنة –1995ص101.

كما ويشترط لقيام جريمة السرقة حسب النصوص القانونية السابقة أن يقع الاعتداء على مال مملوك للغير، فلا تقوم جريمة السرقة إذا اختلس الشخص مالا منقولا ملك له، أي لا بد أن يكون المال المنقول مملوكاً للمجني عليه أوفي حيازته وقت فعل الاختلاس، ذلك انه إذا انصب الاعتداء على مال يملكه الجاني فهو استعمال لحقه على الشيء، وإذا انصب على مال غير مملوك لأحد فهو اكتساب مشروع للملكية، فيلزم لحدوث السرقة أن يكون هنالك اعتداء على الملكية صورته أو وسيلته انتزاع الحيازة.

2-1-2 أركان جريمة السرقة

بالعودة إلى تعريف السرقة في النصوص السابقة، فإن التعريف يتضمن الإشارة إلى موضوع السرقة بأنه مال الغير المنقول، ثم ركن مادي، وهو فعل الاختلاس أو الأخذ دون الرضاء، أما الركن المعنوي فيستخلص من الأحكام العامة، ويتألف من القصد العام، بالإضافة إلى قصد خاص، وهو: «نية التملك»، وسوف نتناول كل ركن من هذه الأركان على النحو التالي من البيان، ونتناول في نفس الوقت ما ينطبق من موضوعنا على تلك الأركان قدر المستطاع:-

الركن المادي لجريمة السرقة هو الاختلاس أو ما تسميه بعض التشريعات العربية، كالتشريع الأردني واللبناني بالأخذ ويعد مصطلح الأخذ أفصح من الناحية اللغوية من الاختلاس، ويعرف على أنه: «نقل الشيء أو نزعه من المجني عليه بغير علمه وبغير رضاه وإدخاله إلى حيازة الجاني، وعرف الأخذ أو الاختلاس بأنه: «سيطرة الجاني (السارق) على الشيء المسروق والظهور عليه بمظهر المالك[11]؛ إذ يلزم لقيام الركن المادي في جريمة سرقه المعلومات والبيانات أن يقوم الجاني بنشاط خارجي ملموس أو فعل مادي يعبر به الجاني عن انصراف إرادته في انتهاك نظام الحماية أو أخذ تلك المعلومات الموجودة على النظام الإلكتروني مع علم الجاني بأن ما يقوم به الجاني على غير رضا المجني عليه[12]، وقد بين الشارع الركن المادي بأنه: «الأخذ دون الرضاء»، ويعرف بأنه: «نقل الشيء أو نزعه من المجني عليه بغير علمه ورضاه وإدخاله إلى حيازة الجاني، أو هو الاستيلاء على الحيازة الكاملة للشيء بمفهومها المادي والمعنوي، بدون رضاء مالكه وهو ما يتحقق من الناحية مادية بحرمان صاحب الحيازة القانونية منها.[13]

وعرفته محكمه النقض المصرية بأنه: «من المقرر أن السرقة تتم بالاستيلاء على الشيء المسروق استيلاء تاماً يخرجه من حيازة صاحبه ويجعله في قبضة السارق وتحت تصرفه،[14] فمن الممكن تطبيق نصوص جريمة السرقة العادية على سرقة الشيء الإلكتروني أو التلاعب به، حيث إن اختلاس الشيء – المتمثل بالبيانات والمعلومات – يتحقق بالنشاط المادي الذي يصدر عن الجاني وذلك بتشغيله للحاسوب للحصول على المعلومة التي يرغب بها أو التلاعب بها للحصول على مردود مادي فتتحقق النتيجة بحصوله عليها،[15] فالجاني صدر عنه سلوك إرادي يؤدي إلى النتيجة، فهناك نشاط ونتيجة ورابطة سببية بينهما، ويمثل هذا الجانب الموضوعي، أما الجانب الشخصي سوف نتناوله عند الحديث عن الركن المعنوي، والذي يتمثل في نية المجرم الإلكتروني في الاستيلاء على الشيء وعدم الرضا الصادر عن المجني عليه لاستيلاء الجاني على ماله.[16]

ويتضح من التعريفات السابقة أن هنالك شرطين يجب توافرها لتحقيق الاختلاس، يتلخص الشرط الأول بفعل الأخذ، أي أخذ الشيء بغير رضاء حائزه، بحيث يقوم الجاني بإخراج المال من حوزة المجني عليه وإدخاله في حيازته، بحيث يتطلب المشرع تبديل للحيازة، والشرط الآخر هو انعدام رضاء المجني عليه، وإن كان الشرط الأول بحاجه إلى شيء من التوضيح أكثر، حيث إن تبديل الحيازة يتطلب إنهاء سلطه المجني عليه على الشيء، فالضابط في دخوله الحيازة الجديدة، هو استطاعة الحائز الجديد أن يباشر وحده السلطات التي تنطوي عليها الحيازة، بحيث لا يكفي لارتكاب فعل الاختلاس مجرد إخراج الشيء من حيازة المجني عليه إذا لم يعقب ذلك إدخاله في حيازة جديدة، فذلك لا يحقق تبديل الحيازة الذي يتطلبه فعل الاختلاس،[17] وتبديل الحيازة بهذا المعنى، يفترض أن الحيازة لم تكن أصلاً للجاني، وقد يتحقق فعل الاختلاس كما لو كان المال في صورة معلومات هامة بحيث قام صاحبها بتدوينها للحفظ في مستند فقام الجاني بنسخ صورة من تلك المعلومات على المستند بحيث احتفظ بها لنفسه ولإبعاد الشبهات عنه قام بإتلاف المستند الأصلي، فيكون بفعله هذا قد نقل الجاني المعلومات إلى نفسه، وهو ما يتحقق به معنى الاختلاس، وإن كان لمحكمه النقض الفرنسية اتجاه آخر، ففي حكم لها حول واقعه، أن عاملاً في مشروع قام بتصوير مستند يتعلق بنظام العمل في المشروع دون رضاء صاحبه، أيدت المحكمة اعتباره سارقاً للصورة التي قام بتصويرها وليس للمعلومة التي كانت على المستند الأصلي.[18]

من ذلك يتضح أن هنالك اتجاهين مختلفين في تكييف واقعه الاختلاس، إذ يذهب اتجاه إلى أن المعلومات في حد ذاتها يمكن أن تكون موضوعاً للسرقة، وبالتالي تجريم سرقه المعلومات، فالمعلومات وفق هذا الاتجاه يمكن أن تصلح موضوعاً لجريمة السرقة، فالسلوك المادي الصادر عن الجاني والمتمثل في الاستيلاء على المعلومات بأية وسيله فنيه على غير إرادة صاحبها أو حائزها القانوني يعد اختلاساً تقوم به جريمة السرقة إذا ما اكتملت باقي أركانها، على أن تكون تلك المعلومات التي تم الاستيلاء عليها سرية وغير متاحة للكافة بحيث يتحقق الضرر من ذلك الاستيلاء، كما لا بد أن يكون نشاط الجاني صادراً عن إرادة حرة ساعية إلى أحكام السيطرة والحيازة على تلك المعلومات، فمن يقوم بالاستيلاء على أوراق سرية للمؤسسة التي يعمل بها بحيث أراد تصويرها ثم يعيدها فهو سارق لها، [19] أما الاتجاه الآخر فيذهب إلى عدم إمكانية خضوع تلك المعلومات في سرقتها لنصوص السرقة التقليدية، على اعتبار أن المعلومات شيء غير مادي وغير قابل للتملك، وان أمكن وضعه في حيز معين، بحيث لا تقوم سرقة المعلومات بشكل منفصل عن الدعامة المادية التي تحوي تلك المعلومات .

وبالعودة إلى فعل الاختلاس الذي لا يقع إلا إذا كان بغير رضاء المجني عليه، فلا يقوم الاعتداء إلا إذا ارتكب الفعل دون موافقة الحائز لها؛ لأنه إذا تم ذلك بموافقة المجني عليه فلن يكون هنالك اعتداء على حيازته، ويتعين في الرضا وفقاً للقواعد العامة أن يصدر سابقاً أو معاصراً لتبديل الحيازة، أما إذا كان **لاحقاً** عليه فهو لا ينفي فعل الاختلاس،[20] ولا يغني عن الرضا العلم بالفعل، فالعلم بالفعل لا يعني الرضاء به، فقد يسكت اختبارا للمتهم أو استدراجاً له لضبطه في حاله الجرم المشهود، فالعلم المجرد لا يتضمن تعبيراً عن إرادة، ومن ثم لا ينفي عن تبديل الحيازة ما ينطوي عليه من اعتداء عليها، فعدم الرضا لا عدم العلم هو الذي يهم في جريمة السرقة،[21] وبناء على ذلك فإذا أثبتت محكمه الموضوع أن تسليم الشيء إلى المتهم كان برضاء حائزها، ثم أدانت المتهم بالسرقة كان حكمها منطويا على تناقض[22]، كما لم يتطلب المشرع أن يتحقق تبديل الحيازة في السرقة عن طريق وسيلة أو طريقة معينة فكل الوسائل تتساوى، فهي سواء في ارتكاب الجريمة، فليس بشرط أن تكون اليد هي فقط أداء

11 د.محمود نجيب حسني – شرح قانون العقوبات –القسم الخاص –ط6 لسنة 1989 –دارالنهضة العربية – القاهرة – ص838.
12 د. بلال أمين زين الدين – جرائم نظم المعالجة لآليه البيانات – سنه 2008 – دار الفكر العربي – ص 271.
13 د. احمد فتحي سرور – الوسيط في قانون العقوبات – القسم الخاص – ط3 – سنه 1992 – ص806.
14 نقض 1978/10/5 – مجموعة أحكام النقض – ص28 – رقم 24 – ص684.
15 The No Electronic Theft (NET) Act, enacted in 1997 by the U.S. Congress, amended titles 17 and 18, United States Code, to provide greater protection for copyright owners by amending criminal copyright infringement provisions, and for other purposes.
16 د.هدى حامد قشقوش – المرجع السابق – ص 61 وما يليها.
17 د. محمود نجيب حسني – المرجع السابق – ص67.
18 مشار إليه د. عمر الفاروق الحسيني – المرجع السابق – ص103.
19 د. السيد عتيق – جرائم الإنترنت – الطبعة الأولى – سنه 2000 – دار النهضة العربية – ص103 .
20 د. محمود نجيب حسني – شرح قانون العقوبات اللبناني – القسم العام – ص257.
21 نقض 12/ 1/–1942 مجموعه القواعد القانونية – ج-5 رقم –337 ص605.
22 نقض 1929/11/14 – مجموعه القواعد القانونية – ج –1 رقم –324 ص370.

الأخذ، بل يجوز أن يستعين الجاني بأداة منفصلة عن جسمه، كخطاف أو ما أشبه أو حيوان يدربه على النشل، والسرقة تفترض فعل الأخذ ويتحقق ذلك بأن يتم إخراج المال موضوع السرقة من حيازة المجني عليه وإدخاله في حيازة أخرى، فجوهر الأخذ هو استبدال حيازة بحيازة، أما التسليم فهو ينفي فعل الأخذ الذي جرمه المشرع ذلك لأنه ينفي الاعتداء على الحيازة، فلا تقوم جريمة السرقة كذلك إذا كان المال مملوكاً للمتهم.

الركن المعنوي في الجريمة الإلكترونية شأنها شأن أيه جريمة من الجرائم التقليدية، فهي جريمة مقصودة، يتخذ ركنها المعنوي صوره القصد العام والخاص، فلا بد أن ترتكب من شخص قادر على تحمل تبعة أفعاله مدرك لها، ويتحقق القصد الجنائي العام بتوافر عنصريه: العلم والإرادة، ويتخذ القصد الخاص في السرقة نية التملك، ونستعرض كلاهما على البيان التالي:-

القصد العام في اختلاس المال المعلوماتي

القصد العام هو إرادة ارتكاب الجريمة على ما عرفها القانون، ويتم ذلك في إطار الجريمة الإلكترونية بالاعتداء على النظام الإلكتروني، وحسب ما ورد في نص الفقرة 1من المادة 323 من قانون العقوبات الفرنسي الجديد، فالقصد العام يقتضي توافر علم الجاني بالعناصر التي اشترطها القانون في جريمة السرقة، ثم إرادة ارتكاب النشاط المادي للجريمة والذي يبتغي تحقيق النتيجة الإجرامية، حيث **إن** علم الجاني بأن المال مملوك للغير هو قرينة على علمه بما ينطوي عليه فعله من اعتداء على حيازة الغير ومن ثم توافر القصد الجنائي، فهو العلاقة التي تربط بين ماديات الجريمة وشخصيه الجاني وتتمثل في سيطرة الجاني على سلوكه ونتائج هذا السلوك، وجوهر هذه العلاقة الإرادة،[23] فالجريمة تعد مرتكبه عمداً إذا كان الفاعل عالماً بفعله واتجهت إرادته إلى ارتكابه أو كان عالماً أن من شأن فعله أو امتناعه إحداث نتيجة غير مشروعة فرضا بذلك.

القصد الخاص

يتمثل القصد الخاص في هذه الجريمة بتوافر نية تملك الشيء المسروق والظهور عليه بمظهر المالك، وذلك باتجاه إرادة الجاني إلى اختلاس المعلومات والبيانات وإدخاله في حيازته وممارسة سلطات المالك عليها، بحيث يتعين أن يكون الجاني قد قصد من ذلك ليس مجرد الانتفاع بالشيء محل السرقة وردة ثانية، بل يجب أن يكون لديه نية الاحتفاظ بالشيء ومباشرة سلطات المالك عليه حتى يمكن اعتباره سارقاً، فاشتراط هذه النية هو ما يتفق وما يتطلبه القضاء دائما لإدانة المتهم، وتطبيقاً لذلك قضى بأن من يأخذ مالاً مملوكاً للغير بقصد معاينته أو مجرد المزاح مع صاحبه أو الانتفاع به ورده ثانية إلى صاحبه أو الاحتفاظ به كرهن لديه حتى يقوم المجني عليه بسداد دينه لا يعد سارقاً.[24]

لعل التساؤل الذي يطرح نفسه في هذا المقام هل يلزم أن تتعاصر نية التملك لفعل الاختلاس أم يمكن أن تكون نية التملك لاحقه لفعل الاختلاس، انقسم الفقه في الإجابة على هذا التساؤل، نلخص ذلك على البيان التالي:-

الاتجاه الأول: يرى أن فعل الاختلاس الذي يمثل الاستيلاء على حيازة تلك المعلومات والبيانات بقصد تملك المال محل الاعتداء، فلا بدّ من إثبات القصد الجنائي ولحظه تواجده والتي يجب أن تكون لحظه ارتكاب الفعل، فمن الضروري لدى أصحاب هذا الاتجاه أن تتوافر لدى الجاني نية تملك الشيء عند إتيان الفعل المكون للركن المادي حتى يمكن القول باعتبار الفعل سرقة، وأن عدم توافر هذه النية حال ارتكاب الفعل لا يعد الفعل سرقه، وإن توافرت النية بعد ذلك لا يؤثر على تكييف الفعل.[25]

الاتجاه الثاني:- يذهب إلى عدم ضرورة ولزوم تعاصره النية مع الفعل، فإذا ما استولى شخص على مال مملوك للغير بقصد استعماله ثم أعاده إليه مرة أخرى، ثم اتجهت إرادته إلى الاحتفاظ به بنية تملكه يعتبر سارقاً في الحظة التي توافرت فيها هذه النية،[26] فلم يتطلب هذه الاتجاه لزوم معاصرة النية لفعل الاختلاس، بل رتبت توافر نية التملك اللاحقة وإنشاء نفس الأثر القانوني.[27]

2-2 العقبات القانونية التي تعترض تطبيق نصوص الاختلاس على المال الإلكتروني

يعبر البحث عن الطبيعة القانونية للجرائم ومدى إمكانية اعتبارها من ضمن أنماط الجرائم التقليدية بحيث يتم بسط نصوص جريمة السرقة وغيرها من جرائم الأموال، وذلك من خلال الأخذ بالنموذج القانوني لمحل الجريمة، ومع إدراكنا الكلي أن سرقة المعلومات والبيانات المخزنة في جهاز الحاسوب هي أكثر الجرائم المنتشرة في مجال الاعتداء في الجريمة الإلكترونية؛ كون المعلومات والبيانات تشكل محور ارتكازها، والتي لا تزال بحاجه إلى تشريعات تكفل حمايتها من مخاطر الاعتداء عليها.

ولعل التساؤل لذي يطرح نفسه عن مدى انطباق عناصر ونصوص جريمة السرقة العادية (التقليدية) على سرقة المعلومات والبيانات المخزنة في الحاسوب؟ وهل نستطيع من خلال النصوص التقليدية لجريمة السرقة أن نحقق الحماية الجنائية المطلوبة لتلك البيانات والبرامج المخزنة؟

2-2-1 الطبيعة القانونية للمعلومات والبيانات الإلكترونية

بالرجوع إلى دراسة نصوص قانون العقوبات سواء الأردني أو المصري يتضح لنا أن كلاهما لم ينص على تعريف البيانات والبرامج والمعلومات الإلكترونية بحيث تركا ذلك للفقه، وإن كان المشرع الأردني عرف البيانات والمعلومات في المادة 2 من قانون الجرائم الإلكترونية رقم 27 لسنه 2015م، فالبيانات: «هي الأرقام أو الحروف أو الرموز أو الأشكال أو الأصوات أو الصور أو الرسومات التي ليس لها دلالة بذاتها، وعرف المعلومات في نفس المادة بأنها: «البيانات التي تمت معالجتها وأصبح لها دلالة»، كما عرفها نظام مكافحة جرائم المعلوماتية السعودي بأنها: «المعلومات أو الأوامر أو الرسائل أو الأصوات أو الصور التي تعد أو التي سبق إعدادها لاستخدمها في الحاسب الآلي، كالأرقام والحروف والرموز وغيرها»، وعرفها مشروع قرار بقانون المعاملات الإلكترونية الفلسطيني[28]- البيانات الإلكترونية، بأنها: «بيانات ممثله أو مرمزة إلكترونياً سواء على شكل نص أو رمز أو صوت أو غيرها».

كما اتجه الفقه في تعريفها، بأنها: مجموعه من الرموز أو الحقائق أو المفاهيم أو التعليمات التي تصلح لأن تكون محلاً للتبادل أو الاتصال أو التفسير أو التأويل أو للمعالجة بواسطة الأفراد أو الأنظمة وهي تتميز بالمرونة بحيث يمكن نقلها وتجزئتها وجمعها أو نقلها بوسائل مختلفة.[29] وعرفت بأنها: مجموعة الأوامر والتعليمات التي تكتب بلغة معينة والتي تصدر من الإنسان إلى الحاسوب، أي أن البرامج **في جوهره** معلومات والتي تأخذ شكل رسالة يمكن نقلها من خلال وسيلة معينة أو علامة متعارف عليها لنقل هذه الرسالة إلى الآخرين.[30]

إن ظاهرة الجرائم الإلكترونية وفق التحديد المتقدم أفعال غير مشروعة مرتبطة بنظام الحاسوب، ومع أن النصوص القانونية السابق ذكرها لا تحول دون وقوع السرقة على شيء معنوي، أي غير مادي وعلى الرغم من ذلك، فإن نص المادة (311) من قانون العقوبات المصري، والمادة (399) من قانون العقوبات الأردني، لم تشر لا من قريب أو بعيد إلى الشيء أو المال محل السرقة، معنى ذلك أن المشرع لم يتقيد في نصوصه بطبيعة هذا المحل، بحيث يستوي لديه أن تقع السرقة على

23 د. محمود نجيب حسني – النظرية العامة للقصد الجنائي – الطبعة الثالثة 1988-.
24 نقض 1963/5/20 – أحكام محكمة النقض المصرية – س 14 –رقم –84 ص 435.
25 د. أحمد فتحي سرور – المرجع السابق – ص232.
26 لنفرض أن شخصاً وجد دابة مملوكة لآخر وأراد أن يركبها ليصل بها إلى مكان معين وبغير إذن مالكها وبغير أن يكون قاصدا تملكها فهو لا يعد سارقاً بالإجماع؛ لأنه لا يختلسها بقصد تملكها، ولنفترض أن هذا الشخص بعد أن ركب الدابة وسار بها قليلاً بدا له أن يستولى عليها، وتصرف فيها تصرف المالك فيما يملك ، فهل يقال في هذه الحالة أنه لا يعد سارقاً الآن قصد التملك لم يكن مفارقا لوقت وضع يده على الدابة، بحيث يجب اعتباره سارقا لأنه وقت أن اراد الاستيلاء على الدابة لم تكن يده عليها وغير حائز بالمعنى الذي ينتفي معه الاختلاس للمزيد د. نور الدين هنداوي – جرائم الاعتداء على الأشخاص والأموال –المرجع السابق– ص 239.
27 د. السعيد مصطفى السعيد– مجلة القانون والاقتصاد – سنه 12 العدد الأول ص63 . د. رؤوف عبيد – جرائم الاعتداء على الأشخاص والأموال – سنة 1985 – ص352.
28 هو قانون غير نافذ يحمل اسم مشروع قرار بقانون المعاملات الإلكترونية 2016 م .
29 د. نهال عبد القادر المومني – الجرائم المعلوماتية – ط1 – سنة 2008 – دار النشر والتوزيع – ص99.
30 د. محمد فتحي عبد الهادي – مقدمة في علم المعلومات – سنة 1984 – مكتبة غريب – القاهرة –ص 11 وما يليها .

أشياء مادية أو معنوية، أما المشرع الفرنسي في المادة (379) من قانون العقوبات الفرنسي القديم لسنة 1810، وتقابلها المادة (311) من قانون العقوبات الصادر في العام 1994 فذكر كلمة «شيء»، مطلقة دون قيد بحيث يشتمل محل السرقة على الأشياء المادية وغير المادية طالما تقبل السرقة.[31]

ويفسر اقتصار القضاء والفقه على تناول الأموال المادية، أن نصوص السرقة وضعت في ظروف ووقت كانت فيه الأموال المعنوية قليلة العدد والقيمة من ناحية، حيث عمدت في تلك الفترة على توفير الحماية الجنائية للأموال المنقولة المادية والتي كانت لها قيمة كبيرة تفوق قيمة بعض العقارات، ومن ناحية ثانية فإن الأشياء المعنوية الجديدة- والتي لم يؤلها المشرع حمايته في تلك الفترة – زاد عددها مع التطور بحيث زادت قيمتها الاقتصادية حتى إن بعضها زاد عن قيمة الأموال المادية المنقولة والعقارية على السواء، وهذا الأمر غفل عنه المشرع وقت وضع النصوص القانونية لحماية الأموال المنقولة المادية، ويصدق هذا الحال إن كان محل الاعتداء في الجريمة الإلكترونية هي المكونات المادية للنظام الإلكتروني – الحاسوب، والإنترنت – كالأجهزة والمعدات الإلكترونية التي تؤمن وصول الخدمة- شبكة الاتصال-، والحاسبات أو الشاشات وحتى آلات الطبع المرفق بها، وهنالك أيضا البرامج التي تكون عادة مثبته على دعامة أو حامل support مثل الأقراص أو الشرائط والفلاشات أو ما درج على تسميتها وحدات التخزين، والتي يصدق عليها وصف المال وفقاً لتحديد التقليدي، فتلك البرامج والوحدات تصلح لأن تكون محلاً لجرائم الأموال على الرغم أن تلك الوحدات منفصلة تعتبر ضئيلة القيمة إذا ما قيمت بقيمه تلك البرامج، فالاعتداء هنا قد وقع على شيء مادي مما يصلح تكييفه حسب الاعتداء الإجرامي من جرائم الأموال التي يتفق نموذجها مع هذا الاعتداء.[32]

ففي تلك الأحوال السابقة ليس هنالك ما يثار على أننا بصدد جرائم تقليدية تصلح لتطبيق النصوص التشريعية التي عالجت جرائم السرقة والاحتيال، فالحاسوب يعتبر أداة ارتكاب الجريمة الإلكترونية، كما أن الجاني يستطيع من خلال تلك الأجهزة ارتكاب جرائم السرقة أو النصب والاحتيال أو خيانة الأمانة أو تزوير تلك المعلومات، ذلك من خلال التلاعب في الحاسوب والإنترنت،[33] وهذا ما اعتدت به محكمة استئنافAnvers البلجيكية، حيث اعتبرت في حكم لها صادر بتاريخ 13 ديسمبر 1984م أن قيام المتهم بنسخ ثلاثة برامج تحتوى معلومات وبيانات خاصة للمؤسسة التي يعمل بها قاصداً في ذلك تحقيق منفعته الخاصة يشكل جريمة سرقة، وقد بينت المحكمة أساس حكمها: «على أن كلمة شيء (chose) التي وردت في الفقرة الأولى من المادة 461 من قانون العقوبات البلجيكي، والتي نصت على أنه: «كل من يختلس شيئا مملوكا للغير يعد مرتكباً لجريمة السرقة، إنما يجب أن ينظر إليها في إطار المعنى الشائع والمألوف للكلمة بحيث يكون هذا المعنى متوافقا مع مفهوم اختلاس هذا الشيء وهو ما يتحقق حال نسخ البرامج والمعلومات والتي تعد من عناصر الذمة المالية للشركة التي تمتلكها، فهذه البرامج والمعلومات لا تعد – كما يدعي المتهم – مجرد مجموعة من التعليمات ذات الطبيعة غير المادية ولا تصلح بالتالي أن تكون محلاً للاختلاس، وإنما هي على العكس من ذلك أشياء قابلة للنقل وإعادة الإنتاج، كما أن لها أهمية اقتصادية ومن ثم تصلح محلاً للسرقة،[34] حيث إن الاعتداء على البرامج والمعلومات التي توجد داخل الحاسب الآلي يشكل جريمة سرقة؛ لأنه يمثل اعتداء على حق الملكية.

إن ما يتطلب في محل جريمة السرقة أن تتوافر الصفة المادية في موضوعها بحيث يكون مالا، ويقصد بالشيء في الجريمة الإلكترونية الحاسوب أو الكمبيوتر بكل مكوناته، والذي يمكن تعريفه بأنه: مجموعه من الكيانات التي تسمح بدخول المعلومات ومعالجتها وتخزينها واستشارتها أو استرجاعها عند الرغبة، وعلى ما سبق نجد أن هذا الشيء أو المال يتكون من كيانين: كيان مادي، وكيان معنوي، بحيث يشتمل الكيان المادي على الأجهزة المادية المختلفة، وهي تشمل جهاز الإدخال، وجهاز الإخراج، ووحدات التشغيل والتخزين، والتي من خلالها تتم معالجة المعلومات وتخزينها وإخراجها، أما الكيان المعنوي فيشمل البرامج المختلفة التي يتحقق ويتمكن من خلالها الحاسوب من القيام بوظائفه المختلفة،[35] ولطبيعة الكيان المعنوي، هنالك من ذهب إلى عدم التسليم بفكرة الكيان المادي للمعلومات والبيانات الإلكترونية رغم أن التطور التكنولوجي السريع يحتم ذلك، على اعتبار أن العلة من اشتراط أن يكون موضوع أو محل جريمة السرقة مال منقول مملوك للغير، وعليه فإن المعلومات والبيانات لا تصلح محلاً لجريمة السرقة لكونها تقع على مال مادي وليس معنوي؛ كون المال المعنوي يتجرد وفق هذا الاتجاه من الصفة المادية، فجريمة السرقة هي اعتداء على حق الملكية، ومن شروط موضوع الاعتداء يلزم شروط تنتج من فكرة واحدة، وهي ضرورة أن يكون الشيء الذي ينصب عليه السلوك الإجرامي محلاً لحق الملكية، بحيث ينال الاعتداء بارتكاب ذلك السلوك، مما يتطلب وجوب كون ذلك الشيء مالاً حتى نتصور صلاحيته محلا للحق ثم وجوب كونه مملوكاً لغير مرتكب الجريمة، بحيث يتصور أن يكون ثمة اعتداء من المجرم على ملكيه غيره.

2-2-2 الحجج المؤيدة لتطبيق نصوص جريمة السرقة على المال المعنوي

اختلفت الآراء في تحديد ما إذا كانت المعلومات والبيانات تعد كيان مادي أم كيان معنوي وحتى نتمكن من القول بكون تلك المعلومات والبيانات محلاً لجريمة السرقة الإلكترونية، يجب أن يصدق عليها وصف المال، حيث يظهر من خلال التعريفات السابقة، أن المعلومات تعد من قبيل الأشياء المعنوية لا المادية، مما يشكل صعوبة في تطبيق نصوص جريمة السرقة التقليدية على سرقة المعلومات والبيانات المخزنة على جهاز الحاسوب؛ لانعدام الكيان المادي لتلك المعلومات والبيانات، ولعل التساؤل الذي يثار حول مدى صحة انطباق وصف المال على تلك المعلومات والبيانات بالرغم من طبيعتها اللامادية، ولتوضيح مدى صحة انطباق وصف المال على تلك المعلومات نتناول الحجج التي تعتبر الأشياء المعنوية تصلح لذلك على النحوالتالي

- لقد عرفت الفقرة 1 من المادة (81) من القانون المدني المصري المال بأنه: «هو كل شيء غير خارج عن التعامل بطبيعته أو بحكم القانون»، وبحسب ما ورد في نص المادة (53) من القانون المدني الأردني فان تعريف المال: «هو كل عين أو حق له قيمة مادية في التعامل»، كما نصت المادة 54 من نفس القانون على أن: «كل شيء يمكن حيازته مادياً أو معنوياً والانتفاع به انتفاعاً مشروعاً ولا يخرج عن التعامل بطبيعته أو بحكم القانون يصح أن يكون محلاً للحقوق المالية»، وقد قضت محكمة التمييز الأردنية بأن المال هو: «كل شيء يمكن حيازته مادياً أو معنوياً والانتفاع به انتفاعاً مشروعاً، ولا يخرج عن التعامل بطبيعته أو بحكم القانون»،[36] ومن خلال التعريفات السابقة للمعلومات والبيانات، فإن الشيء في نظر القانون يتطلب _وهو هنا المعلومات والبيانات – شرطين حتى ينطبق عليه وصف المال، وهما: إمكانية الحيازة والانتفاع المادي بها.
- فالموضوع في جريمة السرقة هو كل ما يصلح أن يكون محلاً لحق من الحقوق المالية سواء أكان مادياً أم معنوياً، بحيث أدخلت الأشياء المعنوية ضمن المال، وهذا ما بينه المشرع الأردني الذي يتبنى اعتبار المال المعنوي من الحقوق المالية التي يمكن حيازتها، وكذلك المشرع المدني المصري لم يعتبر المال المعنوي خارج التعامل بحكم القانون، وبالتالي فالقانون الأردني والمصري يعتبران المال المعنوي قابلاً للسرقة، وعليه فالأشياء تنقسم إلى أشياء مادية، وأشياء غير مادية أو معنوية، علماً بأن الأموال من وجهه النظر التقليدية لجريمة

31 د. هدى حامد قشقوش المرجع السابق – ص65،66.

32 Hardy, I. Trotter (2002). "Criminal Copyright Infringement". William and Mary Bill of Rights Journal 11: 209342-.

33 د. محمد على العريان – الجرائم المعلوماتية – سنة 2004 – دار الجامعة الجديدة للنشر – ص 47.

34 مشار إليه في :نائلة عادل محمد فريد ، المصدر سابق ، ص 135 ؛ وينظر: عفيفي كامل عفيفي ، جرائم الكومبيوتر ، دراسة مقارنة ، منشورات الحلبي الحقوقية ، ط2 ، 2007 ، ص 151.

35 د. هدي قشقوش – جرائم الحاسوب الإلكتروني في التشريع المقارن – سنة 1992 – دار النهضة العربية – القاهرة – ص 124 وما يليها.

36 قرار محكمة التمييز الأردنية (حقوق) رقم 609 /1986 –هيئه عامه – تاريخ 1987/2/4 منشورات مركز عدالة .

السرقة لا ترد إلا على الأشياء المادية بحيث يكون له حيز مادي ملموس يمكن حيازته، مهما كانت قيمة المال ،حيث تقع جريمة السرقة ولو كان المال المسروق تافه القيمة، فالسرقة اعتداء على الملكية والحيازة معاً؛ لأن المحل الأصلي للاعتداء هو الملكية، أما الحيازة فهي اعتداء عرضا، وهو غير مقصود لذاته، فالجاني يتجه في قصده إلى الاعتداء في الجرائم الإلكترونية على الشيء أو المال الإلكتروني، بحيث يكون هذا الشيء أو المال محلاً أو موضوعاً لها.

- أن الأصل في تطبيق النص الجنائي أن يتم بعيداً عن المعايير المسبقة التي تحكمه وفقاً لمبدأ الشرعية، فالنظرية الشخصية في تفسير النص الجنائي تكمن وتحدد في نطاق الهدف الذي كان يقصده المشرع وقت وضع النص، إلا أن الحاجة الناتجة عن التطور العلمي تدعو إلى معالجه حالات جديدة لم تكن معروفه وقت وضع النص، لذلك نرى صحة أسلوب النظرية الموضوعية في التفسير في مجال تجريم السلوكيات المتعلقة بالجرائم الإلكترونية، حيث تهدف هذه النظرية إلى البحث عن المصلحة الحقيقة للمشرع التي أراد حمايتها،[37] وهذا يتم من خلال تطبيق النص الجنائي التقليدي على الحالات التي لم تكن موجودة وقت أن تم وضع النص، مثال ذلك: سرقة التيار الكهربائي والتي تم تطبيق نصوص جريمة السرقة التقليدية عليه،[38] وكذلك التوسع في تعريف الطرق الاحتيالية لما شاهدته هذه الجريمة من طرق جديدة بحاجة إلى معالجة حيث إن علة النص الواردة في النصوص التقليدية للجريمة السرقة والاحتيال يمكن تطبيقها على بعض جرائم الأموال الإلكترونية الحديثة ومنها سرقة المعلومات والبيانات الإلكترونية.
- أن التطورات التي حدثت في الزمن القريب وما زالت مستمرة جعلت بعض الأشياء المعنوية – في مجال المعلومات والبيانات الإلكترونية – أكثر أهمية وقيمة من الأشياء المادية، مما استدعى إعادة النظر في حصر الأموال على الأشياء المادية فقط، مما دفع إلى إعادة النظر في ذلك والبحث عن معيار آخر غير طبيعة الشيء الذي يرد عليه الاعتداء من كونه مال، مما يسهل من إصباغ صفة المال على الشيء المعنوي، ومن تلك الأشياء المعنوية ذات القيمة المالية المعلومات والبيانات التي يحتويها الحاسوب ويتم التعامل بها عن طريق الشبكة الإلكترونية، حيث إن هذه المعلومات والبيانات بالغه الأهمية في مجال تكنولوجيا المعلومات، ففي ببعض الأحيان ترتفع قيمه تلك المعلومات والبيانات عن قيمة الأموال المادية، مما تدفع باتجاه إمكانية إصباغ صفة المال على المكونات المعنوية للنظام الإلكتروني على أساس ما تتمتع به من قيمة مالية اقتصادية.[39]
- أن الجريمة الإلكترونية تتفق مع جريمة السرقة من كون كلاهما يتطلب طرفي الجريمة الجاني والمجني عليه، حيث في الجريمة الإلكترونية يتجه قصد الجاني إلى الاعتداء على الشيء أو المال الإلكتروني (البيانات والمعلومات الخزنة)، حيث إن هذا الشيء أو المال محلاً أو موضوعاً للجرائم الإلكترونية، وتشمل الحاسوب أو الكمبيوتر بكل مكوناته التي تسمح بدخول المعلومات والبيانات والبرامج ومعالجتها وتخزينها وإخراجها ونقلها عبر ذلك الجهاز ومكوناته، وبالتالي فهي تمثل أهمية اقتصادية كبيرة وبدونها لا يكون للحاسوب قيمة أكثر من قيمة المواد التي صنع منها، فالفقه الحديث يرى أن الضابط في اعتبار الشيء مالاً ليس على أساس ماله من كيان مادي، وإنما على قيمه تلك المعلومات من الناحية الاقتصادية، ولعل ذلك مرده أن مفهوم الشيء أو المال نابع من الذهن وليس من طبيعة هذا الشيء، لذا فإن تلك المعلومات والبيانات وما يتفق معها من حيث الطبيعة وإن **كانت** شيئا غير ذو كيان مادي، فإن لها قيمه اقتصادية تستحق الحماية القانونية لما تشتمل عليه تلك البرامج والمعلومات والبيانات الخاصة بالحاسوب والإنترنت من قيمة اقتصادية ومالية، علماً أن المشرع الحديث يعترف لصاحب هذه المعلومات بما يطلق عليه الحق في الملكية الذهنية أو الأدبية التي لصاحبها الحق في سرية تلك المعلومات واحتكارها واستغلالها بالكيفية التي يرغب، بها دون أي اعتداء من الآخرين.[40]
- أن البرامج والمعلومات والبيانات لها كيان مادي يمكن رؤيته على الشاشة مترجمة إلى أفكار وأنه يمكن قياس سرقة هذه البرامج على سرقة الكهرباء والهاتف،[41] الأمر الذي يمكن أن يستنتج منه أن جريمة السرقة تقع في كل حالة يحرم فيها مالك أو حائز لشيء – ولو لفترة قصيرة – من مميزات حق الملكية التي له على الشيء حتى ولو لم يتحرك هذا الشيء من مكانه». [42]حيث مدت بعض نصوص قوانين العقوبات المتصلة بتجريم الأموال وتحديداً نصوص السرقة على سرقة الكهرباء نتيجة قياسها عليها، وأيدها في ذلك بعض الفقهاء، بحيث أشاروا إلي إمكانية مد القواعد القانونية التي تنطبق على السرقة بحيث تنطبق على جرائم القرصنة والنسخ، فالسرقة تتم بنشاط إيجابي، وهو نسخ البرامج أو تصويره، وأن أسلوب الأخذ (الاختلاس) قد تطور بأن تتم جريمة السرقة بأخذ نسخة من تلك البرامج أو المعلومات.[43]
- في جريمة السرقة كل شيء يصلح محلاً لحق عيني، والأصل أن كل شيء نافع للإنسان – أي يستطيع أن يشبع حاجة له – يصلح أن يكون هدفاً لاستئثار بعض الناس به وإنشائهم الحقوق عليه، فهذه الأشياء ذات فائدة للأفراد وللمجتمع والاستئثار به، يعني وجوب كونه ذا قيمة أو متقوم، ولم يشترط أن تكون قيمه الشيء مادية فإذا لم تكن للشيء غير قيمه معنوية كالخطاب والأوراق فهي متقوم، [44] ويصلح موضوعاً للسرقة حتى ولو كان قصاصه من ورق، طالما يمكن أن تخضع لسيطرة الإنسان ويسعه أن يوجهها على النحو الذي يحقق منفعته فهي من جرائم الضرر؛ لأنها تقع بخروج المنقول من ملكية صاحبه إلى الفاعل، وقد يترتب على هذا الأخذ ضرر إما أن يكون مادياً وقد يكون أيضاً ضررا معنوياً.
- أن المشرع الفرنسي في قانون العقوبات الجديد وتحديداً المادة 311، أورد كلمة شيء والتي تشمل الأشياء المادية وغير المادية، فطالما أمكن حيازة الأشياء غير المادية مثل: حق الارتفاق والدين وحق الانتفاع، فإنه لا يوجد ما يمنع حيازة المعلومات والتي تخضع لسلب الحيازة، فالتشريع الفرنسي كان السباق في حماية المال المعلوماتي، ويظهر ذلك في الفقرتين 2/1 من المادة 323 من القانون الجنائي الفرنسي النافذ، كما لعب القضاء الفرنسي دور كبير في تطويع النصوص العقابية التقليدية وفسرها تفسيرا دل على حرصه على توفير أكبر قدر من الحماية لهذه الأموال موضع الجدل والنقاش،[45] على خلاف التشريعات والقضاء في غيرها من الدول التي ما زالت بعيدا عن معالجة هذا القضايا المستحدثة وتطبيقها على هذا المال المعلوماتي، باستثناء الدول التي عملت على سن تشريعات خاصة لمواجهه الجرائم الإلكترونية.

وعلى ما سبق نجد أن تحديد طبيعة معطيات الحاسوب والمعلومات تعد حجر الأساس في تقدير الموقف من قابلية تطابق النصوص التقليدية، لا على جريمة الاختلاس فقط، بل وعلى طائفة معتبرة من جرائم الحاسوب، وما أثير بشأنها من خلاف حاد ومتعارض أشبه ما يكون بالخلاف الذي أثير حول مدى شمول نصوص السرقة لأنشطة الاستيلاء

37 د. محمود نجيب حسني – شرح قانون العقوبات – سنة 1979 – دار النهضة العربية –ص 66 وما يليها.
38 اصدارت بعض الدول ومنها مصر قانون الكهرباء رقم 87 لسنة 2015 والذي نظم جريمة سرقة التيار الكهربائي والعقاب عليه.
39 د. نهال عبد القادر المومني – المرجع السابق – ص 109 .
40 د.عبد الرشيد مأمون شديد – الحق الأدبي للمؤلف – النظرية العامة وتطبيقاتها – رسالة دكتوراه – سنه 1978 –دار النهضة العربية – ص22 .
Mark Motivans (2004). Intellectual Property Theft, 2002 (Report). Bureau of Justice Statistics.
41 جرائم المعلوماتية بحث منشور على الإنترنت ، متوفر على الموقع الآتي :
(http://www.djelfa/vb/showthreadphp?t=204052) 10- 3- 2015
42 د.عفيفي كامل عفيفي، مرجع سابق ، ص 153.
43 د. نائله عادل محمد فريد ، جرائم الحاسب الالي الاقتصادية، دراسة نظرية وتطبيقيه ،ط1 ، (لبنان :منشورات الحلبي الحقوقية، 2005)، 133 وما بعدها – ينظر أيضاً د. منير محمد الجنبيهي وممدوح محمد الجنبيهي(2005)، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها ، دار الفكر الجامعي، الإسكندرية ، 106 .
44 د.محمود نجيب حسني – المرجع السابق – ص32
45 انظر: هذا الحكم القضائي لدى: TGI Paris 1 ch. Correctionelle 16 Dec. 1997, Ministere Publique C. Glovanisky, dis. Enligne en Dec. 2000, a:http://www.legalis.net.

على القوى المحرزة كالكهرباء وخطوط الهاتف، وأساس مشكلة الخلاف الدائرة الآن حول فهم طبيعة المعلومات والبيانات ومدى إمكان إخضاعها لنصوص جريمة السرقة في البلدان التي لا يوجد فيه تشريعات خاصة بالجرائم الإلكترونية، وهي نفسها من أسباب الخلاف الذي كان مثارا حول طبيعة التيار الكهربائي والاعتداء عليه، حيث إن الموقف من تجريم سرقة الكهرباء في بدايته يشبه إلى حد قريب من الجدل الدائر الآن حول صلاحية المعلومات ومعطيات الحاسوب للسرقة، بحيث تم في النهاية تطبيق نصوص السرقة التقليدية على سرقة التيار الكهربائي، فقد توسعت النظم القانونية في دلالة تعبير المال أو الشيء المادي، وذلك إما من خلال الاجتهاد القضائي أو التشريعي من خلال نصوص صريحة في قانون العقوبات، بحيث اتصلت في نطاق القوى المحرزة، كالطاقة الكهربائية سواء من خلال اعتبار الكهرباء ذات كيان مادي ملموس وبالتالي تصلح محلاً للملكية والحيازة، أو بالاعتماد على قيمة الكهرباء الاقتصادية، ونحن لسنا في هذا المقام لتوضيح الاتجاهات التي دارت إلى أن تم إخضاع سرقة التيار الكهربائي إلى نصوص جريمة السرقة، ذلك أن الكهرباء مادة تحولت إلى طاقة تتدفق عبر الأسلاك لمقتضيات الاستخدام والاستعمال في مجالات مختلفة، وهي في نفس الوقت مال؛ لأنها ذات قيمة مالية، فمقابل الاستعمال والاستخدام هنالك عائد مادي كبير، كما أنه منقول لإمكان حيازتها وملكيتها ونقلها من مكان لآخر دونما اعتبار لطبيعته أو لصورته، وقد أكدت محكمة النقض المصرية على أن التيار الكهربائي مالاً منقولاً عندما قضت في أحد أحكامها: «أن التيار الكهربائي منقول قابل للتملك والحيازة وبالتالي للسرقة»،[46] وبعبارة أخرى فالاختلاس في جريمة سرقة التيار الكهربائي تقوم على عنصرين كما هو في جريمة السرقة العادية: يتمثل العنصر الأول في سلب حيازة التيار الكهربائي أو الاستيلاء عليه هو العنصر المادي، والعنصر الآخر هو العنصر المعنوي، وهو عدم رضا مالك أو حائز التيار الكهربائي.

ولعل صلاحية المعلومات والبرامج للاختلاس ينطلق بالاعتماد عما سبق من الحديث عن سرقة التيار الكهربائي، ومن خلال مقارنه ذلك بسرقة التيار الكهربائي من حيث طبيعة الشيء محل السرقة أو بالنظر إلى كيفية الاستفادة منه وأسلوب استخدمه والذي يمكن الجاني من القيام بالنشاط المحقق للاختلاس، فالأشياء المادية لا تثير صعوبة عند اختلاسها من خلال نشاط مادي، بحيث يمكن وقوع الاختلاس على المعلومات والبيانات الموجودة على الدعامة التي تثبت عليها، ولكن الموضوع يختلف حين يكون الاستيلاء على المعلومات دون الاستيلاء على تلك الدعامة، فالصورة الأولى لا تثير إشكالاً كون الجاني قد استولى على شيء معنوي، فهو هنا لم يقم بأي نشاط مادي، بل إن ما قام به مجرد نشاط ذهني (معنوي) للسيطرة على تلك المعلومات سواء كان بالنظر أو بالسمع الذي أدرك به المعلومات ثم اختزنها في ذاكرته، فذلك يؤدي إلى تحقيق الاختلاس بحق من يقرأ أو يسمع معلومة أو برنامج علما أن القانون لا يعاقب على الأفكار ومجرد النوايا، وعلى الرغم من كون المعلومات لا تعد شيئاً مادياً فإن إنقاص الذمة المالية للشيء المادي يتحقق بخروج الشيء من ذمة المجني عليه ودخوله في ذمة الجاني، أما إذا كان الشيء غير مادي (معنوي)، فإننا لا نكون بحاجة إلى مثل ذلك، ونقل الشيء كون الاختلاس ما هو إلا إنقاص لذمة المجني علية، وإنقاص ذمة الأخير قد تمت بانتقاص قيمة المعلومات؛ لأن صاحب (حائزها) المعلومات والبرامج أو مالكه لم يعد هو الوحيد صاحب المعلومة على الرغم من أن أصل المعلومة لا زال بين يديه بل أصبح هنالك من يزحمه في ذلك، فهو لم يبقَ الحائز أو صاحب الحق الوحيد في احتكار المعلومة واحتكار استغلالها واستعمالها.

3-0 إجراءات التفتيش والضبط في جرائم الاختلاس الإلكتروني

يعد التفتيش من أهم وأخطر إجراءات التحقيق،[47] ونظراً لهذه الأهمية، نجد العديد من الدول التي رفعت هذا الحق إلى مصاف الحقوق الدستورية؛ كونه السياج الذي يحمي الحياة الخاصة للإنسان ضد تعسف وانتهاكات من أوكل لهم المشرع مهام التنقيب والبحث والمعاينة وضبط الأشياء المتعلقة بالجريمة، والتي تفيد وتساهم في كشف الحقيقة في مستودع السر، والتفتيش يجب أن لا يخدش كرامة الإنسان؛ وذلك إعمالاً لقوله تعالى في سورة الإسراء: (وَلَقَدْ كَرَّمْنَا بَنِي آدَمَ وَحَمَلْنَاهُمْ فِي الْبَرِّ وَالْبَحْرِ وَرَزَقْنَاهُم مِّنَ الطَّيِّبَاتِ وَفَضَّلْنَاهُمْ عَلَى كَثِيرٍ مِّمَّنْ خَلَقْنَا تَفْضِيلاً)،[48] فنص القانون الأساسي الفلسطيني في الفقرة 2 من المادة 11 بالنص: «لا يجوز القبض على أحد أو تفتيشه أو حبسه أو تقيد حريته بأي قيد أو منعه من التنقل إلا بأمر قضائي وفقاً لأحكام القانون، كما نص نفس القانون في المادة 17 على حرمة المساكن حيث جاء فيها: «للمساكن حرمة، فلا تجوز مراقبتها أو دخولها أو تفتيشها إلا بأمر قضائي مسبب ووفقاً لأحكام القانون ...»، كما نص الدستور الأردني على هذا الحق في المادة 11 من الدستور الأردني على حرمة المساكن وذكر أن: «للمساكن حرمة فلا يجوز دخولها إلا في الأحوال المبينة في القانون وبالكيفية المنصوص عليها فيه»، وكذلك قرر الدستور المصري هذا الحق فنص في المادة 44 منه على أن: «للمساكن حرمه فلا يجوز دخولها ولا تفتيشها إلا بأمر قضائي مسبب وفقاً لأحكام القانون»، تقابلها المادة 31 من الدستور السوري.

كما أن الاتفاقية الأوروبية لحماية حقوق الإنسان والحريات الأساسية لسنة 1950م، والتي أكدت المادة 8 منها على أنه: «لكل شخص الحق في احترام الحياة الخاصة والعائلية ومسكنه ومراسلاته» ،وقد أصدرت المحكمة الأوروبية لحقوق الإنسان عدة أحكام تتعلق بالتفتيش، وكان من شأن هذه الأحكام أن قامت فرنسا بإصدار قانون جديد لتنظيم مراقبة المحادثات لسنة 1991م،[49] وفي هذا الاتجاه شدد المجلس الأوروبي منذ عام 1989م على ضرورة تدويل جرائم التكنولوجيا، وخاصة المتعلقة بالمعلوماتية، وفي نفس السنة أقر مجلس الوزراء الأوروبي توصية تحث الدول الأعضاء على ضرورة مراجعة قوانينها الإجرائية لتكون قادرة على مواكبة الجرائم الإلكترونية وما يلحقها من تطور، وذلك من خلال تنظيم إجراءات التفتيش والضبط، وضرورة الرقابة الفنية من أجل نجاح التحقيق الجنائي بخصوص هذه الجرائم، ومرجع ذلك عجز القوانين الجنائية الموضوعية والإجرائية التقليدية وحدها لمواجه الجرائم المعلوماتية عابرة الحدود، بل لا بد من إيجاد استراتيجيات مكملة على المستوى الفني التقني والقضائي وتحديث الآليات التقليدية على مستوى التعاون القضائي الدولي، كما أوصى المؤتمر على الصعيد الإجرائي بوضع كافة الإمكانات تحت تصرف سلطات التحقيق والتحري، شرط التوازن والملاءمة بين تطبيق تلك الحقوق والإجراءات، وفي نفس الوقت احترام حقوق الإنسان وحرمة الحياة الخاصة، بحيث لا تقبل تقيد حقوق الإنسان من قبل السلطات العامة إلا على أساس قانوني واضح غايته مكافحة الجرائم الإلكترونية والحد منها.[50]

لذلك نرى أن نقسم الدراسة في هذه المبحث إلى ثلاثة مطالب :

المطلب الأول: أشكليات التفتيش وما في حكمه في البيئة الإلكترونية.

المطلب الثاني: مدى قابلية جرائم الحاسوب والشبكات الإلكترونية للتفتيش عن أدلتها.

المطلب الثالث: ضبط أدلة جرائم الحاسوب والانترنت واجراءات ذلك.

3-1 اشكايات التفتيش في البيئة الإلكترونية.

إن البحث في الغاية من التفتيش ومدى قابلية مكونات الحاسوب والشبكات الإلكترونية المرتبطة به ترجع إلى أهمية تحديد ماهية التفتيش والغاية منه، بحيث تكمن الغاية من التفتيش في الوصول إلى ما تحويه نظم الحاسوب من أشياء مادية أو معنوية تفيد في كشف الحقيقة ونسبتها إلى المتهم وما دار حول ذلك من جدل فقهي ونقاش حول مدى إخضاع مكونات الحاسوب إلى التفتيش، وبحيث نتناول هذا المطلب على البيان التالي :-

46 نقض 1937/4/5 مجموعه القواعد القانونية – ج4 – ص63.
47 جلسة 25/ 9/ 2002 الطعن رقم 8792 – لسنة 72 ق– محكمة النقض المصرية.
48 سورة الإسراء – الآية 70.
49 د.حسام احمد – الإذن بالتفتيش والضبط « دراسة مقارنة « ط-3 سنة 2003 –دار النهضة العربية –ص3.
50 د– عمر الفاروق الحسيني ، المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية، مرجع سابق، صـ48 وما بعدها.

3-1-1 الغاية من التفتيش

إن التفتيش عبارة عن الاطلاع على محل منحه القانون حرمة خاصة، باعتباره مستودع سر صاحبه، فلا يجوز الاطلاع عليه أو على ما بداخله إلا في الأحوال المنصوص عليها قانوناً، أو برضاء صاحبه، وقد يكون محل التفتيش الشخص أو المسكن أو محلاً أخر ألحقه القانون في الحكم بالمسكن،[51] فالتفتيش مقرر للبحث عما يظهر حقيقة أفعال جرمها القانون، ويخضع التفتيش لأحكام مقررة بموجب القانون، والتفتيش في الجرائم الالكترونية ليست بالبسيط، فهنالك مكونات الحاسوب المادية والمعنوية الخاضعة للتفتيش، حيث يتطلب التفتيش معرفة ودراية بملفات الحاسوب وما يتصل به، وترجع صعوبة ذلك إلى سهولة إتلافها، مما يصعب تحديد مكان الدليل في البيئة الإلكترونية، فالتفتيش ومع أنه إجراء يمس حق السر إلا أنه شرع من أجل مصلحة أكبر وهي مصلحة المجتمع في شعوره بالأمن والطمأنينة ومكافحة الجريمة؛ لذا يتعين عدم اللجوء إليه إلا بعد حصول الجريمة ووجود قرائن جدية بأن الشخص المنوي تفتيش مسكنه هو فاعل الجريمة أو شريك فيها. [52]

ولذلك يقع باطلاً التفتيش الذي يقع لغاية أخرى غير ما حدده المشرع؛ لأن كل تفتيش يتم بغير أن يتبين وجه المصلحة منه يكون باطلاً، ويعد التفتيش من الإجراءات التي لا غنى عنها للمحقق في تقوية أواصر الأدلة أو في إسناد الواقعة في مواجهة المتهم، فالعثور على أدلة الجريمة من شأنه تقوية الاتهام ضد المتهم وبالتالي عدم إفلاته من العقاب، أو تقوية أدلة البراءة وبالتالي الحكم بإخلاء سبيل المتهم والحكم له بالبراءة.

وعلى الرغم من كون التفتيش من أهم إجراءات التحقيق، لما فيه من مساس بحريات وحقوق الأفراد ومستودع أسرارهم، نجد القليل من التشريعات التى عمدت الى تعريف التفتيش[53]؛ لكن معظمها ترك التعريف للقضاء والفقه، إذ عرفت محكمة النقض المصرية التفتيش بأنه: «هو ذلك الإجراء الذي رخص الشارع فيه التعرض لحرمة ما بسبب جريمة وقعت أو ترجح وقوعها، وذلك تغليباً للمصلحة العامة على مصالح الأفراد الخاصة واحتمال الوصول إلى دليل مادي يفيد في كشف الحقيقة[54]، كما عرفته بأنه: «البحث عن عناصر الحقيقة في مستودع السر فيها» ،[55] ويلاحظ على هذه التعريفات إغفاله لركيزة أساسية كان يفترض أن تتضمنها، كبيان القائم بهذا الإجراء، لذا فهو إجراء تقوم به سلطة التحقيق ومن تفوضه بذلك من رجال الضابطة القضائية للبحث والتنقيب والاطلاع على محل أو مسكن يتمتع بحرمة خاصة للبحث عن الأدلة اللازمة في مستودع السر؛ لاستكمال التحقيق الجنائي بغض النظر عن إرادة صاحبه، وقد وفق المشرع الفلسطيني في توضيح مفهوم التفتيش، حيث جاءت الفقرة (1) من المادة 39 من قانون الإجراءات الفلسطيني ونص على أن: «دخول المنازل وتفتيشها عمل من أعمال التحقيق لا يتم إلا بمذكرة من قبل النيابة العامة أو في حضورها، بناء على اتهام موجه إلى شخص يقيم في المنزل المراد تفتيشه بارتكاب جناية أو جنحة أو باشتراكه في ارتكابها، أو لوجود قرائن قوية على أنه يحوز أشياء تتعلق بالجريمة»، إذ جاء التعريف واضح على مضمون التفتيش وعلى السلطة التي تقوم به، محدداً في نفس الوقت الجرائم التي تستدعي تفتيش مستودع السر بحصر التفتيش على جرائم من نوع الجنايات والجنح مستبعدا جرائم المخالفات ذلك لضئالة الحق المعتدى عليه، وعلى نفس المعنى نصت المادة 91 من قانون الإجراءات الجزائية المصري، كما نصت الاتفاقية الأوربية عن التفتيش والضبط، فقد أجازت المادة (32) من الاتفاقية الأوروبية بشأن مكافحة الجرائم المعلوماتية والتي أعدها المجلس الأوروبي (The Council of Europe) وتم التوقيع عليها في بودابست في عام 2001م إمكانية الدخول بغرض التفتيش والضبط في أجهزة حاسب أو شبكات تابعة لدولة أخرى بدون إذنها في حالتين: الأولى إذا تعلق التفتيش بمعلومات أو بيانات متاحة للعامة، والثانية: إذا رضي المالك أو حائز هذه البيانات بهذا التفتيش، ومن هنا تظهر الغاية من التفتيش لكونه إجراء تحقيقي تتولاه سلطة مختصة للبحث عن أدلة الجريمة وجمعها هادفاً من ذلك الكشف عن جريمة في محل خاص يتمتع بالحرمة دون اعتبار لإرادة صاحبه أي سواء رضي أم لم يرضَ، فيجب أن يتم التفتيش على وفق الغرض الذي أعد له، بمعنى أن تكون غاية التفتيش ضبط الأشياء المتعلقة بالجريمة أو التي تفيد في كشف الحقيقة.

3-1-2 مدى خضوع مكونات الحاسوب المادية والمعنوية للتفتيش

إن التفتيش في هذه البيئة ينظُر إليه في الغالب على أنه غير مجد لما يكتنفه من صعوبات أثناء تنفيذ التفتيش، خاصة ما يتم في الفضاء الافتراضي (في بيئة الإنترنت) مقارنة بالجرائم التقليدية، فضلاً عن صعوبة إثبات واكتشاف الجريمة الإلكترونية للأسباب التالية:

- سهولة إخفاء الجريمة الإلكترونية.
- غياب الدليل المادي.
- سهولة محو وإتلاف آثار الجريمة الإلكترونية في وقت قصير.
- إحجام المعتدي عليهم عن الإبلاغ، إما عن جهل أو نقص خبرة.
- نقص خبرة القائمين على مكافحة الجريمة الإلكترونية من حسن طريقة التفتيش والبحث عن الأدلة.[56]

عند الحديث عن تطبيق إجراء التفتيش على مكونات الحاسوب والشبكات المرتبطة به من خلال الإنترنت وما يوصل بينهما من أسلاك وملحقات، فإن للحاسوب مكونات مادية (Hardware) وأخرى معنوية أو برمجية (Software)، كما أن له شبكات اتصال (Network Telecommunications) سلكية وغير سلكية محلية ودولية.

والتفتيش عن الأدلة في الجريمة الإلكترونية، هو تفتيش عن معطيات الحاسوب المادية وغير المادية المخزنة في الحاسوب، والتي هي عبارة عن ذبذبات إلكترونية قابلة للتخزين والحفظ في الجهاز أو على أقراص وإسطوانات، ولعل التفتيش الذي يرد على مكونات الحاسوب المادية وملحقاته لا خلاف يذكر حول خضوعها للتفتيش والضبط طبقاً لقواعد قانون الإجراءات الجزائية، بما في ذلك البيانات والمعلومات المخزنة في أوعية أو وسائل مادية كالأشرطة الممغنطة والأقراص الصلبة والضوئية، وذلك تبعاً للمكان أو الحيز الموجودة فيه،[57] بحثاً عن أي دليل يتصل بالجريمة الإلكترونية التي وقعت، ويخضع تفتيش الحاسوب والمكونات المادية إلى أحكام تفتيش المكان الذي يوجد به ذلك الجهاز، فإذا كان الحاسوب مودعاً في مكان خاص، فإنه يخضع لحكم الأماكن الخاصة وتلحق بالشخص المتهم، كمسكن المتهم أو أحد ملحقاته، فتأخذ حكم المسكن، فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكن المتهم، وبذات الضمانات المقررة قانوناً في التشريعات المختلفة، وقد يطال التفتيش أيضاً شخص صاحبه، فقد يكون مستودع السر في المسكن أو ملحقاته وقد يكون في الأوراق الخاصة بالمتهم أو ما يملك بالمسكن، ويتعين على الخاضع له الإذعان للقائمين بالتفتيش لإكمال المهمة المنوطة بهم، فإذا كانت موجودة بمسكن المتهم أو أحد ملحقاته فتحكمها القواعد ذاتها التي يخضع لها تفتيش المسكن، إذ يجوز ضبطها وتفتيشها متى كان تفتيش المسكن جائزاً، والعكس صحيح، وفي حال وجودها في مكان عام فيحكمها ما يحكم هذا المكان من أحكام.

وقد دار حول مدى خضوع مكونات الحاسوب المعنوية للتفتيش خلاف كبير في الفقه بشأن جواز تفتيشها من عدمه، فذهب رأي إلى جواز تفتيش البيانات الإلكترونية بمختلف أشكالها، حيث اعتبر هذا الرأي أن المكونات المعنوية لا تختلف عن الكيان المادي للحاسوب من حيث خضوعها لإجراءات التفتيش وما في حكمه، على اعتبار أن البيانات والمعلومات عبارة عن نبضات إلكترونية قابلة وممكنة التخزين على

51 د.حسن صادق المرصفاوي- أصول الإجراءات الجنائية – الطبعة الأخيرة – سنة -1983 منشاة المعارف – الإسكندرية- ص37.

52 د.عبد الحميد الشواربي- إذن التفتيش في ضوء الفقه والقضاء – منشاة المعارف – الإسكندرية- ص10.

53 ذهب المشرع السعودي في المادة 80 من نظام الإجراءات السعودي إلى تعريف التفتيش بأنه: «التفتيش عمل من أعمال التحقيق ولا يجوز الالتجاء إليه إلا بناء على اتهام موجه إلى شخص يقيم في المسكن المراد تفتيشه بارتكاب جريمة أو باشتراكه في ارتكابها أو إذا وجدت قرائن تدل على أنه حائز لأشياء تتعلق بالجريمة ».

54 نقض 17 /1959/11 – مجموعه أحكام محكمه النقض المصرية – ص-10 ص888 .

55 نقض 31/مارس / 1959 – مجموعه أحكام محكمه النقض المصرية – س10 رقم 87 –ص 319 . نقض 17/ديسمبر / -1962 مجموعه أحكام محكمة النقض المصرية – س13 – رقم 205 – ص 853.

56 Prude(J):conclusion du collogue sues l,informatique et droid pe,nal, pares, cujas. 1983.p.155.

57 د.هشام رستم – المرجع السابق – ص 64 وما بعدها.

أوعية أو وسائط كالأشرطة الممغنطة والإسطوانات والأقراص، وبالتالي تكون تلك المكونات المعنوية صالحة للضبط والتفتيش شأنها في ذلك شأن الوسائط المادية وما في حكمها.

وفي نفس هذا الاتجاه نجد أن المادة (251) من قانون الإجراءات الجنائية اليوناني، والتي تعطي السلطات إمكانية القيام بأي إجراء بغية الحصول على الدليل، فالتفتيش بحد ذاته ليس بدليل ولكنه وسيلة للحصول على الدليل حيث منحت المادة (251) سلطات التحقيق إمكانية القيام بأي شيء يكون ضروريا لجمع الدليل وحمايته، ويفسر الفقه اليوناني عبارة «أي شيء» بأنها تشمل البيانات المخزنة أو المعالجة إلكترونياً، وبالتالي فإن ضبط المعطيات الإلكترونية بمختلف صورها المخزنة في الذاكرة الداخلية للحاسوب لا تثير أي خلاف في اليونان، وهناك يطلب المحقق من الخبير أن يقوم بجمع أدلة مقبولة دليلا في المحاكمة الجزائية، كما أن قانون أصول المحاكمات الجزائية الأردني أباح لسلطة التحقيق وفقا للمادة (87) منه بأن تقوم بضبط «جميع الأشياء التي تراها ضرورية لإظهار الحقيقة»، ويفسر الفقه الأردني عبارة «الأشياء» بأنه يمتد ليشمل الكيانات المعنوية للحاسب الآلي.

أما الاتجاه الآخر فيرى أن المفهوم المادي لا يصلح كي ينطبق على هذه المكونات المعنوية والتي لا تصلح بطبيعتها لأن تكون كذلك، على اعتبار أن التفتيش يهدف في المقام الأول إلى تفتيش وضبط الأدلة المادية، وحسب هذا الاتجاه تستلزم وجود أحكام خاصة تكون أكثر شمولية وملاءمة لهذه المعلومات والبيانات الالكترونية .[58]

ونرى أن الاتجاه الأول أكثر منطقية؛ ذلك أن البيانات والمعلومات المخزنة في الحاسوب ومكوناته تصلح لأن تكون محلاً للضبط والتفتيش، حيث يمكن ضبطها واستنساخها على الورق أو على الأقراص، أو على إسطوانات أو على أي دعامة أخرى، كالفلاش ميم وري (Flash Memory)، بحيث يمكن الاستناد إليها كدليل على ارتكاب المتهم الجريمة في مرحلة المحاكمة، لذلك ينبغي الإشارة في قوانين الإجراءات الجنائية على إمكانية تفتيش المكونات المادية والمعنوية لأجهزة الحاسوب ومكوناته.

وباستقراء موقف التشريعات الحديثة نجدها قد ذهبت إلى تأكيد هذا الاتجاه، بحيث أوضحت أن المكونات المعنوية للحاسوب ضمن الأشياء التي تصلح أن تكون محلاً لتفتيش والضبط، ففي التشريع الأمريكي على سبيل المثال: تقضي المادة (34) من القواعد الفيدرالية الخاصة بالإجراءات الجنائية لسنه 1970م بعد تعديلها بمد نطاق التفتيش ليشمل أجهزة الحاسب الآلي وأوعية التخزين والبريد الإلكتروني والصوتي والمنقول عن طريق الفاكس، فضلاً عن أن الاتفاقية الأوروبية للجريمة الافتراضية (اتفاقية بودابست) تقضي في المادة (19) منها بإلزام الدول الأطراف في هذه الاتفاقية بضرورة تبني التدابير والإجراءات التشريعية التي تخول السلطات المختصة ولوج البيئة الإلكترونية، وذلك من أجل تيسير إثبات هذه الجرائم.

وهذا أيضا ما أكد عليه قانون الإجراءات الجنائية الكندي، والذي يجيز ضبط الأشياء ذات الطبيعة المادية، وضبط المكونات المعنوية من المعطيات المخزنة في الأقراص والدعامات المادية، فضبط الأشياء المخزنة في الحاسب الآلي يشمل ضبط كياناته المادية والمعنوية، كما نص قانون الإثبات الكندي code of Evidence على أنه: «ما لم يرد ما يخالف ذلك في أمر التفتيش وضبط الدفاتر والسجلات الخاصة بمؤسسة مالية يقتصر على تفتيش المكان بغرض تفقده وأخذ نسخ من مواد المكتوبة، وينطبق هذا النص سواء كانت سجلات مكتوبة أم كانت على شكل إلكتروني، أما إذا كان التفتيش في مكان غير تابع لمؤسسة مالية، فإن أخذ السجلات الأصلية أو الحصول على نسخ منها فحسب، أمر يخضع بشكل عام للسلطة التقديرية للشرطة، مع ضرورة العمل على تطوير النصوص القانونية التقليدية المتعلقة بالتفتيش والضبط في الجرائم الإلكترونية، لتشمل البيانات والمعلومات الإلكترونية، فيجب أن يدخل في نطاق التفتيش والضبط، التفتيش عن المكونات المعنوية للحاسب الآلي، كالبيانات الإلكترونية والمراسلات والاتصالات الإلكترونية، وإلا أدى ذلك إلى إيجاد العديد من الصعوبات أمام جهات التحقيق فيما يتعلق بجمع الأدلة التي تفيد في كشف الحقيقة في الجريمة الإلكترونية، وقد يؤدي عدم اعتبار المكونات المعنوية للحاسب الآلي من الأشياء التي تخضع لتفتي إلى عدم قيام الجريمة الإلكترونية وذلك متى كانت هذه المكونات المعنوية هي السبيل الوحيد للوصول إلى حقيقة الجريمة الإلكترونية.

3-2 الشروط المتطلبة لصحة التفتيش الإلكتروني

الأصل أن يستهدف التفتيش في الجريمة الإلكترونية ضبط كل شيء يفيد في كشف الحقيقة، فإن لم يكن للتفتيش غاية يستهدفها، فالتفتيش باطل، ولكي يكون التفتيش صحيحا يجب أن يتوافر فيه عدة شروط، منها شروط موضوعيه، وشروط شكليه، وهي على البيان التالي:-

3-2-1 الشروط الموضوعية للتفتيش الإلكتروني

الأصل في القانون أن الإذن بالتفتيش هو إجراء من إجراءات التحقيق لا يجوز إصداره إلا بعد وقوع جناية أو جنحة وترجحت نسبتها إلى متهم معين، وتوافر إلى جانب ذلك أمارات قوية أو قرائن على وجود أشياء تفيد في كشف الحقيقة لدى المتهم أو غيره، وهو ما أقرته محكمة النقض المصرية في عدة أحكام لها، بحيث لخصت الشروط الموضوعية المتطلبة لصحة التفتيش، حيث ذكرت في أحد إحكامها: «من المقرر أن كل ما يشترط لصحة التفتيش الذي تجريه النيابة أو تأذن في إجرائه في مسكن المتهم، أو ما يتصل بشخصه، هو أن يكون رجل الضبط القضائي قد علم من تحرياته واستدلالاته أن جريمة معينة – جناية أو جنحة قد وقعت من شخص معين وأن تكون هنالك من الدلائل والأمارات الكافية أو الشبهات المقبولة ضد هذا الشخص بقدر يبرر تعرض التحقيق لحريته أو حرمة مسكنه في سبيل كشف مبلغ اتصاله بتلك الجريمة»،[59] وبناء على ما سبق وتطبيقاً على الجرائم الإلكترونية فإنه لا بد ليكون التفتيش مشروعاً توافر عدة شروط كما يلي:

- **وقوع الجريمة المعلوماتية**:حيث عرفت بأنها أي فعل يرتكب متضمناً استخدام الحاسب الآلي أو الشبكة الإلكترونية،[60] وعرفت بأنها: أي سلوك غير مشروع يرتبط بإساءة استخدام الحاسب الآلي ويؤدي إلى تحقيق أغراض غير مشروعة، والإذن بالتفتيش جائز إذا كانت الجريمة جناية أو جنحة، أما المخالفات فالتفتيش فيها غير جائز؛ لأنها قليلة الأهمية والخطورة، وبالتالي لا تستحق التعرض لحريات الأشخاص أو انتهاك خصوصياتهم وهذا ما أكد عليه المشرع الفلسطيني حين نص في الفقرة 1 من المادة 39 «بارتكاب جناية أو جنحة أو باشتراكه في ارتكابها»، فهو لا يتم إلا بشأن جريمة تحقق وقوعها فعلاً؛ كون التحقيق لا يبدأ إلا بعد أن يكون هنالك جريمة قد وقعت، وعليه فالتفتيش كإجراء من إجراءات التحقيق غير جائز إلا بعد وقوع جريمة، فهو غير جائز بالنسبة لجريمة مستقبلية أو محتملة الوقوع.[61]
- **وجود دلائل ضد شخص معين**: فلابد من اتهام شخص أو أشخاص معينين بارتكاب هذه الجريمة أو المشاركة في ارتكابها، بحيث ينبغي أن تتوافر وتتحقق في حق الشخص المراد تفتيشه أمارات قوية أو قرائن على وجود أجهزة إلكترونية أو أي أدلة تفيد في كشف الحقيقة ونسبته إلى المتهم، وبالتالي أدانته، وفي جريمة الاختلاس الإلكتروني يجب أن تتوافر في حق الشخص المطلوب تفتيشه أو تفتيش مسكنه أو حاسبه الآلي دلائل كافية تؤدي إلى الاعتقاد بأنه قد أسهم في ارتكاب جريمة الاختلاس الإلكتروني بصفته فاعلاً أو شريكاً في هذه الجريمة، وهو ما أكد عليه قانون الجرائم الإلكترونية الأردني رقم 27 لسنة 2015م في المادة 13 /أ. فيجب عدم إجراء التفتيش إلا إذا توافرت للمحقق دلائل كافية على أنه يوجد في مكان أو لدى الشخص المراد تفتيشه أدوات استخدمت في ارتكاب الجريمة، أو أشياء متحصله منها أو أي مستندات أو محررات إلكترونية يحتمل أن يكون لها فائدة في استجلاء الحقيقة لدى الشخص المتهم بارتكاب الجريمة، والدلائل تعني علامات معينة تستند إلى العقل

58 د.هشام محمد فريد رستم، جرائم الحاسوب كصورة من صور الجرائم الاقتصادية المستحدثة، مجلة الدراسات القانونية، جامعة أسيوط العدد 17، 1995م، ص64 وما يليها.
59 نقض رقم 1970/1/12 مجموعه القواعد القانونية – س 39 – رقم 1592 – ص 65 .
60 نظام مكافحة جرائم المعلوماتية السعودي- قرار مجلس الوزراء رقم 79 بتاريخ 3/7/ 1428 .
61 نقض 1962/1/1 أحكام محكمة النقض المصرية – س13 – ق5 – ص20 .

وتبدأ من ظروف أو وقائع يستنتج منها بأن جريمة ما قد وقعت، وأن شخصاً معيناً هو مرتكبها، ومن ثم هي مجرد افتراضات قد لا تصلح وحدها سبباً للإدانة، أو هي ذلك القدر الضئيل المبني على احتمال معقول تؤديه الظروف والاستنتاجات التي تكفي للاعتقاد بارتكاب جريمة وتبرر اتخاذ بعض الإجراءات الماسة بالحرية الفردية ضماناً لحسن سير العدالة،[62] وفي جريمة الاختلاس الإلكتروني لابد أن يصدر الإذن بالتفتيش لضبط وقوعها بحيث تتوافر مجموعة من الأمارات والمظاهر التي تكفي وفقاً للسياق العقلي والمنطقي ترجيح ارتكابها ونسبتها إلى المتهم وإلى من ساهم في ارتكاب الجريمة سواء بوصفه فاعلاً أو شريكاً فيها، وإلا وقع التفتيش باطلاً ،ويمكن الاسترشاد بذلك بالرجوع إلى نص المادة18/ 39 من قانون الإجراءات الجزائية الفلسطيني، وكذلك ما نصت عليه المادة 44 من ذات القانون، لذا فالمشرع اشترط لصحة التفتيش توافر قرائن قوية على أن الشخص هو مرتكب الجريمة، وقد اشترطت كافة التشريعات الجزائية العربية في أن التفتيش يجب أن يهدف إلى كشف الحقيقة سواء تعلق الأمر بإثبات التهمة أو نفيها، وإذا ما كان الهدف غير ذلك كالإساءة إلى المشتكى عليه أو تحقيق غايات أخرى كان التفتيش باطلاً مشوباً بالتعسف باستعمال السلطة.[63]

- **محل التفتيش**: والمقصود به: هو الشيء الذي يقع عليه التفتيش، وهو هنا جهاز الحاسوب بكل مكوناته المادية والمعنوية وشبكات الاتصال الخاص به، يضاف إلى ذلك الأشخاص الذين يستخدمون الحاسوب محل التفتيش، وتشمل كذلك الأماكن التي توجد بها تلك الأشياء، وتشمل المكونات المادية للحاسوب وحدة الإدخال، وهي الذاكرة الرئيسة (Main Memort)، ووحدة الحساب والمنطق (Arithmetic)، ووحدة الإخراج (Output unit)، ووحدة التخزين الثانوية (Seconndary Storage Unit).

أما المكونات المعنوية للحاسوب، وتشمل الكيانات الأساسية أو برامج التطبيقات سابقة التجهيز وبرامج التطبيقات المستخدمة من قبل مستخدم الحاسوب، كما ويشمل الحاسوب بمكوناته السابقة مجموعة من الأشخاص لديهم خبرة ومهارة في تقنية نظم المعلومات وهم مشغلو الحاسوب، ومبرمجو الحاسوب والذين قد يكونون من المحللين أو مهندسي الصيانة والاتصالات، أو من أي أشخاص آخرين يكون بحوزتهم أجهزة أو معدات إلكترونية أو أجهزة الحاسوب المحمول، هذا ما يتعلق بمحل التفتيش المتعلق بالحاسوب والمكونات والأشخاص، يضاف إلى ذلك المنازل أو ما في حكمها، ويقصد بها كافة محال الإقامة والملحقات المخصصة لمنافعها والتي يشغلها الشخص سواء بصفة دائمة أو مؤقتة وسواء كانت ثابتة أم متنقلة، متى ما وجدت فيها مكونات الحاسوب أصبحت محلاً للتفتيش، بحيث تخضع عملية التفتيش هنا لذات الشروط والقواعد والإجراءات التي يخضع لها تفتيش المساكن،[64] وهنالك الأماكن العامة التي يمكن تفتيشها دون الحاجة إلى مذكرة التفتيش، حيث لا يعد من الخصوصية بشيء تفتيش الوثائق المخزنة على أجهزة الكمبيوتر المتاحة لاستخدام العام في المكتبة العامة، كما أن رضا المشتكى عليه يمنح صلاحية التفتيش بدون مذكرة تفتيش إذا يصح التفتيش من خلال الرضا الصادر من الأم في تفتيش غرفه ابنها وما تحتويه من أجهزة إلكترونية، كما رأت المحكمة الأمريكية أن موافقة زوجة المدعى عليه يمكن أن يعتد بها على نحو صحيح في تفتيش جهاز الكمبيوتر الخاص بزوجها المحمي بكلمة مرور زوجها.[65]
- **صدور أمر التفتيش من هيئه قضائية مختصة**: يختص بإصدار أمر التفتيش كل من النيابة العامة، أو قاضي التحقيق، أو محكمه الموضوع باعتباره إجراء من إجراءات التحقيق، ليكون أمر التفتيش صحيحا ونافذا يجب أن يصدر من الجهات سابقة الذكر، حتى لا يكون عيب مادي في الإذن فينقض ما يترتب عليه لاحقا، فالتفتيش إجراء قانوني من إجراءات التحقيق الابتدائي من شأنه المساس بأسرار الشخص الذي تم تفتيشه، لذلك فإنه يخضع للقواعد العامة التي تخضع لها أعمال التحقيق كافة، لذا حدد المشرع الجهة التي تصدر أمر التفتيش ومن يقوم بتنفيذ هذا الأمر، بحيث لا يباشر إلا من قبل الجهة المختصة به، وهي حسب التشريع الفلسطيني النائب العام أو عضو النيابة المختص، كما يختص مأمور الضابطة القضائية بالتفتيش، واستثناء من ذلك فقد منحت المادة 21 من قانون الإجراءات الجزائية الفلسطيني مأموري الضبط القضائي مباشرة التفتيش في الحالات المنصوص عليها في تلك المادة، وهما: حالة التلبس بالجريمة والإنابة، وفى التشريع الأردني فإن الأصل في ممارسة التفتيش أن يتم من قبل المدعي العام، حيث يخول المشرع الأردني موظفي الضابطة العدلية إجراء التفتيش في أحوال استثنائية حددها على سبيل الحصر كالجرم المشهود، والقبض، والدلائل الكافية، والندب، وعليه فإن الاختصاص بإجراء التفتيش أما أن يكون أصلياً لسلطة التحقيق أو استثنائيا لمأمور الضبط القضائي، وهذا ما أكد عليه قانون أصول المحاكمات الجزائية الأردني في الجرائم التقليدية، أما الجرائم الإلكترونية فقد أوضحت السلطة المختصة بالتفتيش وذلك من خلال قانون رقم 27 لسنة م2015 من قانون الجرائم الإلكترونية حيث نص في المادة 13/أ " ... يجوز لموظفي الضابطة العدلية بعد الحصول على إذن من المدعي العام المختص أو من المحكمة المختصة الدخول إلى أي مكان تشير الدلائل إلى استخدامه لارتكاب أي من الجرائم المنصوص عليها في هذا القانون كما يجوز لهم تفتيش الأجهزة والأدوات والبرامج وأنظمة التشغيل ... "كما يخول القانون المصري الاختصاص بالتفتيش كإجراء تحقيق للنيابة العامة بصفة أصلية ولقاضي التحقيق في حالات خاصة،[66] مع ضرورة العلم أن التفتيش في الجرائم التقليدية يختلف عن التفتيش في الجرائم الإلكترونية، إذ يجوز لهم تفتيش الأجهزة والأدوات والبرامج وأنظمة التشغيل والشبكة المعلوماتية والوسائل التي تشير الدلائل في استخدامها لارتكاب أي من تلك الجرائم، وفي جميع الأحوال على الموظف الذي قام بالتفتيش أن ينظم محضراً بذلك ويقدمه إلى المدعي العام المختص، ومما سبق يتضح أن عمل رجال الضابطة القضائية هو إكمال دور النيابة العامة وتقديم المساعدة بغية الوصول إلى الأدلة المادية للجريمة كون التفتيش وسيلة تهدف إلى الوصول إلى كل ما يثبت قيام الجريمة وضبط الأدلة وإظهار الحقيقة من على مسرح الجريمة، والذي يعد الميدان الرئيس للجريمة، وهو أجهزة الحاسوب ومكوناته ومعطياته الموجودة في المكان أو توابعه أو المكتب إلى يوجد بها الحاسوب والأقراص التي تحتوي على معطيات الحاسوب، أو على الشخص المتهم، فقد يقع التفتيش على الفرد الذي يحمل الحاسوب أو القرص أو الإسطوانة أو أي جهاز أخر قد يتعلق بموضوع الجريمة.

3-2-2 الشروط الشكلية للتفتيش الإلكتروني

إلي جانب الشروط الموضوعية التي سبق وتناولتها، توجد هنالك شروط ذات طابع شكلي، ضرورية لا بد من الأخذ بها عند القيام بالتفتيش؛ حرصاً على الحريات الفردية من التعسف وانتهاك الحقوق، بحيث تزرع في نفس المتهم الطمأنينة وتنزع عن التفتيش أي لبس أو غموض لدى المحكمة ونستعرض هذه الشروط على النحو التالي:-

تسبيب إذن التفتيش:

يعد تسبيب الأمر بالتفتيش من الضمانات المقررة في قوانين الإجراءات الجزائية، بحيث يشتمل أمر التفتيش على بيان العناصر الأساسية التي تمكن المحقق من القيام بالتفتيش والتحقق من توافر الدلائل الكافية والمشتملة على ما يبرر القيام بالتفتيش والتي تدل على أن في المكان

62 د . مجدي محمود محب – إذن التفتيش –دراسة تحليلية تطبيقية في التشريع المصري والتشريعات العربية المقارن في ضوء الفقه والقضاء في 100 عام – سنة 2004 – دار محمود للطباعة والنشر– ص77 .

63 نقض 20 ديسمبر سنة 1937 مجموعه القواعد القانونية – ج 4 رقم 131 – ص121 .

64 د. صالح البريري– دور الشرطة في مكافحة جرائم الإنترنت – مؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية – دبي 2003 – ص392.

65 States v. Buckner, 407 f. Supp. 2d 777 (W,D Va. 2006), the Court held that.

66 د. الدكتور فاروق الكيلاني – محاضرات في قانون أصول المحاكمات الجزائية الأردني المقارن – ط1 – دار الثقافة للنشر والتوزيع – سنة 1995م. ص 251.

أو الشخص المراد تفتيشه ما يفيد في كشف حقيقة الجريمة التي صدر إذن التفتيش بناءً على وقوعها، بحيث تدل الظواهر والمظاهر على أن إجراء التفتيش سوف يكشف عن الحقيقة بحيث تستطيع المحكمة التأكد من جدية مبررة التفتيش، وقد نص القانون الأساسي الفلسطيني في المادة 17 «للمساكن حرمة فلا تجوز مراقبتها أو دخولها أو تفتيشها إلا بأمر قضائي مسبّب ووفقاً لأحكام القانون»، كما ونصت المادة 39 فقرة 2 من قانون الإجراءات الجزائية الفلسطيني على وجوب أن تكون مذكرة التفتيش مسببة، مبيناً أمر التفتيش الأسباب التي أدت بالنيابة العامة إلى إجراء هذا التفتيش، وهذا ما أوضحته الفقرة أ من المادة 13 من قانون الجرائم الإلكترونية الأردني،[67] هذا ويجب أن يكون الأمر بالتفتيش مكتوباً حتى يكتسب القوه القانونية، حيث إن الأوامر الشفهية لا تكتسب الصفة القانونية، ويجب أن تكون مؤرخة حتى يمكن التأكيد أن الإجراء قد تم خلال المدة المصرح بها في القانون، ويتعين أن يكون أمر التفتيش موقعا حتى يمكن التأكيد على أنه صادر من الموظف المختص ويتضمن كذلك اسم المتهم المنسوب إليه، وهذا ما أكدت عليه المادة 40 من القانون السابق، ويلتزم القائم بتحرير إذن التفتيش أن يأخذ بالحسبان التحقق من تسبيب الإذن بحيث يكون مبني على دلائل قوية وقرائن تدل على أنه حائز لأشياء تتعلق بالجريمة، وتحريات سليمة دقيقة تفيد في كشف الحقيقة، بحيث تبعث الطمأنينة لدى مصدر الأمر بوقوع الجريمة ونوعها –جناية أو جنحة – والتحقق أيضا من جدية الاتهام الموجهة إلى شخص المتهم الذي يقيم في المسكن المراد تفتيشه بارتكاب الجريمة أو باشتراكه في ارتكابها، ويضاف إلى ذلك إعداد محضر بالواقعة يتضمن الأسباب التي بني عليها أمر التفتيش وما تم أثناء إجراءات التفتيش.

وفى مجال الجرائم الإلكترونية نرى ضرورة العمل على صياغة مذكرات التفتيش من قبل الجهات المختصة على وجه الدقة مما يسهل عملية التفتيش والبحث من جهة، وفي نفس الوقت يجب العمل على صيانة الحقوق حتى لا يكون هنالك تجاوز لعملية التفتيش والتعرض لأجهزة الكمبيوتر أو الشبكات الإلكترونية مما يسبب الكثير من الأضرار من جهة أخرى، مما يوصلنا إلى ضرورة صياغة مذكرات التفتيش بما يتلاءم وحماية الخصوصية التي نصت عليها معظم دساتير العالم، فقد يكون إذن التفتيش بخصوص معلومات معينة لكن قد يكون تفتيش نفس الحاسوب فيه الكثير من المعلومات التي تمس العديد من المناطق المختلفة من حياة الشخص، لذا فلا بد من الدقة في التفتيش وفي صياغة أمر التفتيش بحيث يكون واضح ومحدد، فمن حق الإنسان أن يكون آمناً في شخصه ومنزله من أورق وآثار ضد التفتيش والاحتجاز غير المعقول، وعليه فلا يجوز التعدي، ولا يجوز إصدار مذكرة التفتيش إلا في حال سبب معقول معزز التوكيد على وقوع الجريمة بحيث يصف المكان المراد تفتيشه والأشخاص والأشياء المراد تفتيشها واحتجازها،[68] مع ضرورة حضور المتهم عند تفتيش حاسبه الآلي إن كان الأمر متعلقاً بضبط دليل ضده؛ وذلك لإتاحة الفرصة أمام المتهم لمواجهته بالدليل المتحصل من التفتيش، شريطة ألا يسبب حضوره إضراراً بسير التحقيق.

تكوين فريق التفتيش

الجريمة الإلكترونية بحاجة إلى فريق من المختصين والفنيين في مجال الحاسوب والأنظمة الإلكترونية للقيام بالانتقال إلى مسرح الجريمة بصورة سريعة؛ حتى يتمكنوا من الحفاظ على مكان الجريمة والمحافظة على الأدلة من النسخ أو الإتلاف أو الشطب أو التعديل، بالإضافة إلى رجال الشرطة المختصين بالحماية والأمن؛ من أجل ضبط الجريمة الإلكترونية، مع مراعاة إبعاد المشتبه فيهم والعاملين على أجهزة الحاسوب عن المكان، ومن ثم يتم تفتيش جميع الأجهزة ومعرفة المعطيات؛ ذلك لسرعة قيامها وسرعه تغير وإخفاء معطيات الحاسوب، وبالتالي ضياع الأدلة واختفاء الجريمة، وإتلاف المعلومات المخزنة أو محوها،[69] وهذا ما أكدت عليه الفقرة أ من المادة 13 من قانون رقم 27 لسنة 2015م من قانون الجرائم الإلكترونية الأردني والتي نصت على أنه: «مع مراعاة الشروط والأحكام المقررة في التشريعات النافذة ومراعاة حقوق المشتكى عليه الشخصية، يجوز لموظفي الضابطة العدلية بعد الحصول على إذن المدعي العام المختص أو من المحكمة المختصة الدخول إلى أي مكان تشير الدلائل إلى استخدامه لارتكاب أي من الجرائم المنصوص عليها في هذا القانون»، كما ألزمت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010م، في المادة 25 الدول الأطراف بتمكين السلطات المختصة من صلاحيات الحصول على أية معلومات مخزنة لدى أي كان أو لدى مزودي الخدمة أو تحت سيطرتهم، بينما تلزم المادة (26) من نفس الاتفاقية بتمكين تلك السلطات من تفتيش المعلومات المخزنة.

ونرى ضرورة وضع استراتيجية البحث في الجرائم الإلكترونية بحيث ينبغي على المحققين في مجال الجرائم الإلكترونية الوضع في اعتبارهم أن كل العناصر يجب أن تخضع للتحقيق والفحص، فجهاز الكمبيوتر هو مستودع السر ومستودع البيانات التي هي دليل على وجود الجريمة، فيجب قبل ذهاب النيابة العامة إلى المحكمة توضيح مصادر الأدلة الإلكترونية، والتي لها صلة بعناصر الجريمة فقد يستخدم جهاز الكمبيوتر كأداة في اختراق المواقع وتوزيع الحقوق والنسخ والإتلاف فمن خلال القرص الصلب بجهاز الكمبيوتر يمكن استكشاف العديد من أنواع الأدلة المختلفة،[70] وفي الغالب يكون ميدان الجريمة الإلكترونية مثل باقي مسارح الجرائم الأخرى عندما يكون الهدف منها الاعتداء على المعلومات والبيانات الإلكترونية، بحيث يكون التحرك إلى مسرح الجريمة بقصد المداهمة والتفتيش عن أدلة الجريمة وضبطها على حالتها الطبيعية مع إمكانية الاستعانة باعترافات المتهمين وشهادات الشهود والقرائن، إلا أن هنالك ضوابط لا بد من مراعاتها عند الانتقال إلى مسرح الجريمة، إذ لا بد من توافر معلومات كافية عن المكان الذي تمت فيه الجريمة وعدد الأجهزة المتوقع مشاركتها في الجريمة وأنواعها ومواقعها وموقع ملحقاته من خزائن ومعطيات تابعه للأجهزة المشتركة في الجريمة، أما فيما يتعلق بالموارد البشرية من رجال النيابة العامة والضابطة القضائية فالأصل في مثل هذه الجرائم لا بد من إعداد فريق من المتخصصين في مجال الجرائم الإلكترونية بغيه البحث والتحري والتفتيش وضبط الأدلة في مثل هذه الجرائم بحيث تحدد المهام المطلوبة من كل فرد فيهم على أن يكونوا من ذوي الخبرة في مجال التحقيق الجنائي في مثل هذه الجرائم.

3-3 ضبط أدلة الجريمة الإلكترونية وإجراءاته

الغاية من التفتيش هي ضبط الأشياء، ويقصد به وضع اليد على شيء يتصل بجريمة وقعت يفيد في كشف الحقيقة عنها وعن مرتكبها وهو من حيث طبيعته القانونية من إجراءات التحقيق، ويلزم في الضبط أن يكون قد تم اتخاذه لغاية محددة، وهي الكشف عن أشياء تتعلق بالجريمة الإلكترونية أو تفيد في إظهار الحقيقة ومراعاة إبعاد المشتبه فيهم عن مسرح الجريمة – مكان الأجهزة التي أسهمت في أحداث الجريمة.

بحيث يتم تفتيش جميع الأجهزة الإلكترونية ذات العلاقة بالجريمة ومعرفة المكونات والمعطيات المخزنة فيه، والتي تفيد في كشف كيفية وقوع الجريمة من خلال معرفة رقم الاتصال أو ما تم من نقل أو نسخ أو إتلاف للمعلومات والبيانات، ويمكن بالتالي وضع معيار يحدد الأشياء التي يجوز ضبطها بأنها: «جميع الأشياء – أيا كانت طبيعتها – التي يقدر المحقق أنها تفيد في كشف الحقيقة»، فالمعيار هو الصلة أو الرابط بين الشيء والجريمة، ويجب على المحقق أن يستخلص منة دليل إدانة أو براءة.[71]

---

67 حيث نصت ف أ/13 « مع مراعاة الشروط والأحكام المقررة في التشريعات النافذة ومراعاة حقوق المشتكي عليه الشخصية يجوز لموظفي الضابطة العدلية بعد الحصول على إذن المدعي العام المختص أو من الحكمة المختصة الدخول إلى أي مكان تشير الدلائل إلى استخدامه لارتكاب أي من الجرائم المنصوص عليها في هذا القانون، كما يجوز لهم تفتيش الأجهزة والأدوات والبرامج وأنظمة التشغيل والشبكة المعلوماتية والوسائل التي تشير الدلائل في استخدامها لارتكاب أي من تلك الجرائم وفي جميع الأحوال على الموظف الذي قام بالتفتيش أن ينظم محضراً بذلك ويقدمه إلى المدعي العام المختص».

68 Similarly, the Tenth Circuit has refused to allow such exhaustive searches of a computer, s hard drive in the absence of awarrant or some exception to the warrant requirement. see United States v Carey, 172 f.3d 1268,127310)75-th CIR.1999).

69 see United States v. Ortiz, 84 F.3D 977,984 (7th Cir. 1996 (in conducting search incident to arrest, agents were justified in retrieving numbers from pager because pager information is easily destroyed).

70 Electronic Theft Unlawful Acquisition in Cyberspace. AUTHORS: PeterGrabosky, Australian Institute of Criminology, Canberra. Russell G. Smith, Australian Institute of Criminology, Canberra. Gillian Dempsey, University of Queensland/DATE PUBLISHED: July 2010.

71 مراجعة المادة 91 من قانون الإجراءات الجنائية المصري.

ويتطلب حسن تنفيذ هذا التفتيش، أن يجري من قبل فريق من الفنيين والمتخصصين في مجال الإلكترونيات ولهم علم واسع بالحاسوب والشبكات والأنظمة الإلكترونية، وبالإضافة إلى رجال الضابطة القضائية المختصين بالحماية والأمن، والضبط في الجريمة الإلكترونية يشمل جهاز الحاسوب بأنواعه وملحقاته، مثل: والنوت بوك، واللاب توب، ولوحة المفاتيح، والشاشة، والشرائط الممغنطة، والمودم (Modem)،[72] والطابعات، وملفات الكمبيوتر والاتصالات والسجلات وبيانات الشبكة، وضبط المراسلات والبريد الإلكتروني، وما يتصل منها بضبط المكونات المادية لأنظمة الحاسوب، وكذلك المكونات المعنوية والبرمجيات وكل المعطيات التي تتناقل أو يجري تبادلها عبره شبكة المعلومات التي تربط أجهزة الحاسوب معاً، فكل ذلك يعد أثرا أو جزءا من جسم الجريمة، بحيث ينبغي البحث عنها وفحصها والتحري عنها من اجل الاستفادة منها في عملية التفتيش، علماً أن التعامل مع تلك المعطيات في البحث والتفتيش يحتاج إلى خبرة فنية متخصصة في مجال الحاسوب والشبكة الإلكترونية ومعرفة بالقانون وقواعد البيئة الإلكترونية التي يجب على النيابة العامة الأخذ بها والاستعانة بهم، كونها صاحبة الصلاحية في ذلك، وقد أوجبت المادة 487 من القانون الكندي ضبط كل ما تتوافر بشأنه مبررات معقولة تدعو للاعتقاد بأن جريمة قد وقعت أو يشتبه في وقوعها، أو أن هنالك نية لاستخدامه في ارتكاب جريمة ذات طابع إلكتروني.[73]

طبيعة الضبط ترد وبحسب التنظيم القانوني على الأشياء دون الأشخاص، فهم لا يصلحون محلاً للضبط بالمعنى الدقيق، وإن كانت هنالك بعض القوانين قد اتجهت على إمكانية اشتمال الضبط على الأشخاص، إن كان مفهوم ذلك القبض عليهم وإحضارهم، ويظهر واضحاً الفرق بين القبض على الأشخاص وضبط الأشياء.[74]

ومحل الضبط في مجال الجرائم الإلكترونية هو البيانات والمعلومات المعالجة إلكترونياً، كما ألزمت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010م، في المادة (27) بنصوص معنونة بضبط المعلومات المخزنة، كما وألزمت المادة (28) بالجمع الفوري لمعلومات تتبع المستخدمين، وعلى الرغم من النقاش الذي دار حول إمكانية إخضاع وصحة تلك البيانات والمعلومات للضبط ومدى اعتبار المكونات المعنوية مساوية للمكونات المادية وحتى لا يكون هنالك تكرار نحيل الدارس إلى المطلب الثاني في المبحث الأول منعاً للتكرار، إذ أن الاتجاه السليم يعتبر أن تلك البيانات ما هي إلا ذبذبات إلكترونية تقبل التسجيل والحفظ والنسخ والتخزين على وسائط وداعمات مادية مما لا يمكن إنكار وجودها المادي، وهنالك رأي يؤكد صحة ضبط المكونات المعنوية والمادية، وهذا ما أكده قانون الإجراءات اليوناني في المادة 251 والقانون الجنائي الكندي، والذي أجاز ضبط الأشياء ذات الطبيعة المادية وضبط المكونات المعنوية كونها من المعطيات المخزنة في الأقراص والدعامات المادية.[75]

نتفق ونرى ونؤكد على ضرورة تطوير النصوص القانونية التقليدية المتعلقة بالتفتيش والضبط في الجرائم الإلكترونية لتشمل البيانات الإلكترونية والمعلومات، فيجب أن يدخل في نطاق التفتيش والضبط، التفتيش عن المكونات المعنوية للحاسب الآلي، كالبيانات والمعلومات الإلكترونية والمراسلات والاتصالات الإلكترونية، وإلا أدى ذلك إلى إيجاد العديد من الصعوبات أمام الجهات المختصة بالتحقيق فيما يتعلق **بجمع** الأدلة والإثبات التي تفيد في كشف الحقيقة في الجريمة الإلكترونية، وقد يؤدي عدم اعتبار المكونات المعنوية للحاسب الآلي من الأشياء التي تخضع للتفتيش إلى عدم قيام الجريمة الإلكترونية وذلك متى كانت هذه المكونات المعنوية هي السبيل الوحيد للوصول إلى حقيقة الجريمة المعلوماتية.

فالضبط لا بد أن يفيد في كشف الحقيقة، ولتمام ذلك تصدر النيابة العامة الإذن الخاص بالتفتيش والذي يجيز تفتيش الجهاز أو الأجهزة المشتركة في الجريمة وكافة معطيات ومكونات الحاسوب، على أن يكون الإذن على ما سبق الذكر محدد على وجه الدقة والوضوح من حيث مكان التفتيش (مسرح الجريمة) عنوان الشخص وصفته والأشياء التي يتم البحث والتحري عنها، وإثبات جميع الإجراءات التي اتخذت أثناء التفتيش والإجراءات المتخذة بالنسبة للأشياء المضبوطة.

يذكر أن التفتيش في الجرائم الإلكترونية يتناول الدخول إلى جهاز الكمبيوتر وضبط ما يحتويه من بيانات ومعلومات تفيد في الوصول إلى خيوط الجريمة، ومن خلال تلك الإجراءات يتم الضبط بحيث يتم إدخال المعلومات والبيانات الإلكترونية المضبوطة والأدلة المتحصلة من عملية الضبط ويتم تصنيفها وتحريزها في المغلفات والصناديق المعدة لذلك ويتم تميزها من خلال وضع علامات عليها، ثم تبدأ عملية فحص الأدلة التي تم العثور عليها ومحاولة تجربتها من خلال أجهزة أخرى حتى لا يتم المساس بالدليل الأصلي من قبل الفنيين المختصين بمثل هذا النوع من الجرائم، ويتم توثيق جميع تلك الإجراءات في محضر التحقيق بالتاريخ واليوم الذي تم فيه بحيث يشتمل على كافة المعلومات والإجراءات التي تمت في سبيل كشف ملابسة هذه الجريمة.

4-0 الخاتمة

وفي النهاية يبدو ضرورياً جلياً أن خصوصية جرائم المعلومات والبيانات وما يلحقه من اعتداء يستوجب وجود تشريعات خاصة تحكمها نظرا لتسارع تطورها؛ لأن الأحكام العامة المنصوص عليها في قوانين العقوبات، قد لا تستطيع أن تفي بالغرض، وبهذا النوع المتجدد من الجرائم، مما يرتب إفلات كثير من المجرمين من دائرة التجريم، وبالتالي عدم إمكانية معاقبتهم، إضافة إلى ذلك أن في مثل هذه الحالات لا يمكن استخدام القياس والاجتهاد للتجريم عملاً بمبدأ: «لا جريمة ولا عقوبة دون وجود نص»، حيث **كشفت** الاستطلاعات الحديثة أن وسائل الحماية التي توفرها القوانين النافذة لم تكن كافية ولا شاملة ولا فعالة، إذ رغم وجودها فإن حجم جرائم قرصنة المعلومات يتزايد باستمرار، فضلا عن أن هناك كثير من الدول ليست طرفا في الاتفاقيات التي توفر فرصة للتعاون الدولي، ومع هذا فهي بؤرة كبيرة لانطلاق جرائم قرصنة المعلومات.

لقد حاولنا في هذه الدراسة أن نتناول موضوعا حديثا، وهو الاختلاس الإلكتروني ومدى انطباق نصوص السرقة التقليدية على المعلومات والبيانات الإلكترونية، ولم يكن دافعنا في ذلك فقط تحديد مدى تمتع تلك المعلومات من إخاضعة إلى النصوص القانونية التقليدية المطبقة على جريمة الاختلاس، بل أيضا توضيح الطبيعة القانونية لتلك المعلومات والبيانات ذات الطابع الإلكتروني، وقد حاولنا من خلال هذه الدراسة تطبيق القواعد العامة في قانون العقوبات على ما تثيره تلك المعلومات والبيانات من جدال ونقاش من حيث مدى تطبيق تلك النصوص على المكونات المادية والمعنوية، وإكمالا على ذلك فإن التجريم يجب أن يشمل كافة الصور التي يتم فيها نقل المعلومات والبيانات، فيقرر القانون العقوبات المناسبة على تلك الأفعال والتي تؤدي بذاتها أو عن طريق وسائل معينة يستخدمها الجاني للحصول على معلومات أو بيانات أو تغيرها أو حذفها أو إتلافها سواء كانت هذه المعلومات تم حفظها أو تداولها في جهاز أو نظام أو بأي وسيلة كانت، بحيث تشدد العقوبة إذا ما استعملت المعلومات وتلك البيانات التي حصل عليها بطريقة ما للحصول على مال أو منافع وخدمات شخصية.

ونظرا لتعدد الموضوعات التي تندرج ويمكن تناولها تحت عنوان حدود القانون في السيطرة على السرقة الإلكترونية ولم يكن من الممكن أن نتناول كلها، فقد اقتصرنا على دراسة الاختلاس الإلكتروني تحديداً ولم يكن من الممكن أن نتناول هذا الموضوع دون أن نسبق ذلك بمحاولة التعرف على مفهوم جريمة الاختلاس وأركانه، وتناولنا من خلال هذه الدراسة تحديد طبيعة مكونات الكمبيوتر، وجريمة السرقة أو الأخذ التي قد تقع على تلك المكونات المادية (hardware) أو على مكونات الكمبيوتر المعنوية والتي تشمل (software or data bases).

كما تم تسليط الضوء على المخاطر الإجرامية المتعددة التي قد تتعرض لها تلك المكونات في ميدان الجريمة سواء تعلق الأمر بنقل المعلومات أو سرقتها أو حذفها أو إتلاف الكمبيوتر نفسه أو إتلاف البيانات أو البرامج، أو استخدم الكمبيوتر والإنترنت كأداة لذلك، ثم انتقلنا إلى إجراءات

72 هي الوسيلة التي تمكن أجهزة الحاسوب من الاتصال مع بعضها البعض علر خطوط الهاتف، وللمودم أشكال وهياكل تتطور مع تطور تقنية صناعة الالكترونيات .
73 د. على حسن الطولية- التفتيش على نظام الحاسوب والإنترنت -سنة2004 – عالم الكتب الحديثة – إربد – ص36 وما يلها.
74 د. محمد على سالم عياد واخرون -الوسيط – ج2 ص350
75 يونس عرب – جرائم الكمبيوتر والإنترنت -قدم بحث في مؤتمر الامن العربي-2002- ص520.

التفتيش والضبط في الجرائم الإلكترونية، حيث تناولت الدراسة إجراءات التفتيش في البيئة الإلكترونية وبيان الأحكام المقررة في مدى خضوع مكونات الحاسوب للتفتيش سواء المادية منها أم المعنوية، كما تم تناول إجراءات ضبط أدلة جرائم الحاسوب في حدود جريمة السرقة وتحديد معنى كل من التفتيش والضبط والشروط المتطلبة لصحة التفتيش من شروط موضوعية وشكلية لا بد من توافرها لسلامة إجراءات التفتيش.

4-1 التوصيات والنتائج

- ضرورة العمل وبصورة عاجلة على تحديد مصطلح وأنواع وعقوبة جرائم الكمبيوتر،مع ضرورة التعاون العربي والدولي في مكافحة هذه الجريمة، وضرورة التنسيق بين مختلف الجهات الأمنية، مع وضع تشريعات خاصة لحماية أجهزة الكمبيوتر ومعطياته وبرامجه، والأهم من ذلك نشر الوعي المعلوماتي بين الجمهور وتعليمهم كيفية التعامل السليم والصحي والأمن مع شبكة الإنترنت لحمايتهم من الوقوع فريسة سهلة لمحترفي الجرائم الإلكترونية وذلك من خلال نشر التوعية من خلال وسائل الإعلام وإنشاء مراكز علمية متخصصة من أجل ذلك.
- لا بد أن تسعى الدول فيما بينها إلى بذل كل جهد في مواجه إساءة استخدام الجرائم الإلكترونية، وذلك من خلال إقرار جزاءات جنائية وجملة من التدابير المناسبة والتعديلات الملائمة للجرائم الإلكترونية وسرعة تطورها تستهدف تدريب وتحسين وتنمية الوعي والقدرات لدى القضاء والنيابة العامة ورجال الضابطة القضائية المنوط بهم تتبع الجرائم الإلكترونية فيما يخص إجراءات التحقيق والتفتيش والضبط ومحاكمة مرتكبيها وإصدار الأحكام المتعلقة بها مما يخلق قوة قادرة على الحد منها.
- تنظيم المؤتمرات والندوات والمنتديات وورش العمل التي تختص بمناقشة جرائم الكمبيوتر والإنترنت وسبل التصدي لها، وزيادة التعاون مع الدول العربية من أجل تفعيل وتطوير منظومة مكافحة الجرائم الإلكترونية والاستفادة من تجارب الدول العالمية في هذا المجال.
- ندعو القائمين على القرار بقانون الفلسطيني المتعلق بالجرائم الإلكترونية بإعادة النظر في القانون بحيث يكون شاملا ولا يقتصر على تغطية جزائية من تلك الجرائم، حيث غفل عن كثير من الأمور الضرورية التي كان لا بد من النص عليها، مثل: تعريف الجرائم الإلكترونية، وإجراءات التحقيق التي يفترض اتباعها في حال الجرائم الإلكترونية.
- حث الجهات التعليمية في الوطن العربي عامة وفي فلسطين خاصة على تثقيف الطلاب والطالبات في المدارس في مختلف المراحل بجرائم الإنترنت والكمبيوتر ومخاطر الاستخدام السيء للإنترنت، وما يترتب علية من إيقاع العقوبات والجزاءات وفقاً للأنظمة والتشريعات والقوانين المتعلقة بجرائم الإنترنت المعمول بها في كثير من الدول العربية والعالمية، بالإضافة إلى توعية أولياء الأمور بتلك المخاطر ووضع استخدام أبنائهم للإنترنت والكمبيوتر تحت الرقابة الفاعلة منهم، بالإضافة إلى تضمين مناهج الحاسوب في المدارس العربية كافة والفلسطينية خاصة بمواضيع تثقفيه مختصرة أو مطولة وذلك حسب المرحلة العمرية للأنظمة والقوانين الوطنية والعربية المتعلقة بجرائم الحاسوب والإنترنت.
- ضرورة إعداد الكوادر الأمنية القادرة على مواجه مخاطر الإنترنت والحاسوب، وكذلك إعداد سلطات التحقيق من الناحية الفنية والتحري والتحقيق وجمع الأدلة والتفتيش والضبط في مجال جرائم الحاسوب والإنترنت، وما يستلزم ذلك من إنشاء مراكز متخصصة وفرق مدربة على هذا النوع من الجرائم وطرق مكافحتها وكيفية التعامل مع أجهزة الكمبيوتر، والعمل على تخصيص شرطة خاصة لمكافحة هذا النوع من الجرائم المستحدثة.
- العمل على تعديل قوانين الإجراءات الجنائية بالقدر الكافي الذي يسمح ببيان الأحكام وإلزام اتباعها حال مباشرة إجراءات التحقيق ومنها التفتيش على أجهزة الحاسوب وضبط المعلومات التي تحتويها تلك الأجهزة وضبط البريد الإلكتروني حتى نستطيع ضبط الأدلة المشروعة بحيث يتمكن القاضي من أن يستند إلى الأدلة المستخرجة من الحاسوب الآلي والإنترنت مما يساعد في الإثبات وإدانة المتهم
- تجريم سرقة المال الإلكتروني المعنوي (المكونات المعنوية) بنصوص صريحة بوجه عام وذلك على أنه مال بالمعنى التقليدي المنصوص عليه في جريمة السرقة المنصوص عليها في قانون العقوبات، مع المساواة في الحماية بين المال المادي (المكونات المادية) والمال المعنوي الذي كان محل جدل ونقاش بين الفقهاء حول مدى إخضاعه للحماية القانونية المنصوص عليها في جريمة السرقة.
- يجب أن يخضع التفتيش في الجرائم الإلكترونية لمجموعة من الضمانات التي توضح حدوده المكانية والزمانية والموضوعية والإجرائية، نظراً لخطورته ومساسه بالحريات الشخصية للأشخاص وحياتهم الخاصة وحرمة منازلهم، ومن أهم هذه الضمانات مباشرته من قبل سلطة التحقيق وفقاً للإجراءات المقررة قانونا، بحيث تلتزم سلطة التحقيق والتفتيش واجب الحيطة والحذر أثناء التفتيش فلا يطلع على الأشياء والأماكن إلا بالقدر الذي يحتمل أن يجد فيها بيانات أو برامج أو أشياء أو أدلة لها علاقة بالجريمة الإلكترونية.