جامعة بنغازي
ليبيا

كلية الحقوق
قسم القانون الجنائي

مدى قبول الدليل الرقمي في الإثبات الجنائي

"دراسة مقارنة"

لغرض استكمال متطلبات الحصول على الدرجة العالية ((الماجستير)) في القانون الجنائي

إعـداد الطالب

عبدالمنعم حمد مُحَّد

تحت إشراف الأستاذ الدكتور

سعد حماد القبائلي

العام الجامعي

(2016 – 2017)

اقْرَأْ بِاسْمِ رَبِّكَ الَّذِي خَلَقَ (1) خَلَقَ الْإِنْسَانَ مِنْ عَلَقٍ (2) اقْرَأْ وَرَبُّكَ الْأَكْرَمُ (3) الَّذِي عَلَّمَ بِالْقَلَمِ (4) عَلَّمَ الْإِنْسَانَ مَا لَمْ يَعْلَمْ (5)

سورة العلق الآيات (1–5)

الإهداء

إلى من ربياني على حب العلم صغيراً
وحقق الله حلمهما وأنا كبيرٌ
والدتي (رحمة الله عليها)
والدي أطال الله في عمره

إلى إخوتي الذين تقاسموا معِ هذا العمل
قوت يومهم وراحتهم

إلى هؤلاء جميعاً .. اهدي هذا البحث المتواضع

الشكر والتقدير

في البداية ، الشكر والحمد لله ، جل في عُلاه
فإليه يُنسب الفضل كله في الإكمال
والكمال يبقى لله وحده هذا العمل
وبعد الحمد لله ، فإنني أتوجه إلى أستاذي
الأستاذ الدكتور سعد حماد القبائلي
المشرف على الرسالة بالشكر والتقدير والذي
لن تفيه أي كلمات حقه ، فلولا مثابرته ودعمه
المستمر ، ما تم هذا العمل
فله مني جزيل الشكر وعظيم الامتنان.

الفهرس

الموضوع	الصفحة
المقدمة	1
أولاً . أهمية الموضوع	2
ثانياً . الهدف من الدراسة	2
ثالثاً . إشكالية البحث	3
رابعاً . نطاق البحث	3
خامساً . منهج البحث	3
سادساً . خطة البحث	4
الفصل الاول	
ماهية الجرائم الإلكترونية والدليل الرقمي	5
المبحث الاول	
ماهية الجرائم الإلكترونية	6
المطلب الاول	
تعريف الجرائم الإلكترونية وخصائصها وأهدافها	6
الفرع الأول	
تعريف الجرائم الإلكترونية	6
أولاً . الاتجاه الموسع لتعريف الجرائم الإلكترونية	7
ثانياً . الاتجاه المضيق لتعريف الجرائم الإلكترونية	8
الفرع الثاني	
خصائص الجرائم الإلكترونية	9
أولاً . أن وسائل تقنية المعلومات هي أداة ارتكاب الجرائم الإلكترونية	10
ثانياً . صعوبة اكتشاف الجرائم الإلكترونية	10
ثالثاً . يتم ارتكاب الجرائم الالكترونية بأقل عنف في التنفيذ	10
رابعاً . جريمة قد تكون عابرة للحدود	11
خامساً . التبليغ عن الجرائم الإلكترونية	11
سادساً . عدم كفاية القوانين السارية في مواجهة الجرائم الإلكترونية	11

الموضوع	الصفحة
الفرع الثالث	
أهداف الجرائم الإلكترونية	12
أولاً . السعي إلى تحقيق الكسب المالي	12
ثانياً . الانتقام	12
ثالثاً . الرغبة في قهر النظام والتفوق على تعقيد الوسائل التقنية	12
رابعاً . جمع المعلومات	13
خامساً . دوافع سياسية أو عسكرية أو دينية	13
سادساً . الأشخاص أو الجهات	13
المطلب الثاني	
أنواع الجرائم الالكترونية وفئات المجرمين المعلوماتيين	14
الفرع الأول	
أولاً . الجرائم الالكترونية التي تمثل اعتداء على الاشخاص	15
ثانياً . الجرائم الالكترونية التي تمثل اعتداء على الأموال	16
ثالثاً . الجرائم الالكترونية التي تمثل الاعتداء على الآداب العامة وحقوق الملكية الفكرية	20
رابعاً . جرائم الاعتداء ضد سريّة البيانات والنظم	21
الفرع الثاني	
فئات المجرمين المعلوماتيين	26
أولاً . القراصنة	26
ثانياً . المجرمون الحاقدون	26
ثالثاً . المحتالون	27
رابعاً . الجواسيس	27
المبحث الثاني	
ماهية الدليل الرقمي	28
المطلب الأول	
التعريف بالدليل الجنائي	28

الموضوع	الصفحة
الفرع الأول	
تعريف الدليل الجنائي	28
أولاً . الدليل لغةً	28
ثانياً . الدليل في الاصطلاح القانوني	28
ثالثاً . الدليل اصطلاحاً	29
الفرع الثاني	
خصائص الدليل الجنائي	30
أولاً . الجريمة تصنع أدلتها	30
ثانياً . استظهار عناصر الأدلة يتوقف على الكفاءة الشخصية لرجال الضبط القضائي وسلطات التحقيق	31
ثالثاً . يتميز الدليل الجنائي بصعوبة استخلاصه	31
رابعاً . الدليل الجنائي هو الوسيلة الوحيدة الذي ينقل أحداث الجريمة إلى علم القضاء	32
خامساً . قطعية الدليل	32
سادساً . الدليل الجنائي يخضع لتقدير سلطة المحكمة	33
سابعاً . يتميز الدليل الجنائي بتسانده مع الأدلة الأخرى	33
الفرع الثالث	
تقسيمات الدليل الجنائي	34
أولاً . تقسيم الأدلة من حيث قوتها في الإثبات	34
ثانياً . تقسيم الأدلة من حيث علاقة الدليل بالواقعة المراد إثباتها	34
ثالثاً . تقسيم الأدلة من حيث وظيفتها	35
رابعاً . تقسيم الأدلة من حيث مصدرها	36
المطلب الثاني	
التعريف بالدليل الرقمي	37
الفرع الأول	
تعريف الدليل الرقمي	37
أولاً . الاتجاه المضيق لتعريف الدليل الرقمي	38
ثانياً . الاتجاه الموسع لتعريف الدليل الرقمي	39

الموضوع	الصفحة
الفرع الثاني	
خصائص الدليل الرقمي	40
أولاً . الدليل الرقمي دليل علمي	40
ثانياً . الدليل الرقمي دليل تقني	40
ثالثاً . الدليل الرقمي يسهل التخلص منه	41
رابعاً . إن نشاط الجاني لمحو الدليل الرقمي يسجل عليه كدليل أيضاً	41
خامساً . الدليل الرقمي قابل للنسخ	41
سادساً . الأتساع العلمي لمسرح الدليل الرقمي	41
سابعاً . الدليل الرقمي يمتاز بالسعة التخزينية العالية	42
ثامناً . يمتاز الدليل الرقمي برصد معلومات عن الجاني	42
الفرع الثالث	
تقسيمات الدليل الرقمي	42
أولاً . تقسيم الدليل الرقمي من منظور وزارة العدل الأمريكية	42
ثانياً . تقسيم الدليل الرقمي من منظور فقهي	43
الفصل الثاني	
إجراءات جمع الدليل الرقمي	46
المبحث الأول	
الإجراءات التقليدية لجمع الدليل الرقمي	46
المطلب الأول	
المعاينة في مسرح الجرائم الإلكترونية	46
الفرع الأول	
تعريف المعاينة وأهميتها	46
أولاً . تعريف المعاينة	46
ثانياً . أهمية المعاينة	47
الفرع الثاني	
إجراءات المعاينة في مسرح الجرائم الإلكترونية	48
أولاً . وقوع الجريمة على الكيان المادي للحاسب الآلي	48

الموضوع	الصفحة
ثانياً . وقوع الجريمة على الكيان المعنوي أو الغير المادي أو المنطقي أو بواسطة جهاز الحاسب الآلي	49
المطلب الثاني	
التفتيش في مسرح الجرائم الإلكترونية	51
الفرع الأول	
الضوابط الموضوعية لتفتيش مسرح الجرائم الإلكترونية	51
أولاً . سبب تفتيش مسرح الجرائم الإلكترونية	51
ثانياً . محل تفتيش مسرح الجرائم الالكترونية	54
ثالثاً . السلطة المختصة بالتفتيش في مسرح الجرائم الإلكترونية	59
الفرع الثاني	
الضوابط الشكلية لتفتيش مسرح الجرائم الإلكترونية	63
أولاً . الحضور الضروري لبعض الأشخاص أثناء إجراء التفتيش في مسرح الجرائم الالكترونية	63
ثانياً . الميقات الزمني لإجراء تفتيش مسرح الجرائم الإلكترونية	63
ثالثاً . محضر التفتيش في الجرائم الإلكترونية	64
المطلب الثالث	
ضبط الدليل في الجرائم الإلكترونية	66
الفرع الأول	
ضبط الكيانات المادية في الجرائم الإلكترونية	66
أولاً . ضبط المنقولات في الجرائم الإلكترونية	67
ثانياً . وضع الأختام على العقارات الموجود بها المنقولات في الجرائم الإلكترونية	69
الفرع الثاني	
ضبط الكيانات المعنوية في الجرائم الإلكترونية	70
المطلب الرابع	
الشهادة في الجرائم الإلكترونية	74
الفرع الأول	
تعريف الشهادة وأهميتها	74

الموضوع	الصفحة
أولاً . تعريف الشهادة في الجرائم الإلكترونية	74
ثانياً . أهمية الشهادة في الجرائم الإلكترونية	75
الفرع الثاني	
التزامات الشاهد في الجرائم الالكترونية	77
أولاً . التزام الشاهد بالحضور الضروري أمام الجهة القضائية التي استدعته	77
ثانياً . قسم اليمين القانونية أمام الجهة القضائية التي استدعته	78
ثالثاً . التزام الشاهد بقول الحقيقة أمام الجهة القضائية التي استدعته	78
المطلب الخامس	
الخبرة في الجرائم الإلكترونية	80
الفرع الأول	
القواعد القانونية التي تحكم الخبرة في الجرائم الإلكترونية	80
أولاً . تعريف الخبرة وبيان أهميتها	80
ثانياً . شروط صحة عمل الخبير	82
الفرع الثاني	
القواعد الفنية التي تحكم الخبرة في الجرائم الإلكترونية	84
أولاً . المسائل التي يستعين فيها بالخبير الإلكتروني	84
ثانياً . الإمكانيات الإلكترونية لمختبر الجرائم الإلكترونية	84
ثالثاً . خطوات استخلاص الدليل الرقمي بواسطة الخبير الالكتروني	86
المبحث الثاني	
الإجراءات الحديثة لجمع الدليل الرقمي	87
المطلب الأول	
التحفظ السريع على البيانات المخزنة وتجميعها	87
الفرع الأول	
التحفظ السريع على البيانات المعلوماتية المخزنة	87
أولاً . تعريف التحفظ السريع على البيانات المعلوماتية المخزنة	88
ثانياً . إجراءات التحفظ السريع على مضمون البيانات المخزنة	88

الموضوع	الصفحة
الفرع الثاني	
التجميع في الوقت الفعلي للبيانات المتعلقة بخط سير البيانات	90
المطلب الثاني	
الأمر بتقديم بيانات معلوماتية متعلقة بالمشترك	92
الفرع الأول	
موقف التشريع الفرنسي	92
الفرع الثاني	
موقف التشريع الأمريكي	93
الفرع الثالث	
موقف التشريع الليبي	94
المطلب الثالث	
اعتراض الاتصالات الإلكترونية المتعلقة بالمشترك	95
الفرع الأول	
تعريف اعتراض الاتصالات الإلكترونية واهميتها	95
أولاً . تعريف اعتراض الاتصالات الإلكترونية	95
ثانياً . أهمية اعتراض الاتصالات الإلكترونية	97
الفرع الثاني	
الضمانات القانونية لمشروعية اعتراض الاتصالات الإلكترونية	98
أولاً . ضرورة إصدار إذن من القاضي باعتراض الاتصالات الإلكترونية	98
ثانياً . أن يكون إذن القاضي باعتراض الاتصالات الإلكترونية مسبباً	102
ثالثاً . عدم جواز اعتراض الاتصالات الإلكترونية إلا بصدد جريمة معينة وقعت فعلاً	103
رابعاً . أن يكون هناك مدة محددة قانوناً لاعتراض الاتصالات الإلكترونية	103
خامساً . أن يكون المتهم طرفاً في المحادثات التي يؤمر باعتراضها أو تسجيلها	104
الفصل الثالث	
حجية الدليل الرقمي أمام القضاء الجنائي	105
المبحث الأول	

الموضوع	الصفحة
قبول الدليل الرقمي أمام القضاء الجنائي	106
المطلب الأول	
موقف الأنظمة الإجرائية من قبول الدليل الرقمي أمام القضاء الجنائي	106
الفرع الأول	
نظام الإثبات المقيد أو القانوني	106
الفرع الثاني	
نظام الإثبات الحر	109
الفرع الثالث	
نظام الإثبات المختلط	111
المطلب الثاني	
شروط قبول الدليل الرقمي أمام القضاء الجنائي	113
الفرع الأول	
مشروعية الدليل الرقمي	113
أولاً . النظام اللاتيني	114
ثانياً . النظام الانجلوساكسوني	115
ثالثاً . النظام المختلط	116
الفرع الثاني	
مناقشة الدليل الرقمي	117
أولاً . عدم جواز أن يحكم القاضي في الجرائم الالكترونية بناءً على معلوماته الشخصية.	118
ثانياً . عدم استناد القاضي في حكمه بناءً على رأي الغير.	119
ثالثاً . ضرورة تأهيل القضاة لمعرفة تكنولوجيا المعلومات.	120
الفرع الثالث	
تقيد القاضي الجنائي بأدلة معينة في جريمة الزنا	120
الفرع الرابع	
تقيد القاضي الجنائي بطرق الاثبات الخاصة بالمواد غير الجنائية	121
المبحث الثاني	

الموضوع	الصفحة
تقدير القضاء الجنائي للدليل الرقمي	123
المطلب الاول	
الصعوبات التي تؤثر على الدليل الرقمي	123
الفرع الاول	
المصلحة الأولى بالرعاية	123
الفرع الثاني	
صعوبة تعارض الاثبات بالدليل الرقمي مع حرية القاضي الجنائي في تكوين عقيدته.	125
أولاً . عدم رؤية الدليل الرقمي	125
ثانياً . صعوبة الاصالة في الدليل الرقمي	126
ثالثاً . ضخامة نفقات الحصول على الدليل	126
رابعاً . عدم إلمام رجال العدالة الجنائية بالمعرفة التقنية	127
الفرع الثالث	
الطبيعة العلمية للدليل الرقمي	129
أولاً . دور الخبير في الدعوى الجنائية	129
ثانياً . تقدير القضاء للدليل العلمي	130
المطلب الثاني	
يقينية الدليل الرقمي	131
الفرع الأول	
المراحل التي يصل بها القاضي إلى اليقين	131
أولاً . مرحلة خلو ذهن القاضي من الواقعة	131
ثانياً . مرحلة الشك	131
ثالثاً . مرحلة المعرفة العلمية	132
الفرع الثاني	
موقف الأنظمة الإجرائية من يقينية الدليل الرقمي	132
أولاً . النظام الانجلوساكسوني	132
ثانياً . النظام اللاتيني	134
ثالثاً . النظام المختلط	137

الموضوع	الصفحة
المطلب الثالث	
دور القضاء المستعجل في الجرائم الإلكترونية	138
الفرع الأول	
الأساس القانوني لتدخل القضاء المستعجل	138
الفرع الثاني	
شروط اختصاص القضاء المستعجل	139
أولاً . شرط الاستعجال	139
ثانياً . أن يكون المطلوب إجراء وقتي لا يمس أصل الحق	140
ثالثاً . أن يكون هناك خطراً عاجلاً أو محدقاً ماثلاً بالفعل	140
الفرع الثالث	
الدور الوقائي للقضاء المستعجل في الجرائم الإلكترونية	140
الخاتمة	142
أولاً . النتائج	142
ثانياً . المقترحات	143
قائمة المراجع	145

المقدمة

لاشك في أنه مع مطلع القرن الواحد والعشرين[1] ، أصبح المجتمع الدولي يعتمد بصفة أساسية على جهاز الحاسب الآلي[2] ، وشبكات المعلومات وفي مقدمتها الإنترنت[3] ، التي تدار من قبل مواقع حكومية أو شخصية ، تعنى بجميع الأمور الحياتية المختلفة ، وتقوم بتنظيم الأعمال وتحقيق التواصل ، وهذا هو الجانب الإيجابي للثورة المعلوماتية وتقنياتها ، إلا أنه من الطبيعي أن يصاحب هذه الثورة المعلوماتية وجه آخر يتمثل في الجانب السلبي من خلال إساءة استخدام الأنظمة المعلوماتية[4] ، التي أدت إلى ظهور أنماط مستحدثة من الجرائم لم تكن معروفة من قبل اصطلح على تسميتها بالجرائم الإلكترونية التي أصبحت خطراً يهدد مجموعة من المصالح والقيم الاجتماعية والشخصية الأساسية .

وخطورة هذه الظاهرة الإجرامية تتجلى في سهولة ارتكابها ، علاوة على أن مقترفيها يتصفون بقدر عال من الذكاء والمهارة ، ويعتمد غالباً في اقترافها على التضليل والخداع دون اللجوء إلى أسلوب العنف[5]، مما يثير مشكلات كثيرة في إجراءات جمع الأدلة الجنائية وإثبات هذه الجرائم اتجاهها .

وبالتالي فإن إثبات هذا النوع من الجرائم يحتاج إلى وسائل إلكترونية تتناسب مع طبيعتها الخاصة لكشف هذا النمط من الجرائم ونسبتها إلى مرتكبيها ، وتسمى هذه الوسيلة بالدليل الرقمي[6] ، التي أصبحت ضرورة ملحة فرضتها الحاجة إلى أدلة تنتمي إلى البيئة نفسها التي ترتكب فيها أو من خلالها هذه الجرائم.

---

[1] 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 بمركز البحوث والدراسات الإمارات العربية المتحدة 26-27-28/4 / 2003 ، بدون ترقيم صفحات، منشور على الإنترنت :
Http//www.flaw.Net thread.s/1333

[2] الحاسب الآلي هو : " عبارة عن مجموعة من الآلات الإلكترونية صنعها الإنسان لخدمة أغراضه اليومية الذي له المقدرة على معالجة البيانات المدخلة إليه عن طريق وحدات الإدخال وتخزينها ، ومن ثم معالجتها بتنفيذ العمليات الحسابية والمنطقية عليها وفقاً لمجموعة من التعليمات والأوامر المحددة ، وبالتالي الحصول على المعلومات التي يتم استخراجها عن طريق وحدات الإخراج " . (بشير علي القائد ، مقدمة في علم الحاسب الآلي ،الطبعة الرابعة ، دار الحكمة، طرابلس، 2009 ، ص 17 ،18)

[3] الإنترنت هي : " شبكة دولية للاتصالات يمكن الدخول إليها عن طريق جهاز الكمبيوتر المتواجد في أي بقعة من بقاع العالم " (شيماء عبدالغني محمد عطا الله ، الحماية الجنائية للتعاملات الإلكترونية ، دار الجامعة الجديدة ، الإسكندرية ، 2007 ، ص16.).

[4] نظام المعلومات هو : " مجموعة البرامج والأدوات والمعدات لإنتاج وتخزين ومعالجة البيانات أو المعلومات أو إدارة البيانات أو المعلومات " ، المادة الثالثة من قانون جرائم المعلوماتية السوداني الصادر في 2007/6/20 .

[5] موسى مسعود أرحومة ، "السياسة الجنائية في مواجهة جرائم الانترنت" ، مجلة دراسات قانونية ، العدد السابع عشر ، 2008 ص89 .

[6] مصطلح الرقمية"digital":- يرجع أصل هذا المصطلح التقنى إلي استخدام النظام الرقمى الثنائي(1,0) وهى الصيغة التي تسجل بها كل البيانات أشكال وحروف وصور وغيرها داخل الحاسب الآلي ، حيث يمثل (0) وضع الإغلاق off، والواحد (1) وضع التشغيل on ويمثل الرقم (0) أو الرقم (1) مايعرف بالبيت Bit (د. عبدالناصر محمد محمود فرغلي ، د. عبيد سيف سعيد المسماري ، "الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية ، دراسة تطبيقية مقارنة" ، ورقة عمل مقدمة للمؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي المنعقد بالرياض في الفترة 12-2007/11/14 ، ص5) .

أولاً . أهمية الموضوع :

تكمن أهمية الموضوع في أن التطور الذي حدث في العالم في مجال تقنية المعلومات لا يمكن أن يتطور بذاته ، دون أن تتوافر له القواعد القانونية ، التي تنظم طرق استغلالها ، ونظراً لأنه في مرحلة التطور ، فإن شأنه شأن أي تطور جديد يحمل في طياته الجانب المظلم الذي يتجسد في مجال القانون الجنائي بظهور المجرم المعلوماتي والجرائم الإلكترونية .

وأمام هذا النوع الجديد من الإجرام ، لا يبدو قانون الإجراءات الجنائية في وضعه الراهن يفي بالغرض لإثبات الجرائم الإلكترونية ، نظراً للصعوبات الناجمة عن الطبيعة الخاصة الفنية والعلمية للوسائل الإلكترونية المستخدمة في ارتكابها ، بالإضافة إلى أن القواعد الإجرائية التقليدية قد وضعت في ظل تفكير يقتصر إدراكه على الجرائم المادية التي يتعذر معه تطبيقها لحماية الكيانات المعنوية الناتجة عن تقنية المعلومات ، مما يتطلب استجابة القواعد الإجرائية للتغيرات المستمرة ، التي صاحبت تغير طريقة ارتكاب الجرائم أووسائل ارتكابها ، والبيئة التي تتم من خلالها .

كما تكمن أهمية البحث أيضاً في بيان مدى تأثير طبيعة الدليل الرقمي على اقتناع القاضي الجنائي ، حيث أصبح القاضي الجنائي في الوقت الراهن يعتمد على الأدلة العلمية بما فيها الدليل الرقمي ، مما يؤدي إلى سيطرة الخبير بالدرجة الأولى على العملية الإثباتية مقابل تضاؤل دور القاضي الجنائي في تقديره لقيمة الدليل الرقمي .

ثانياً . الهدف من الدراسة :

الهدف المبتغى من هذه الدراسة ، هو المساعدة على شرح بعض المفاهيم الفنية الأساسية بالقدر الذي تقتضيه الدراسة باعتبارها بمثابة الأساس العلمي والمنطقي لبعض المفاهيم القانونية المستحدثة في هذا المجال كمساهمة في خلق فقه جنائي معلوماتي جديد .

كما آمل أن يقدم هذا البحث مزيداً من الفهم لهذا الموضوع ، وأن يقدم تصورات لحل بعض القضايا والإشكاليات المتعلقة بالأدلة الرقمية في مجال الإثبات الجنائي ، فيما يتعلق بكيفية جمعها ، وتقديمها للقاضي الجنائي ، ومدى قبولها لدى القضاء الجنائي وكيفية تقديره لها .

ثالثاً . إشكالية البحث :

تكمن إشكالية البحث في أن الدليل الرقمي يتمتع بخصائص معينة تميزه عن غيره من الأدلة الجنائية ، من حيث أنه غير مرئي ومن السهل إخفاؤه ، فضلاً عن إعاقة الحصول عليه وبالتالي فإن قبوله في إطار الإثبات الجنائي يثير العديد من التساؤلات حول مشروعية الأخذ به ، إذ أنه يشترط في الدليل الجنائي أن يكون قد قبله المشرع ضمن أدلة الإثبات الجنائي ، فما هو موقف المشرع من هذا النوع من الأدلة ؟ وما هي الضوابط اللازمة لاعتماد الدليل الرقمي كدليل إثبات يدخل في مجال النظرية العامة للإثبات الجنائي؟ .

كذلك فإن الحصول على الدليل الجنائي ، يجب أن يتم بطريقة مشروعة وذلك باستخدام وسائل جمع الأدلة المنصوص عليها في قانون الإجراءات الجنائية ، وبالنظر إلى الطبيعة الخاصة التي يتمتع بها الدليل الرقمي من حيث إعاقة الحصول عليها ، فإنه يثار التساؤل عن كيفية الحصول على الدليل الرقمي كدليل إثبات أمام القضاء الجنائي ؟ ولكن عند اللجوء إلى استخدام إجراءات علمية جديدة في البحث عن الحقيقة ، فإن ذلك قد يكون ضد كرامة الإنسان من حيث المساس بحقوقه وحريته الشخصية ، مما يثير التساؤل ، كيف يمكن تحقيق التوازن بين مصلحة المجتمع في كشف أو إظهار حقيقة الجرائم وملاحقة المجرمين ومصلحة الفرد في حرمة حياته الخاصة ؟ كما أن صعوبة فهم الدليل الرقمي المتحصل من الوسائل الإلكترونية يثير التساؤل حول مدى حجية الدليل الرقمي وتأثيره في تكوين عقيدة القاضي الجنائي ؟ .

رابعا . نطاق البحث :

يقتصر نطاق البحث من حيث بيان ماهية الجرائم الإلكترونية والدليل الرقمي ، ومن حيث كيفية جمع الدليل الرقمي ، ومدى حجيته وتأثيره في تكوين عقيدة القاضي الجنائي ، وبالنظر للطبيعة الخاصة لهذا النوع من الأدلة من حيث عدم وجود نص صريح في قانون الإجراءات الجنائية الليبي يبين هذا النوع من الأدلة ، فهذا يعني أن دراستنا ستكون دائرة في فلك القواعد العامة في قانون الإجراءات الجنائية ، غير أن هذا لا يمنع من الرجوع إلى القوانين الجنائية الخاصة ، وكذلك المدنية ، وأي أعمال قانونية أخرى ، كالمعاهدات الدولية ، كلما اقتضت الضرورة ذلك.

خامسا . منهج البحث :

تعتمد هذه الدراسة على منهج الدراسة الوصفي أو الإستقرائي والمقارن .

سادسا . خطة البحث :

سأتناول موضوع البحث من خلال ثلاثة فصول ، سنخصص الفصل الأول لدراسة ماهية الجرائم الإلكترونية والدليل الرقمي ، وسنقسمه إلى مبحثين ، نخصص المبحث الأول للحديث عن ماهية الجرائم الإلكترونية ، ونكرس المبحث الثاني لدراسة ماهية الدليل الرقمي وسنخصص الفصل الثاني لدراسة إجراءات جمع الدليل الرقمي وسنقسمه إلى مبحثين ، نخصص المبحث الأول لدراسة الإجراءات التقليدية لجمع الدليل الرقمي ، ونكرس المبحث الثاني لدراسة الإجراءات الحديثة لجمع الدليل الرقمي ، أما الفصل الثالث سنخصصه لبيان حجية الدليل الرقمي أمام القضاء الجنائي ، حيث سنقسمه إلى مبحثين ، نخصص المبحث الأول منه للحديث عن قبول الدليل الرقمي أمام القضاء الجنائي ، ونكرس المبحث الثاني لدراسة تقدير القضاء الجنائي للدليل الرقمي .

الفصل الأول

ماهية الجرائم الإلكترونية والدليل الرقمي

إن التطور الهائل الذي حدث في مجال تكنولوجيا المعلومات ، لم يخل من الاثار السلبية من خلال سوء إستخدام تقنية المعلومات مما أدى إلى ظهور أشكال جديدة تظاف إلى طائفة الجرائم وهي الجرائم الإلكترونية ، والتي تنقسم من حيث المصلحة المحمية قانونا الى جرائم إلكترونية تقليدية ، من حيث أنها مصالح وحقوق يحميها قانون العقوبات ، ثم طرأ عليها متغير جديد هو إرتكابها بوسائل إلكترونية ، إلا أن الجرائم الإلكترونية المستحدثة تقع على سرية البيانات والنظم ، بالإضافة إلى أن مقترفيها يتصفون بقدر عال من الذكاء والمهارة ، ويعتمد غالبا في إقترافها على إسلوب التضليل والخداع دون اللجوء إلى إسلوب العنف حتى يقوم يتنفيذ جريمته ، والتي تختلف من حيث أهدافها ، فمنها من يسعى الى تحقيق الكسب المالي ، ومنها من يهدف الى الإنتقام وجمع المعلومات ، والقدرة على التفوق وتحدي تقنية المعلومات ، كما تهدف بعض الجرائم الإلكترونية إلى تحقيق أهداف سياسية أوعسكرية أو إيدولوجية ، ونظراً للطبيعة الخاصة لهذا النوع من الجرائم ، فإن إثباتها يحيط به كثير من الصعوبات تتجلى في أن اكتشافها يحتاج إلى طرق أو وسائل إلكترونية تصلح لأن تكون أدلة إثبات لهذا النوع من الجرائم ، وتدعي هذه الوسيلة بالدليل الرقمي ، باعتباره الوسيلة الوحيدة والرئيسية لإثبات هذه الجرائم ، حيث أن الدليل الرقمي يتمتع بخصائص تميزه عن الأدلة الجنائية التقليدية من حيث أنه دليل علمي وتقني وأنه قابل للنسخ ، كما أنه يرصد معلومات عن تحركات الجناة ، بالإضافة إلى الإتساع العالي والتخزيني للدليل الرقمي ، وبالتالي فإن سلطات الإستدلال والتحقيق قد تجد غايتها بسهولة أيسر من الدليل الجنائي المادي ، وبما أن الدليل الرقمي له طبيعة خاصة تميزه عن الدليل الجنائي التقليدي مما يتطلب منا تعريف الدليل الرقمي ، وتحديد خصائصه وبيان تقسيماته.

وبناءً على ما تقدم سنقسم هذا الفصل إلى مبحثين : نخصص المبحث الأول لدراسة ماهية الجرائم الإلكترونية . ونكرس المبحث الثاني لدراسة ماهية الدليل الرقمي .

المبحث الأول

ماهية الجرائم الإلكترونية

نظراً للطبيعة الخاصة للجرائم الإلكترونية ، فإنه يتطلب منا في هذا المبحث أن نعرّف الجرائم الإلكترونية وبيان خصائصها ، ثم نوضح صورها ، مع تحديد فئات المجرمين الذين يقومون بارتكاب الجرائم الإلكترونية ، ومعرفة الهدف أو الغاية من ارتكاب هذه الجرائم .

وتأسيساً على ما تقدم سنقسم هذا المبحث إلى مطلبين : نخصص المطلب الأول تعريف الجرائم الإلكترونية وبيان خصائصها وأهدافها . ونكرس المطلب الثاني لدراسة أنواع الجرائم الإلكترونية وفئات المجرمين المعلوماتيين.

المطلب الأول

تعريف الجرائم الإلكترونية وخصائصها وأهدافها

سنتناول في هذا المطلب تعريف الجرائم الإلكترونية وبيان خصائصها وأهداف الجرائم الإلكترونية كلاً منها في فرع مستقل ، حيث سنخصص الفرع الأول . لدراسة تعريف الجرائم الإلكترونية . ونكرس الفرع الثاني . لدراسة خصائص الجرائم الإلكترونية ، ونفرد الفرع الثالث لدراسة أهداف الجرائم الإلكترونية .

الفرع الأول

تعريف الجرائم الإلكترونية

أدت الحداثة التي تتميز بها الجرائم الإلكترونية ، واختلاف النظم القانونية والثقافية بين الدول ، إلى عدم الاتفاق على مصطلح موحد للدلالة عليها ، حيث تعددت المصطلحات للجرائم الإلكترونية ، فتارةً تُسمى بجرائم الكمبيوتر والإنترنت ، وتارةً أخرى تُسمى بجرائم الحاسب الآلي وكما يُطلق عليها أحياناً بالجرائم السايبيرية ، وكما تُعرف أيضاً بالجرائم المعلوماتية إلى غير ذلك من المصطلحات.

كما تعددت الآراء بشأن تعريف الجرائم الإلكترونية ، فقد وضع الفقهاء والدارسون لها عدة تعريفات ، فهناك جانب من الفقه عرفها من زاوية فنية وأخرى قانونية.[7]

واختلفت كذلك التعريفات ، بحسب المعايير المعتمدة ، كاعتماد التعريف على معيار قانوني كتعريفها بدلالة موضوع الجريمة ، أو الوسيلة المستخدمة ، أو بحسب معيار شخصي ويتحدد في مدى توافر المعرفة والدراية بتقنية المعلومات لدى مرتكب الجريمة ، وفي مقابل هذا وذاك يذهب البعض إلى محاولة الجمع بين أكثر من معيار.

---

[7] عبدالفتاح بيومي حجازي ، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت ، منشأة المعارف ، الاسكندرية ، 2009 ، ص1.

ونشير باستقراء الجهود التي بُذلت لتعريف الجرائم الإلكترونية ، إلى وجود اتجاهين مختلفين ، أحدهما يوسع من تعريف الجرائم الإلكترونية ، والثاني يضيق من تعريف هذه الجرائم ، ولذا سنبين هذين الاتجاهين على النحو التالي :

أولاً . الاتجاه الموسع لتعريف الجرائم الإلكترونية :

يذهب جانب من الفقه إلى التوسع في تعريف الجرائم الإلكترونية ، حيث يعرفها بأنها هي "مجموعة من الأفعال المرتبطة بالمعلوماتية[8] ، التي يمكن أن تكون جديرة بالعقاب"[9] .

أو بأنها "كل سلوك غير مشروع ، أو غير أخلاقي ، أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات ، أو نقلها"[10] .

وقد عرفها بعض الفقهاء بأنها "نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي ، بطريقة مباشرة أو غير مباشرة ، كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود" [11].

كما جرى تعريفها أيضاً بأنها هي " كل سلوك غير مشروع ، يرتكب عن طريق الحاسب الآلي ، أو بمساعدته ، أو أن يكون أداة رئيسية في ارتكابه أو أن يكون له دور هام أو إيجابي في هذا الارتكاب"[12].

وكما هو ملاحظ من التعريفات المتقدمة ، أنها تتسم بالطابع الشمولي فليس بمجرد إشراك الحاسب الآلي ، أو شبكة المعلومات في الجريمة نطلق عليها وصف الجرائم الإلكترونية ، ذلك يمكن أن يكون الاعتداء واقعاً على الكيان المادي[13] للحاسب الآلي أو شبكة المعلومات كسرقة

---

(1) المعلوماتية :هي مشتقة من المعلومة ، وهو ما يستفيده المرء من إجتماع أكثر من بيان ، وهي أكثر شملاً من البيانات ، (بشير علي القائد ، مرجع سابق ، ص21)
أما المعلوماتية فيقصد بها حسب نص المادة الثالثة من قانون جرائم المعلوماتية السوداني الصادر في 2007/6/20 بأنها "نظم وشبكات ووسائل المعلومات والبرمجيات والحواسيب والإنترنت والأنشطة المتعلقة بها" .
أما البيانات فقد عرفها قانون الإثبات الكندي في المادة الأولى منه فقره (أ) بأنها "أي تمثيل في أي شكل كان للمعلومات أو الأفكار " (شيماء عبدالغني ، مرجع سابق ، ص18) .

(9) محمد علي سالم وحسن عبيد هجيج ، "الجريمة المعلوماتية" ، مجلة جامعة بابل العلوم الإنسانية ، المجلد 14 ، العدد 3 ، 2007 ص87.

(10) موقع منظمة التعاون الاقتصادي والتنمية على شبكة الإنترنت .www.occd.org

(11) عبدالفتاح بيومي حجازي ، مرجع سابق ، ص1.

(12) هلالي عبداللاه أحمد ، جرائم المعلوماتية التقليدية والمستحدثة وتطبيقاتها في النظام البحريني ، دار النهضة العربية ، القاهرة ، 2013 ، ص99.

(13)**الكيان المادي للحاسب الآلي** :- يقصد بالكيان المادي "Hardware" لجهاز الحاسب الآلي هي الأجزاء الإلكترونية المكونة لهذا الجهاز التي تشغل حيزاً في الفراغ والداخلة في تركيب الحاسب مثل لوحة المفاتيح والشاشات والطابعات وأجهزة التشغيل المغناطيسية والراسمات.
ويتكون الكيان المادي "Hard ware" من عدة وحدات رئيسية :
- **وحدة المعالجة المركزية "**central processing" ويقصد بهذه الوحدة هي الوحدة الخاصة بمعالجة البيانات .
- **وحدة الإدخال** "Input unit " هي الوحدة الخاصة بإدخال البيانات إلى جهاز الكمبيوتر ، وتحتوي على العديد من الأدوات التي تستخدم لإدخال البيانات المختلفة مثل لوحة المفاتيح "key board" والفارة "mouse" والماسحة الضوئية "scanner"
- **وحدة الإخراج** "output unit" هي الوحدة الخاصة بإخراج البيانات من جهاز الكمبيوتر بأشكالها المختلفة ، مثل شاشة العرض أو المرقاب "monitor"والطابعة "printer" والسماعات "speakers" .
- **وحدة التخزين** "storage unit" هي الوحدة الخاصة بالتخزين الدائم للبيانات ونستخدمها لحفظ البيانات مثل القرص الصلب "Hard Disk" والقرص المرن "Floppy Disk" والفلاش ميموري " Flash memory" والقرص الضوئي أو المضغوط "C.D "
=(إيهاب أبو العزم ، الخطوة الأولى في عالم الكمبيوتر ، الطبعة الأولى ، دار الكتب العلمية للنشر والتوزيع ، القاهرة ، 2009 ، ص11.)

الحاسب الآلي أو تخريب الشبكات ، وهذا ما يمكن وصفه بأنه جريمة تقليدية ، لأن الاعتداء فيها يقع على مال مادي منقول ، وإما أن يكون الاعتداء واقعاً على الكيان المعنوي "المنطقي"[14] للحاسب الآلي ، مثل انتهاك المُلكية الفكرية ، وجرائم القرصنة وغيرها ، وهنا تثار إشكالية تتعلق بتطبيق النصوص الجنائية التقليدية عليها .

ثانياً . الاتجاه المضيق لتعريف الجرائم الإلكترونية :

على نقيض الاتجاه السابق ، يذهب جانب من الفقه إلى تعريف الجرائم الإلكترونية بأنها "كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية ، بقدر كبير لازماً لارتكابه من ناحية ، ولملاحقته وتحقيقه من ناحية أخرى"[15].

أو هي "الأفعال التي يرتكبها شخص على دراية بتقنية المعلومات"[16] .

يشترط وفقاً لهذين التعريفين ، لكي نكون بصدد جريمة إلكترونية ، أن يكون مرتكبها على دراية ومعرفة بتقنية المعلومات .

فتدمير أو إتلاف البيانات والمعلومات المخزنة ، أو المنقولة عبر الإنترنت ، أو تحويرها ، أو تعديلها يتطلب إرتكابها من شخص له دراسه ومعرفه بتقنية المعلومات .

---

[14] - **الكيان المعنوي للحاسب الآلي :** يقصد بالكيان المعنوي للحاسب "computer software" هي البرامج أو البرمجيات اللازمة لتشغيل الحاسب الآلي ، أو لحل مشكلة معينة التي يقوم الإنسان بكتابتها ، وتأخذ حيزاً في ذاكرة الحاسب الآلي ، حيث لايستطيع جهاز الحاسوب أن يعمل بدون هذه البرامج ، وهي التي تقوم بدور كبير في تسهيل التعامل مع هذه الأجهزة ، وتنقسم البرامج إلى نوعين رئيسيين كالتالي :

أ- **برامج النظم** "system programs" هذا النوع من البرامج يتم كتابته عن طريق مبرمجي النظم المتخصصين من قبل الجهة الصانعة للحاسب لمساعدة المستخدم والاستفادة منه على أفضل وجه ومن هذه البرامج مايلي :-

- **أنظمة التشغيل** "operating system" ووظيفتها التنظيم والتحكم في تشغيل جهاز الحاسب الآلي وتكون مخزنة داخل الحاسب حيث يمكن طلبها كلما دعت الضرورة إلى ذلك مثل برامج نظام التشغيل المسماه "Unix" والنوافذ" window "ودوس" Ms-Dos" التي تستخدم مع الأجهزة الشخصية .

- **لغات البرمجة** :توجد لغتين للبرمجة أحداهما ذات مستوى أدنى مثل لغة الآلة ، وأخرى ذات مستوى أعلى مثل لغة سي .

- **معالج اللغات** : ويقصد بها المترجم "compiler" والمفسر "interpreter" .

ب- **البرامج التطبيقية** "Application programs" هي التي يكتبها الإنسان بغرض حل بعض المسائل ، ومن أمثلة هذه البرامج برامج الإحصاء spss وبرنامج إعداد الميزانية ، وتنظيم الملفات ، وبرنامج حل المسائل الرياضية ، وتوجد هناك أيضاً برامج أخرى يطلق عليها البرامج الجاهزة التي تمكن المستخدم من استغلال إمكانيات عمل الحاسب على الوجه الأكمل ومنها :

- **برامج معالجة الكلمات** "word processing" وهي برامج تمكن المستخدم من كتابة النصوص مثل تحرير الرسائل والبحوث وتأليف الكتب وكذلك إضافة الكلمات والقص واللصق وغيرها ، وبالتالي تخزينها لكي تستخدم فيما بعد ومن أشهرها برنامج "windows"

- **برامج قواعد البيانات** "Date Base" ووظيفتها هي إدارة البيانات أو التعديل فيها أو البحث عن معلومات معينة أو محددة .

- **برامج الرسوم البيانية** "Graphics software" ووظيفتها مساعدة المتخصصين في مجال الهندسة المعمارية في تصميم الرسومات والأشكال التي يحتاجون إليها باستخدام الحاسب الآلي مثل برامج التصاميم الهندسية المعروف بـ "AutoCAD"

- **برامج الألعاب** "Games" ومهمة هذه البرامج تقديم العديد من الألعاب بالصوت والصورة ، مثل سباق السيارات ، ولعبة الشطرنج وغيرها .(بشير علي القائد ، مرجع سابق ، ص 38ومابعدها)

[15] نائلة عادل محمد فريد قوره ، جرائم الحاسب الآلي الاقتصادية (دراسة نظرية وتطبيقية) ، دارة النهضة العربية ، القاهرة ، 2004 ، ص28 .

[3] موسى مسعود أرحومة ، مرجع سابق ، ص85.

وقد عرفها أيضاً مكتب تقييم التقنية في الولايات المتحدة الأمريكية بأنها "الجرائم التي تلعب فيها البيانات الكمبيوترية ، والبرامج المعلوماتية دوراً رئيساً"[17] .

وكما هو ملاحظ من هذا التعريف ، أن الجرائم الإلكترونية تقتصر فقط على تلك الجرائم التي تقع على الحاسب الآلي أو على نظامه ، متمثلة في المعلومات المُخزنة داخله ، أو التي يتم تحويلها عن طريقه ، أما الجرائم التي لايكون الحاسب الآلي سوى وسيلة لإرتكابها فتخرج من نطاق الجرائم الإلكترونية ، والمثال على ذلك جريمة غسل الأموال عبر الإنترنت.

ونلخص مما سبق تعريفاً جامعاً للجرائم الإلكترونية ، والذي وضعه مؤتمر الأمم المتحدة لمنع الجريمة ومعاقبة المجرمين ، حيث عرفها بأنها "أية جريمة يمكن إرتكابها بواسطة نظام حاسوبي ، أو شبكة حاسوبية ، أو داخل نظام حاسوب ، وتشمل الجريمة من الناحية المبدئية جميع الجرائم التي يمكن إرتكابها في بيئة إلكترونية".[18]

ومن خلال الموازنة بين التعريفات السابقة نؤيد التعريف الاخير الذي وضعه مؤتمر الأمم المتحدة لمنع الجريمة ومعاقبة المجرمين ، لأنه لم يقتصر على جهاز الحاسوب فقط ، كموضوع للجرائم الإلكترونية ، بل يشمل أيضاً أي شبكة حاسوبية كالإنترنت وغير ذلك من وسائل تقنية المعلومات .

كما ان جهاز الحاسوب أو أي تقنية معلوماتية أخرى قد تكون وسيلة لتنفيذ الفعل الإجرامي .

الفرع الثاني

خصائص الجرائم الإلكترونية

تعتبر الجرائم الإلكترونيه من الجرائم التي تتسم بطبيعة خاصة تميزها عن غيرها من الجرائم التقليدية ، فهي تستهدف مكونات معنوية ، وليست مادية محسوسة ، مما يجعل منها ظاهرة إجرامية جديدة لم يعرفها العالم من قبل ، وسنبين هذه الخصائص التي ميزت بها الجرائم الإلكترونية على النحو الآتي :

---

[17] رشدي محمد علي محمد عيد علي ، الحماية الجنائية للمعلومات على شبكة الأنترنت ، رسالة دكتوراه ، كلية الحقوق ، جامعة القاهرة ، 2009 ، ص66.

[2] رامي متولي القاضي ، مكافحة الجرائم المعلوماتية في التشريعات المقارنة وفي ضوء الاتفاقيات والمواثيق الدولية ، دار النهضة العربية ، القاهرة ، 2011 ، ص23.

أولاً . أن وسائل تقنية المعلومات هي أداة ارتكاب الجرائم الإلكترونية :

تتميز الجرائم الإلكترونية بطبيعة خاصة ، تتمثل في أن ارتكاب هذه الجرائم يتم بواسطة جهاز الحاسب الآلي ، أو عبر شبكة الإنترنت ، وهذه تعتبر خاصية تنفرد بها الجرائم الإلكترونية عن غيرها من الجرائم الأخرى ، ذلك أن الحاسب الآلي هو الوسيلة الوحيدة التي يستطيع الشخص الدخول بها على شبكة الإنترنت وقيامه بتنفيذ جريمته ، وتعد شبكة الإنترنت هي الحلقة التي تربط بين كافة الأهداف المحتملة لتلك الجرائم ، كالشركات والمؤسسات المالية وغيرها من الأهداف التي غالباً ما تكون الضحية لتلك الجرائم. [19]

ثانياً . صعوبة اكتشاف الجرائم الإلكترونية :

تتميز الجرائم الإلكترونية بالغموض حيث يصعب إثباتها ، فالتحري عنها والتحقيق فيها ينطوي على العديد من المشاكل والصعوبات ، التي تواجه الأجهزة الأمنية والقضائية[20] مقارنة بعدد الحالات التي يتم إكتشافها في الجرائم التقليدية ، ويرجع ذلك إلى أن جوهر النشاط الإجرامي الذي تقوم به الجرائم الإلكترونية يقع على المكونات المعنوية ، مثل تغيير أو محو الأرقام والبيانات المُخزنة بأنظمة الحاسب الآلي[21] ، حيث يصعب في كثير من الأحيان العثور على أثر مادي للجرائم الإلكترونية ، ولعل السبب في ذلك يعود إلى أن السلوك الاجرامي فيها يتمثل بعمل سريع لايستغرق إلا بضع ثواني[22]،الذي يعقبه التلاعب وتدمير ومحو المعلومات التي يمكن استخدامها كدليل للاثبات [23]، علاوة على نقص المعارف التقنية لدى الجهاز الأمني والقضائي ضد هذه الظاهرة.[24]

ثالثاً . يتم ارتكاب الجرائم الإلكترونية بأقل عنف في التنفيذ :

لا تتطلب الجرائم الإلكترونية ، عنفاً لتنفيذها أو مجهوداً كبيراً ، فهي تنفذ بأقل جهد ممكن حيث يعتمد مقترفوها على أسلوب التضليل والخداع[25] ، مقارنة بالجرائم التقليدية التي تتطلب مجهوداً عضلياً ، والذي قد يكون في صورة ممارسة العنف والإيذاء كما هو الحال في جريمة القتل والسرقة. [26]

---

[19] منير محمد الجنبيهي ، وممدوح محمد الجنبيهي ، جرائم الإنترنت والحاسب الآلي ، دار الفكر الجامعي ، الإسكندرية ، 2004 ، ص14.

[20] محمود أحمد طه ، المواجهة التشريعية لجرائم الكمبيوتر والإنترنت ، دار الفكر والقانون ، المنصورة ، 2012 ، ص13.

[21] عادل يحيى ، السياسة الجنائية في مواجهة الجريمة المعلوماتية ، دار النهضة العربية ، القاهرة ، 2014 ، ص53.

[22] محمد علي سالم ، وحسن عبيد هجيج ، مرجع سابق ، ص92.

[23] عادل يحيى ، المرجع السابق ، ص53.

[24] صغير يوسف ، الجريمة المرتكبة عبر الانترنت ، رسالة ماجستير ، كلية الحقوق والعلوم السياسية ، جامعة مولود معمري ، 2013 ، ص20.

[25] محمد عبدالله أبوبكر سلامة ، جرائم الكمبيوتر والانترنت ، منشأة المعارف ، الاسكندرية ، 2006 ، ص97.

[26] صغير يوسف ، المرجع السابق ، ص16.

رابعاً . جريمة قد تكون عابرة للحدود :

تتميز الجرائم الإلكترونية بطابع خاص آخر ، وهي أنها عابرة للحدود ، فهي جرائم تنتقل من الحدود الجغرافية أو الوطنية للدولة ، إلى غيرها من الدول الأخرى ، وذلك بعد ظهور شبكة الإنترنت ، التي جعلت العالم قرية صغيرة حيث يمكن التحدث بين البشر ليس في دول مختلفة وإنما في قارات مختلفة في العالم في نفس الوقت على الشبكة المعلوماتية من خلال نظام الدردشة[27]، فغالبية الجرائم الإلكترونية يتم ارتكابها عبر شبكة الإنترنت ،وهو ما يثير في كثير من الأحيان الإشكاليات والتحديات القانونية ، التي من أهمها مسألة تحديد الاختصاص بنظر هذه النوعية من الجرائم ، والقانون الواجب التطبيق من بين قوانين الدول ، التي اقترفت الجريمة الإلكترونية على أراضيها عبر حدودها، وقبول الادلة المتحصلة عليها في دولة ما أمام قضاء دولة أخرى ، وهو ما تحتاج إلى تضافر الجهود الدولية بين مختلف الدول لمواجهة هذه الطائفة من الجرائم ومن ذلك على سبيل المثال اتفاقية الامم المتحدة للجريمة المنظمة عبر الوطنية . [28]

خامساً . التبليغ عن الجرائم الإلكترونية :

لا يتم في كثير من الأحيان ، التبليغ عن الجرائم الإلكترونية ، إما لعدم اكتشاف المجني عليه لها ، وإما حفاظاً على السمعة ، فالمجني عليه في الجرائم التقليدية كالضرب والسرقة يسارع بالإبلاغ عن هذه الجريمة ، أما المجني عليه في الجرائم الإلكترونية يصمت في غالب الأحيان عن الإبلاغ عنها ، وذلك في الحالات التي يكون المجني عليه هو الشخص المعنوي فالمؤسسات المالية وكذلك الشركات التجارية ، تخشى مجالس إداراتها الإبلاغ عن الجرائم الإلكترونية ، التي تعرضت لها حفاظاً على سمعتها ، وماتؤدي إليها الرعاية السلبية التي قد تنجم عن كشف هذه الجرائم إلى تضاؤل الثقة فيها من جانب المتعاملين معها وانصرافهم عنها[29] .

سادساً . عدم كفاية القوانين السارية في مواجهة الجرائم الإلكترونية :

لم تعد القوانين الجنائية التقليدية قادرة على مواكبة هذا التطور الهائل في النظم المعلوماتية ، وذلك نظراً للطبيعة الخاصة للجرائم الإلكترونية ، التي لم تكن موجودة من قبل مما يتطلب من المُشرّع إصدار قوانين حديثة لمواجهة هذه الجرائم مراعاةً لمبدأ الشرعية الجنائية[30] ، علاوة على ذلك أنه لا يوجد شعور عام بعدم أخلاقية السلوك أو النشاط الإجرامي الذي تقوم به الجرائم الإلكترونية ، ولعل ذلك ينبعث من أن كثير من العاملين في مجال تقنية المعلومات ينعدم

---

[27] منير محمد الجنيهي ، ممدوح محمد الجنبيهي ، مرج سابق ، ص15.

[28] محمد مسعود محمد خليفة ، الحماية الجنائية لمعطيات الحاسب الآلي ، رسالة ماجستير ، كلية الحقوق ، جامعة الإسكندرية ، 2005-2006 ، ص22.

[29] التحكم في جرائم الحاسوب وردعها "المراقبة الدولية للسياسة الجنائية" ، ترجمة د. عمر محمد بن يونس ، الطبعة الأولى ، دار النهضة العربية ، القاهرة ، 2005 ، ص29.

[30] صغير يوسف ، مرجع سابق ، ص 18-20.

لـديهم الشـعور بعـدم وجـود خطـأ فـي اسـتعمال شـفرات خاصـة بالـدخول إلـى أنظمـة الحواسـب الآلية[31]

الفرع الثالث

أهداف الجرائم الإلكترونية

هناك دوافع عديدة تحرك الجُناة لاقتراف الجرائم الإلكترونية ، ومن هذه الدوافع مايؤدي إلى تحقيق أغراض مادية مثل الحصول على كسب مالي ، ومنها ما يؤدي إلى تحقيق أغراض معنوية مثل الحصول على المعلومات التي تكون إما محفوظة على جهاز الحاسب الآلي أو تلك المنقولة عبر الإنترنت ، وقد تكون أيضاً من أجل الرغبة في الإنتقام ، أو تحقيق أهداف سياسية أو دينية أو عسكرية ، وهذا ماسوف نبينه على النحو الآتي :-

أولاً . السعي إلى تحقيق الكسب المالي :

يُعد هذا الدافع من أهم الدوافع ، وأكثرها تحريكاً للمجرم لارتكابه الجرائم الإلكترونية ، نظراً للربح المادي الكبير الذي يمكن أن يحققه هذا النوع من الأنشطة الإجرامية ، وغالباً مايكون الدافع لارتكاب هذه الجرائم هو وقوع الجاني في مشاكل مادية لعجزه عن سداد الديون المستحقة عليه ، حيث يسعى الجاني إلى الاحتيال ألمعلوماتي لسداد ديونه وذلك عن طريق التلاعب بالأنظمة المعلوماتية للبنوك ، بتحويل الأموال لحسابه الشخصي.[32]

ثانياً . الانتقام :

يُعد دافع الانتقام من أخطر الدوافع التي يمكن أن تدفع شخص ما إلى ارتكاب جرائمه بُغية الانتقام من غيره ، سواء كان من المنافسين له أو من رجال الأعمال أو من شخص يملك معلومات عن المؤسسة أو الشركة التي يعمل بها ، لأنه غالباً ما يكون أحد موظفيها ويقوم بهذا الدافع نظراً لفصله من العمل أو غير ذلك ، ومن هذه الجرائم جرائم إتلاف البيانات والبرامج بشتى الطرق بما في ذلك زرع الفيروسات. [33]

ثالثاً . الرغبة في قهر النظام والتفوق عليه بتعقيد الوسائل التقنية :

قد يكون الدافع من ارتكاب بعض هذه الجرائم الرغبة في قهر النظام أكثر من الرغبة في الحصول على الكسب المالي ، حيث يميل مقترفو هذه الجرائم إلى إظهار قدراتهم لدرجة أنه إذا ظهرت تقنية جديدة ، فإنهم يحاولون إيجاد الحلول المناسبة في التفوق على هذه التقنية الجديدة ، ويوجد هذا الدافع لدى صغار السن من مرتكبي الجرائم الإلكترونية الذين يمضون وقتاً طويلاً أمام حواسيبهم في محاولة التفوق ، وكسر كل حواجز الحاسب الآلي والانترنت [34]

---

(31) عادل يحيى ، مرجع سابق ، ص 55-56.
(32) صغير يوسف ، مرجع سابق ، ص 38-39.
(33) موسى مسعود أرحومة ، مرجع سابق ، ص88.
(34) محمود أحمد طه ، مرجع سابق ، ص16.

رابعاً . جمع المعلومات:

هناك من يقوم بارتكاب الجرائم الإلكترونية ، بُغية الحصول على الجديد من المعلومات وهؤلاء يقومون بالبحث واكتشاف الأنظمة المعلوماتيه ، والعمل من خلال الجماعة وتعليم بعضهم ، ويفضل هؤلاء القراصنة البقاء مجهولين أكبر وقت ممكن حتى يتمكنوا من الاستمرار في التواجد داخل الأنظمة ، ويدخر البعض منهم كل وقته في تعلم كيفية اختراق المواقع الممنوعة[35] ، ومعظم تلك الجرائم التي يكون الهدف منها جمع المعلومات هي في غالب الأعم تكون من الجرائم الاقتصادية، وذلك للحصول على مزايا أو مكاسب اقتصادية. [36]

خامساً . دوافع سياسية أو عسكرية أو دينية :

قد يكون الهدف من ارتكاب الجرائم الإلكترونية ، دوافع سياسية ، تتمثل في تهديد الأمن القومي ، وظهور ما يعرف بحرب المعلومات والإرهاب الإلكتروني ، والمثال على ذلك مايقوم به القراصنة من اختراق المواقع العسكرية[37] ، والسياسية بهدف الوصول إلى وثائق سرية ، ولعل أبرز مثال لتلك القرصنة ما قام به موقع "ويكيليكس" الشهير الذي نجح في تسريب مئات الآلاف من الوثائق الأمريكية السرية التي تتعلق برسائل ومكالمات ولقاءات مع قادة من مختلف الدول ، مما فتح ملفات سياسية شائكة ، وكذلك توجد دوافع دينية أو أيديولوجية لارتكاب تلك الجرائم ، ، والمثال على ذلك أن الإرهاب الإلكتروني كدعم الأفكار المتطرفة أو نشر الأفكار التي يمكن أن تؤدي إلى فكر تكفيري ، وتقديم معلومات مفصلة عن كيفية تصنيع قنابل يدوية الصنع قد تستخدم في الإرهاب الدولي والمحلي.

سادساً. الأشخاص أو الجهات :

قد يكون الدافع من ارتكاب الجرائم الإلكترونية هو إلحاق أذى بأشخاص أو جهات بعينها تتمثل في الحصول على البيانات والمعلومات الخاصة بتلك الجهات أو الأشخاص لاستخدامها في ارتكاب جرائم ابتزاز أو تهديد أو تشهير تجاههم [38] .

---

[35] صغير يوسف ، مرجع سابق ، ص40.

[36] منير محمد الجنبيهي وممدوح الجنبيهي ، مرجع سابق ، ص16.

[37] كشفت مجموعة الهاكرز الاوكراني "سايبر بيركوت" التي هاجمت موقع إحدى شركات الاسلحة الالكترونية أن هدف قطر من شراء اسلحة الدفاع الجوي نوع "بيتشورا" من كييف ، هو ضرب المقاتلات الروسية في سوريا(www.alalam.ir/News/177)

[38] إيهاب صلاح الدين "الجرائم الالكترونية " مجلة القضاء العسكري ، العدد الخامس عشر ، 2006 ، ص 46-47.

المطلب الثاني

أنواع الجرائم الإلكترونية وفئات المجرمين المعلوماتيين

إذا كان للتقنية المعلوماتية آثارٌ إيجابية ، تتمثل في إعادة هيكلية الدولة بمؤسساتها العامة والخاصة من النواحي الاقتصادية والاجتماعية والثقافية ، لتتجه نحو المعلوماتية فإن الأمر لم يخلُ كما سبق –القول– من الآثار السلبية ، والمتمثلة في إساءة استخدام الأنظمة المعلوماتية ، التي يترتب عليها ظهور أنماط مستحدثه من الجرائم أطلق على تسميتها بالجرائم الإلكترونية .

وقد لاقت الجرائم الإلكترونية اهتماماً محلياًَ ودولياً ، فعقدت المؤتمرات والندوات المختلفة ومن ذلك المؤتمر المغاربي الأول حول المعلوماتية والقانون الذي عقد بأكاديمية الدراسات العُليا بطرابلس 2009/10/28 تحت شعار "نحو قانون مغاربي نموذجي للمعلوماتية" ، والذي قدم فيه العديد من البحوث المتعلقة بجرائم الحاسوب والإنترنت[39] .

وكذلك المؤتمر السادس للجمعية المصرية للقانون الجنائي 1993/11/4م الذي تناول موضوع جرائم الحاسب الآلي والجرائم الأخرى في مجال تقنية المعلومات ، وهذا المؤتمر يعتبر تحضيراً للمؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات ، الذي عُقد في البرازيل 1994/9/8م ، والذي توصل فيها إلى توصيات حول جرائم الحاسب الآلي والإنترنت والتحقيق فيها ومراقبتها وضبطها ، وركز على ضرورة إدخال بعض التعديلات في التشريعات الجنائية لتواكب مستجدات هذه الجريمة[40] ، كما أن المجرم المعلوماتي ليس كغيره من الجُنّاة التقليديين ، بل يتمتع بقدرات ومهارات تقنية خاصة ودراية بكيفية تشغيل الحاسب الآلي.

وبناءً على ماتقدم سنقسم هذا المطلب إلى فرعين : نخصص الفرع الأول لدراسة أنواع الجرائم الإلكترونية . ونكرس الفرع الثاني لدراسة فئات المجرمين المعلوماتيين.

الفرع الأول

أنواع الجرائم الإلكترونية

تنقسم الجرائم الإلكترونية ، بحسب المصلحة المحمية قانوناً إلى جرائم الاعتداء على الأشخاص ، وجرائم الاعتداء على الأموال ، وكذلك جرائم الاعتداء على الآداب العامة وحقوق الملكية الفكرية ، وأيضاً جرائم الاعتداء على سريّة البيانات والنظم ، وذلك ماسنبينه في الفقرات التالية :

اولا . الجرائم الإلكترونية التي تمثل اعتداء على الأشخاص :

---

(1) Http//wwwpanapress.com

(40) محمد عبدالله المنشاوي "جرائم الإنترنت من منظور شرعي وقانوني" بدون ترقيم صفحات ، موقع المنشاوي للدراسات والبحوث على شبكة الإنترنت

Http//www.Minshawi.com/old/internet crime .

تتعدد صور جرائم الاعتداء على الأشخاص إلى جرائم اعتداء ضد حياة الأفراد وسلامتهم ، كجرائم القتل والإيذاء والجرح والضرب المفضي إلى الموت ، وإلى جرائم ضد الحرية والعرض كجرائم المواقعة وهتك العرض إلى غير ذلك من الجرائم [41] ، ومن الجرائم الإلكترونيه التي تمثل اعتداء على الاشخاص هي كالاتي :

أ) جرائم القتل والتهديد بالقتل :

يشير جانب من الفقه الجنائي ، إلى أن الحاسوب والإنترنت قد يكون أداة لارتكاب بعض الجرائم التقليدية ، فقد يستخدم أحياناً في ارتكاب جريمة القتل من خلال الدخول إلى البيانات المُخزنة والتلاعب ببرامجها ، ومثال ذلك تغيير المعلومات الطبية المتعلقة بملف المريض الخاص بتشخيص مرضه ، مما يؤدي إلى وفاته ، أو التحكم في السفينة أو الطائرة من خلال اقتحام البيانات المُخزنة والتلاعب بها مما يؤدي إلى تدميرها وقتل ركابها. [42]

ب) جريمة الاتجار في الجنس البشري عبر الانترنت :

هي كافة التصرفات غير المشروعة التي تحيل الانسان إلى مجرد سلعة أو ضحية يتم التصرف فيها بواسطة وسطاء ومحترفين عبر الحدود الوطنية ، بقصد استغلاله في اعمال ذات أجر متدن أو في اعمال جنسية أو ما شابه ، وسواء تم هذا التصرف بإرادة الضحية أو قسراً عنه أو بأي صورة أخرى من صور العبودية[43] ، وقد عاقب قانون جرائم المعلوماتية السوداني على الاتجار بالجنس البشري بموجب نص المادة (20) على أنه "كل من ينشئ أو ينشر موقعاً على شبكة المعلومات أو أخذ أجهزة الحاسب الآلي أو ما في حكمها بقصد الاتجار في الجنس البشري أو تسهيل التعامل فيه يعاقب بالسجن مدة لا تتجاوز عشر سنوات أو بالغرامة أو بالعقوبتين" وكذلك قانون نظام مكافحة جرائم المعلوماتية السعودي المادة (6) الفقرة (2) .

ج) جريمة الإرهاب الإلكتروني :

يقصد به الهجوم أو إقتحام المواقع[44] ونظم المعلومات ، التي تملكها الدولة بهدف شل حركتها الإدارية والعسكرية. [45]

---

[41] محمد رمضان باره ، القانون الجنائي الليبي، القسم الخاص بجرائم الاعتداء على الأشخاص ، الجزء الأول ، الطبعة الأولى الدار العربية للنشر والتوزيع ، القاهرة ، 2005 ، ص21.

[42] موسى مسعود أرحومة ، مرجع سابق ، ص 85-86.

[43] حسين الغافري ، الانترنت والاتجار بالبشر ، بدون ترقيم صفحات ، مقال منشور على الانترنت .
www.omanlegal.Net/vb/show thread.php?t=36 29 .

[44] **الموقع الإلكتروني**: يقصد به حسب نص المادة الأولى فقرة (9) من نظام مكافحة جرائم المعلوماتية السعودي الصادر بالمرسوم الملكي رقم (17) بتاريخ 1428.3.8 هـ بأنه "مكان إتاحة البيانات على الشبكة المعلوماتية من خلال عنوان محدد".

[45] أمير فرج يوسف ، الجرائم المعلوماتية على شبكة الإنترنت ، دار المطبوعات الجامعية ، الإسكندرية ، 2010 ، ص61.

د) **الجريمة المنظمة عبر شبكة الإنترنت :**

وهي الجريمة التي يستخدم فيها الجُناة شبكة الإنترنت لارتكاب جرائمهم ، وتعتبر عصابات المافيا من أشهر من قامت بالجريمة المنظمة ، حيث استفادوا من الإنترنت على تطوير وتحسين عملياتهم على مستوى العالم. [46]

هـ) جرائم السب والتشهير :

تعد جرائم السب والتشهير من الجرائم التي لها الأثر البالغ سلباً على شخصية الإنسان ، وهي من أكبر الجرائم التي تم تجريمها في كافة القوانين ، سواء في الدول العربية ، أو الدول الأجنبية ، أياً كانت الطريقة التي تتم بها الجريمة[47] سواء كانت تتم بالطرق التقليدية أو بالطرق الحديثة التي تتم باستخدام شبكة الانترنت.[48]

فقد جرم المُشرّع الليبي بموجب نص المادتين (438 ، 439) السب والتشهير دون تحديد للوسيلة التي ترتكب بها الجريمة ، إذ نصت الفقرة الثانية من المادة (439) عقوبات ليبي على أنه ".....وإذا حصل التشهير بالصحف أو غيرها من طرق العلانية أو في وثيقة عمومية تكون العقوبة الحبس الذي لايقل عن ستة أشهر".

ومن التشريعات التي نصت على تجريم التشهير الالكتروني قانون نظام مكافحة جرائم المعلوماتية السعودي حيث نصت المادة (3) فقرة (5) على أنه "يعاقب بالسجن مدة لا تزيد على سنه وبغرامه لا تزيد على خمسمئة الف ريال ، أو بإحدى هاتين العقوبتين ، كل شخص يرتكب جريمة التشهير بالآخرين ، وإلحاق الضرر بهم عبر وسائل تقنية المعلومات".

ثانياً . الجرائم الإلكترونية التي تمثل اعتداء على الأموال :

تُعد جرائم الأموال التي تتم باستخدام وسائل تقنية المعلومات ، هي أيضاً من أكثر الجرائم شيوعاً ، ومثال ذلك جرائم السرقة والتزوير والاحتيال المعلوماتي وجريمة غسل الأموال ، وتجارة المخدرات عبر الإنترنت وهذا ما سنبينه على النحو التالي :

أ) **سرقة الأجهزة أو المكونات أو المعلومات :**

نصت المادة [444] من قانون العقوبات الليبي على أن "كل من أختلس منقولاً مملوكاً للغير يعاقب بالحبس" كما يتضح من النص المذكور أعلاه ، أن أركان جريمة السرقة هي الاختلاس أي الفعل المادي ، ومحل الاختلاس أي المحل المادي من حيث كونه منقولاً مملوكاً للغير والركن المعنوي الذي يتخذ صورة القصد الجنائي. [49]

---

[46] منير محمد الجنبيهي ، وممدوح محمد الجنبيهي ، مرجع سابق ، ص72.

[47] مصطفى الشاذلي ، الجرائم الماسة بالشرف والاعتبار والآداب ، المكتب العربي الحديث ، الإسكندرية ، ص 173-174.

[48] فائزه يونس الباشا ، السياسة الجنائية لجرائم الكمبيوتر "نموذجاً مقارناً" ، الطبعة الأولى ، دار النهضة العربية ، القاهرة ، 2013 ، ص50.

[49] محمد رمضان باره ، القانون الجنائي الليبي ، القسم الخاص جرائم الاعتداء على الأموال ، الجزء الثاني ، مطابع عصر الجماهير ، الخمس ، 2002 ، ص55.

وهذه الأركان إن تحققت في جريمة السرقة التقليدية ، فهي لا تتحقق في جريمة سرقة المعلومات ، لأن الشيء موضوع الحيازة ، قد لا ينتقل من صاحبه ، فقد يتم تحميل أغاني بحظر ، بطريق النسخ على قرص مدمج ، الأمر الذي دفع جانب من الفقه الحديث إلى القول بأن المعلومات التي تحتويها أجهزة الحاسوب أو شبكة الإنترنت ، هي مواد لها قيمة مادية ، وهي قيم ترتبط بحقوق الغير ، حيث حُددت أنواع ثلاثة لجريمة السرقة غير التقليدية:

النوع الأول : يطلق عليه الالتقاط الذهني للبيانات سواء بالنظر أو الاستماع ، وقد عرّف نظام مكافحة جرائم المعلوماتية السعودي الصادر بتاريخ 1428/3/8هـ الالتقاط في المادة (1) فقرة (10) بأنها "المشاهدة أو الحصول على البيانات دون مسوغ قانوني".

النوع الثاني : يتعلق بالنسخ غير المشروع للبيانات المُخزنة إلكترونياً ، سواء عن طريق التعامل المباشر مع نظام الحاسوب المُخزنة فيه البيانات على هيئة نبضات كهربائية ، أو على وسائط التخزين الرئيسية .

النوع الثالث : يتحقق بالتعرض لمعطيات جهاز الحاسوب خلال نقلها أو التقاطها.[50]

ب) جريمة الاحتيال المعلوماتي :

يقصد بالاحتيال المعلوماتي ، هو الخداع أو الغش المعلوماتي الذي يقوم به الجاني بالتلاعب على نظم المعالجة الآلية للبيانات ، كإدخال بيانات غير صحيحة باستخدام اسم كاذب أو انتحال صفة غير صحيحة ، وذلك من أجل الحصول على خدمات أو أموال بدون وجه حق وفي هذا النوع من الجرائم يستخدم الجاني أجهزة دقيقة لتنفيذ فعله الإجرامي بهدف التلاعب في البيانات. [51]

ومن التشريعات التي جرمت الاحتيال المعلوماتي قانون جرائم المعلوماتية السوداني الصادر في 2007.6.20 في الفصل الثالث المتعلق بالجرائم الواقعة على الأموال والبيانات والاتصالات حيث نصت المادة (11) على أنه "كل من يتوصل عن طريق شبكة المعلومات أو أحد أجهزة الحاسوب وما في حكمها عن طريق الاحتيال أو استخدام اسم كاذب أو انتحال صفة غير صحيحة بغرض الاستيلاء لنفسه أو لغيره على مال أو سند أو توقيع للسند يعاقب بالسجن مدة لا تتجاوز أربع سنوات أو بالغرامة أو بالعقوبتين معاً" .

وكذلك من التشريعات التي نصت على تجريم هذا الفعل قانون جرائم أنظمة المعلومات الأردني رقم (30) لسنة 2010 المادة (6) فقرة (أ ، ب)، وقانون نظام مكافحة جرائم المعلوماتية السعودي المادة (4) فقرة (1 ، 2) ، وقانون الاتحادي رقم (2) لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات الإماراتي المادتين (10 ، 11) .

---

[50] فائزة يونس الباشا ، مرجع سابق ، ص41-42.

[51] عمر محمد بن يونس ، مرجع سابق ، ص41-42.

ج) جريمة التزوير المعلوماتي :

يعرف التزوير اصطلاحاً بأنه تغيير الحقيقة ، وهو جوهر السلوك الاجرامي في جريمة التزوير التقليدية التي تقع على محرر (مادي) بتغيير مضمونه[52] ، والفاعل في جريمة التزوير المعلوماتي ، يمكن أن يستخدم الحاسوب كوسيلة لارتكاب جريمة التزوير ، حيث ظهرت وسائل جديدة لتزوير المستندات تتخذ الشكل الليزري أسكنر (SCANNER) ، كما قد يكون الحاسوب هدفاً لتنفيذ الفعل الإجرامي ، وذلك عندما يتم تغيير بالإضافة أو الحذف أو التعديل البيانات المتواجدة في وثيقة مخزنة في جهاز الحاسوب ، فهذه تعتبر جريمة تزوير[53] .

والمثال على ذلك ما قام به بعض الأشخاص في ألمانيا من تلاعب في سجلات الشرطة بهدف حذف أسماء بعض الأشخاص المطلوب القبض عليهم[54] ، ومن التشريعات التي جرمت التزوير المعلوماتي قانون مكافحة جرائم تقنية المعلومات الإماراتي في المادة (4) حيث نصت على أنه "يعاقب بالسجن المؤقت كل من زور مستنداً من مستندات الحكومة الاتحادية أو المحلية أو الهيئات أو المؤسسات العامة الاتحادية والمحلية معترفاً به قانوناً في نظام معلوماتي....." وكذلك قانون العقوبات القطري رقم (11) لسنة 2004 والمتضمن فصل خاص بعنوان جرائم الحاسب الآلي حيث نصت المادة (380) منه على أنه "يعاقب بالحبس مدة لا تتجاوز خمس سنوات ، كل شخص أرتكب تزويراً في المستندات المعالجة آلياً ، أياً كان شكلها ترتب عليه الإضرار بالغير ، أو استعمل هذه المستندات المزورة مع علمه بذلك ، ويعد تزويراً كل تغيير في برامج الحاسب الآلي أو البرامج المسجلة على ذاكرته للحصول على نتائج غير صحيحة".

د) جريمة تجارة المخدرات عبر الإنترنت :

تعد جريمة الاتجار في المخدرات إحدى أقدم الجرائم المنصوص على تجريمها في كافة قوانين دول العالم[55] مما دفع العديد من المواطنين إلى الاهتمام بشؤون أبنائهم بعد انتشار ظاهرة المخدرات في العالم ، إلا أن هذا أصبح أمراً صعباً بعد استخدام الشبكة العالمية للإنترنت ، حيث أصبح في الإمكان لأي شخص أن يكتشف كيفية الحصول على المخدرات عن طريق الإنترنت ، مما أدى ذلك إلى سن بعض التشريعات تجريم الاتجار أو الترويج للمخدرات عبر شبكة الانترنت ، حيث نصت المادة (21) من قانون جرائم المعلوماتية السوداني على أنه "كل من ينشئ أو ينشر موقعاً على شبكة المعلومات أو أحد أجهزة الحاسوب أو ما في حكمها بقصد الاتجار أو الترويج للمخدرات أو المؤثرات العقلية أو ما

---

(52) علي عبدالقادر القهوجي ، الحماية الجنائية لبرامج الحاسب الآلي ، دار الجامعة الجديدة ، الإسكندرية ، 2010 ، ص 140.

(53) عبدالفتاح بيومي حجازي ، الجريمة في عصر العولمة ، الطبعة الأولى ، دار النهضة العربية ، القاهرة ، 2009-2010 ، ص126.

(54) محمد عبدالله ابوبكر سلامه ، مرجع سابق ، ص 143.

(55) منير محمد الجنبيهي ، وممدوح محمد الجنبيهي ، مرجع سابق ، ص 79.

فـي حكمهـا أو يسـهل التعامـل فيهـا يعاقـب بالسجـن مـدة لا تتجـاوز سـنة أو بالغرامـة أو بالعقوبتين معاً".

ومن التشريعات الأخرى التي جرمت الاتجار بالمخدرات عبر الإنترنت قانون مكافحة جرائم تقنية المعلومات الإماراتي المادة (18) ، وقانون نظام مكافحة جرائم المعلوماتية السعودي المادة (6) فقرة (4) .

هـ) جريمة غسل الأموال عبر الإنترنت :

يقصد بجريمة غسل الأموال أنها "مجموعة من الآليات أو الحيل التي يتم اللجوء إليها بهدف إخفاء أو تمويه مصدر الأموال المتحصلة من أنشطة غير مشروعة".

ومع تفجر ثورة الاتصالات في العالم وظهور شبكة الإنترنت كان من المعقول أن يواكب غاسلو الأموال استخدام شبكة الإنترنت وذلك بهدف تطوير أساليبهم الإجرامية لتسهيل عمليات غسل الأموال بين الدول،ومن أبرز الوسائل التقنية المتقدمة في غسل الأموال الخدمات المصرفية الإلكترونية[56]و التجارة الإلكترونية ، فالتجارة الالكترونية مثلاً قد ساعدت كثيراً في عمليات غسيل الأموال ، نظراً لسرعة الاتفاق على الصفقات ، وإتمامها عبر الاتفاق على خطوات ، وترتيبات تنفيذها عبر الانترنت وبطريقة معقدة[57] مما دفع العديد من التشريعات إلى تجريم غسيل الاموال عبر الانترنت، فقد نصت المادة (22) من قانون جرائم المعلوماتية السوداني على أنه "كل من يقوم بعملية غسيل الاموال بالتسهيل أو التحويل أو الترويج أو إعادة تدويرها بواسطة شبكة المعلومات أو أحد أجهزة الحاسوب أو ما في حكمها ، ليكسبها الصفة القانونية مع علمه بأنها مستمدة من مصدر غير مشروع ، يعاقب بالسجن مدة لاتتجاوز عشر سنوات أو بالغرامة أو بالعقوبتين معاً" ومن التشريعات الأخرى التي جرمت غسيل الأموال عبر الانترنت قانون مكافحة جرائم تقنية المعلومات الإماراتي المادة (19) .

وباستقراء قانون رقم (2) لسنة 2005 بشأن مكافحة غسل الأموال ، تبين أن المُشرّع الليبي لم ينص صراحةً على تجريم غسل الأموال عبر الأنترنت ، إلا أن المفهوم من نص المادة (1) فقرة (10) من هذا القانون على تعريف الوسائط ، بأنها أي وسيلة تستخدم أويراد استخدامها بأي وجه في ارتكاب جريمة من الجرائم المنصوص عليها في القانون ، فاستخدام المُشرّع مصطلح أي وسيلة يدخل في مضمونها ارتكاب جريمة غسل الأموال عبر الانترنت.

---

[56] موسى مسعود أرحومة "ظاهرة غسل الأموال والجهود الدولية لمواجهتها" مجلة قاريونس العلمية ، السنة الخامسة عشر ، الأعداد الأول والثاني والثالث والرابع ، 2002 ، ص 107-124.

[57] منير محمد الجنبيهي ، وممدوح محمد الجنبيهي ، مرجع سابق ، ص80.

ثالثاً . الجرائم الإلكترونية التي تمثل الاعتداء على الآداب العامة وحقوق الملكية الفكرية :

أ) جرائم الاعتداء على الآداب العامة :

إن الإنترنت هي إحدى وسائل الاتصال التي تسهل ارتكاب الجرائم ذات الصبغة الجنسية ، مثل الصور والأفلام غير الأخلاقية التي تهدم القيم لدى المجتمع بصفة عامة والأطفال بصفة خاصة ، وللتصدي لهذه الظاهرة يجب أن تكون شبكة الانترنت مزودة ببرامج معينة تمنع ظهور المواد غير المرغوب فيها[58] ، ولقد بادرت دول ومنها ليبيا وتونس بعد ثورات الربيع العربي إلى إغلاق هذه المواقع الإباحية ، في حين ارتأت بعض الدول قصر الحماية على القاصرين فقط[59] .

ومن التشريعات التي جرمت نشر المطبوعات والأفلام المُخلة بالاداب العامة عبر شبكة الإنترنت قانون جرائم المعلوماتية السوداني ، حيث نصت المادة (14) على أنه "1-كل من ينتج أو يعد أو يهيئ أو يرسل أو يخزن أو يروج عن طريق شبكة الإنترنت أو أحد أجهزة الحاسوب أو ما في حكمها أي محتوى[60] ، مُخل بالحياء أو النظام العام أو الآداب ، يعاقب بالسجن مدة لا تتجاوز خمس سنوات أو بالغرامة أو بالعقوبتين معاً.2-كل من يوفر أو يسهل عمداً أو بإهمال عن طريق شبكة المعلومات أو أحد أجهزة الحاسوب ، أو ما في حكمها للوصول لمحتوى مُخل بالحياء أو منافي للنظام العام أو الآداب ، يعاقب بالسجن مدة لاتتجاوز أربع سنوات أو بالغرامة أو بالعقوبتين معاً"،وكذلك قانون نظام مكافحة جرائم المعلوماتية السعودي المادة (6) فقرة (3) .

ب) جرائم الاعتداء على حقوق الملكية الفكرية والأدبية :

من الجرائم التي انتشرت أيضاً ، وبصورة خطيرة ، في الآونة الأخيرة ، جرائم الاعتداء على حقوق الملكية الأدبية والفكرية بواسطة استخدام الحاسبات الآلية وشبكة الإنترنت ، والاعتداء على الحقوق الأدبية والفكرية ، أو ما أصطلح على تسميته "بحقوق المؤلف" لا ينبغي الخلط بينه ، وبين الاعتداء على الملكية الأدبية والفكرية التي تنصب على البرامج والمعلومات في مجال المعلوماتية ، وتكنولوجيا المعلومات ، فهذه الأخيرة الملكية الأدبية والفكرية تنصب على البرامج ونظم المعلومات بصفة عامة ، أما الاعتداء على الحقوق الفكرية والأدبية فهو يقع دائماً على العناصر غير المادية لنظام المعلوماتية ، والمثال على ذلك حالة تخزين معلومات

---

[58] جميل عبدالباقي الصغير ، الانترنت والقانون الجنائي ، دار النهضة العربية ، القاهرة ، 2012 ، ص52.

[59] فائزة يونس الباشا ، مرجع سابق ، ص48.

[60] **المحتوى** :"هو المادة الإلكترونية سواء كان ذلك المحتوى نصاً أو صورة أو صوتاً أو فيديو وما في حكمها" المادة (3) من قانون جرائم المعلوماتية السوداني" .

على حاسب معين ثم يقوم المسؤول عن هذا التخزين باستخدام هذه المعلومات بدون إذن صاحبها[61] .

ويتخصص في ارتكاب جريمة الاعتداء على حقوق الملكية الفكرية والأدبية "القرصنة المعلوماتية" قراصنة المعلوماتية أو الهاكرز، وهم أشخاص على درجة عالية من الإلمام بتقنية المعلومات.[62]

ومن التشريعات التي نصت على تجريم الاعتداء على حقوق الملكية الفكرية والأدبية قانون جرائم المعلوماتية السوداني المادة (19) حيث نصت على أنه "كل من ينشر دون وجه حق عن طريق شبكة المعلومات أو أحد أجهزة الحاسوب أو ما في حكمها أي مصنفات فكرية أو أدبية أو أبحاث علمية أو ما في حكمها يعاقب بالسجن مدة لا تتجاوز سنة أو الغرامة أو العقوبتين معاً" .

رابعاً . جرائم الاعتداء ضد سرية البيانات والنظم :

أ) جريمة الدخول غير المشروع :

إن استخدام الشخص للحاسوب والدخول إلى شبكة الإنترنت للحصول على الخدمة يتطلب ترخيصاً من الجهة المعنية بإعطاء هذه الصلاحية سواء كانت جهة عامة أو خاصة ، مما يتطلب الالتزام بالضوابط والأسس المقررة بكيفية الدخول إلى الحاسب الآلي أو الإنترنت ، وإلا سيتعرض المخالف للمساءلة الجنائية لدخوله إلى الشبكة بدون إذن أو ترخيص.

وقد عرف نظام مكافحة جرائم المعلوماتية السعودي الدخول غير المشروع في المادة (1) فقرة (7) بأنه "دخول شخص بطريقة متعمدة إلى حاسب آلي أو موقع إلكتروني أو نظام معلوماتي أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها" .

ولقد ميز الفقه[63] بين الدخول المادي الذي يكون بإدخال شيء ما داخل الجهاز بطريقة غير مشروعة وبين مصطلح الدخول المعنوي (المنطقي) الذي يتحقق بالدخول إلى النظام بواسطة الاستخدام غير المشروع لأحد خطوط الجهاز أو بانتحال صفة شخص آخر أو استخدام كلمة السر.[64]

كما نصت اتفاقية بودابست المبرمه في 2001/11/23م لمكافحة الجرائم المعلوماتية على هذه الجريمة بموجب نص المادة (2) على أنه "يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أية إجراءات يرى أنها ضرورية من أجل اعتبارها جريمة جنائية وفقاً لقانونه الداخلي للولوج العمدي لكل جزء من جهاز الحاسب الآلي بدون حق، كما يمكن أن يشترط أن ترتكب

---

[61] محمد عبدالله ابوبكر سلامه ، مرجع سابق ، ص 193-194.

[62] فائزة يونس الباشا ، مرجع سابق ، ص44.

[63] فائزة يونس الباشا ، المرجع السابق ، ص20.

[64] ومن التطبيقات العملية لجريمة الدخول غير المشروع حيث تم ضبط موظف سابق بأحد البنوك الفيدرالية قام بالدخول إلى النظام المعلوماتي الخاص بهذا البنك باستخدام كلمة السر (Password) والتي حصل عليها من زميل سابق له وقد نجح في التقاط المعلومات المالية المخزنة فيه ونقلها إلى رئيسه الجديد في العمل حتى يستفيد منها . (عبدالفتاح بيومي حجازي ، الجريمة في عصر العولمة ، مرجع سابق ، ص 81-85) .

الجريمة من خلال إنتهاك إجراءات الأمن بنية الحصول على بيانات الحاسب أو أية نية إجرامية أخرى أو ترتكب الجريمة في حاسب آلي يكون متصلاً عن بعد بحاسب آخر".

وكما هو ملاحظ من نص المادة الثانية من اتفاقية بودابست ، أنها تحث الدول على أن تجرم بموجب قوانينها الداخلية ، الحصول على كل جزء من نظام الكمبيوتر من دون وجه حق ، وأن ترتكب الجريمة عمداً ، وخولت كذلك أي طرف أن يشترط أن تكون الجريمة قد ارتكبت عن طريق انتهاك الإجراءات الأمنية بقصد الحصول على بيانات جهاز الحاسب الآلي أو غيرها بسوء النية.[65]

ومن التشريعات العربية التي جرمت فعل الدخول غير المشروع قانون مكافحة جرائم تقنية المعلومات الإمارتي المادة (2) ، وقانون جرائم المعلوماتية السوداني المواد (4 ، 5 ، 7 ، 8) ، وقانون جرائم المعلومات الأردني المادة (3) .

ب) جريمة الاعتراض غير القانوني :

يقصد بجريمة الاعتراض غير القانوني هو التنصت أو نقل البيانات التي تتم داخل جهاز الحاسب الآلي ، والتي تتم عبر جهازين عن بعد عبر الشبكات المعلوماتية المختلفة ، أوبترجمة الإنبعاثات الكهرومغناطيسية الصادرة من الحاسب إلى البيانات أو التي تتم عبر الأجهزة اللاسلكية ، وذلك عن طريق أي من الوسائل الفنية الغير علنية ، وينطبق هذا الوصف الإجرامي على كل أشكال النقل الإلكتروني للبيانات سواء تم عن طريق التليفون أوالفاكس أو البريد الإلكتروني.[66]

وقد نصت المادة (6) من قانون جرائم المعلوماتية السوداني على أنه "كل من يتنصت لأي رسائل عن طريق شبكة المعلومات أو أجهزة الحاسوب ، وما في حكمها أو يلتقطها أو يعترضها دون تصريح بذلك من النيابة العامة أو الجهة المختصة أو الجهة المالكة للمعلومة ، يعاقب بالسجن مدة لا تتجاوز ثلاث سنوات أو بالغرامة أو بالعقوبتين معاً ."

كما نصت المادة (3) من اتفاقية بودابست المتعلقة بمكافحة الجرائم المعلوماتية على أنه "يجب على كل طرف أن يتبنى الإجراءات التشريعية ، وأية إجراءات أخرى يرى أنها ضرورية من أجل اعتبارها جريمة جنائية ، وفقاً لقانونه الداخلي واقعة الاعتراض العمدي بدون حق ، من خلال وسائل فنيه للإرسال غير العلني ، لبيانات الحاسب في مكان الوصول في المنشأ ، أو في داخل النظام المعلوماتي بما في ذلك الإنبعاثات الكهرومغناطيسية من جهاز حاسب يحمل هذه البيانات

---

[65] هلالي عبداللاه أحمد ، مرجع سابق ، ص249.
[66] نائلة عادل محمد فريد قورة ، مرجع سابق ، ص350.

، كما يمكن لأي طرف أن يستوجب أن ترتكب الجريمة بنية إجرامية بقصد الغش أو أن ترتكب الجريمة في حاسب آلي يكون متصلاً عن بعد بحاسب آخر."[67]

ونلاحظ مما تقدم أن الأعتراض الغير قانوني قد يتم باستخدام وسائل فنية تتعلق بالتنصت أو مراقبة مضمون الاتصالات والحصول على المحتوى بطريقة مباشرة من خلال الدخول إلى النظام المعلوماتي ، أو بطريقة غير مباشرة عن طريق استخدام أجهزة التنصت، كذلك يمكن أن تشمل وسائل الاعتراض الأجهزة الفنية المتصلة بخطوط النقل أو الإتصال مثل الأجهزة اللاسلكية ، كما نجد أن اتفاقية بودابست تحث الدول على أن تجرم وفقاً لقانونها الداخلي واقعة الاعتراض الغير قانوني بدون حق ، وأن ترتكب الجريمة عمداً ، ورخصت كذلك أي طرف أن يشترط أن تكون الجريمة قد ارتكبت بقصد الغش ، أو أن ترتكب الجريمة في حاسب آلي يكون متصلاً عن بعد بحاسب آخر.

ج) جريمة الاعتداء على سلامة البيانات وإعاقة النظام :

ويقصد بها إتلاف البيانات والمعلومات بواسطة إرسال برامج مشفره مصممه بقدرة على الانتشار من أي مكان إلى آخر ، أو من حاسب إلى حاسب من خلال اندماجها في برنامج سليم وتخترق كافة الحواجز من خلال التقاط كلمة السر[68] ، والهدف من اختراقها تدمير البيانات والمعلومات والبرامج المخزنة داخل جهاز الحاسب الآلي ، وتعطيل شبكة المعلومات كلياً وقد يكون جزئياً ، ويطلق عليه في هذه الحالة "تشويه أو تعييب أو إعاقة النظام" ويتمثل في ادخال فيروس داخل الجهاز بحيث يعمل على التقليل من كفاءته أو يبطئ حركة الجهاز ذاته[69]ومن أمثلة إعاقة النظام بطريقة مادية أعمال العنف المادية التي تقع على أجهزة الحاسب الآلي وشبكات الاتصال عن طريق تخريبها بكسرها أو منع العاملين في النظام من العمل[70] وهناك العديد من برامج الفيروسات التي تؤثر على النظام المعلوماتي وهي كالآتي :

1- فيروس حصان طروادة :

وهي عبارة عن برامج فيروسية لديها القدرة على الإختفاء داخل برامج أخرى أصلية للمستخدم بحيث عندما تعمل البرامج الأصلية ينشط الفيروس ، وينتشر ليبدأ أعماله التخريبية وهو يؤدي إلى تعديل البرنامج وتزوير المعلومات ومحو بعضها ، وقد يصل إلى تدمير النظام بالجملة. [71]

2- فيروس الدودة المعلوماتية :

---

[67] هلالي عبداللاه أحمد ، مرجع سابق ، ص252.
[68] محمد مسعود محمد خليفة ، مرجع سابق ، ص30.
[69] محمد عبدالله ابوبكر سلامه ، مرجع سابق ، ص152.
[70] عبدالفتاح بيومي حجازي ، الجريمة في عصر العولمة ، مرجع سابق ، ص89.
[71] عطا عبدالعاطي محمد السنباطي ، موقف الشريعة الاسلامية من جرائم الحاسب الآلي والانترنت ، الطبعة الأولى ، دار النهضة العربية ، القاهرة ، 2002 ، ص31.

وهي عبارة عن برامج لديها إمكانية تعطيل أو إيقاف نظام الحاسوب كُلياً ، وذلك عن طريق وجود أي خلل أو فجوة في نظام تشغيل الحاسوب ، لكي تنتقل من حاسب لآخر أو من شبكة لأخرى عبر الوصلات التي تربط بها[72] .

3- فيروس القنبلة المعلوماتية :

وهي عبارة عن برامج تنفذ في لحظة محدودة ، أو في زمن معين ، ويتم وضعه في شبكة معلوماتية بهدف تحديد ظروف النظام لغرض تسهيل تنفيذ عمل غير مشروع. [73]

ولا أهمية لنوع الفيروس متى أستهدف تدمير النظام المعلوماتي سواء بصورة كاملة أو جزئية ، وهو ما يعتبر اعتداء على الأموال المعلوماتية المملوكة للغير سواء بإتلافها أو تدمير المعلومات أو محوها أو تعديلها أو نقلها. [74]

ويعتبر هذا السلوك مُجرّم بموجب القانون الفرنسي الصادر في 5/يناير/سنة1988 ، والمعدل بقانون 1994 المتعلق بجرائم الغش المعلوماتي ، ومنها جريمة إتلاف النظم المعلوماتية والبيانات التي نصت عليها المادة (462) فقرة (2 ، 3) والتي حلت محلها المادة (323) فقرة (2 ،3) من قانون 1994 التي نصت على تجريم كل تغيير أو إتلاف أو تبديل أو تحريف أو تعديل لبيانات الحاسب الآلي [75] .

ومن التشريعات الاخرى التي جرمت الاعتداء على سلامة البيانات وإعاقة النظام قانون مكافحة جرائم تقنية المعلومات الإماراتي المادة (2) وقانون نظام مكافحة جرائم المعلوماتية السعودي المادة (5) وقانون جرائم المعلوماتية السوداني المواد (8 ، 9) ، كما تجد هذه الجريمة صداها في اتفاقية بودابست المواد (4 ، 5) .

---

[72] هدى حامد قشقوش ، جرائم الحاسب الإلكتروني في التشريع المقارن ، دار النهضة العربية ، القاهرة ، ص 104.

[73] محمد عبدالله أبوبكر سلامه ، مرجع سابق ، ص153.

[74] فائزة يونس الباشا ، مرجع سابق ، ص28.

[75] في فرنسا قام محاسب من الخبراء في نظم المعلومات ، وبدافع الانتقام على أثر فصله من المنشأة التي يعمل بها بوضع قنبلة زمنية في شبكة المعلومات الخاصة بتلك المنشأة ، بحيث تنفجر تلك القنبلة بعد مضي ستة أشهر من رحيله عن المنشأة ، وترتب على ذلك أن حدث إتلاف لكل البيانات الخاصة بها .
(بلال أمين زين الدين ، جرائم المعلوماتية في التشريع المقارن والشريعة الاسلامية ، دار الفكر الجامعي ، الاسكندرية ، 2014 ، ص 319-320.) .

د) جريمة إساءة استخدام الحاسب الآلي :

نصت المادة السادسة من الاتفاقية الأوروبية المتعلقة بالإجرام المعلوماتي على أنه "يجب على كل طرف أن يتبنى الإجراءات التشريعية وأية إجراءات أخرى يرى أنها ضرورية للتجريم تبعاً لقانونه الداخلي القيام عمداً ودون حق ما يلي :

1- إنتاج أو بيع أو الحصول من اجل الاستخدام أو الاستيراد أو نشر أو أي أشكال أخرى للوضع تحت التصرف :

- أي جهاز يحتوي على برنامج معلوماتي مصمم أو موفق بشكل أساسي لغرض ارتكاب إحدى الجرائم المنصوص عليها وفقاً للمواد من (2 : 5) السابق الإشارة إليها .

- كلمة المرور أو شفرة الدخول أو أي بيانات متماثلة تسمح بالولوج إلى كل أو جزء من نظام الحاسب الآلي بنية استخدامها لارتكاب جريمة من الجرائم المشار إليها في المواد (2 :5) ، ويمكن لأي طرف أن يشترط في قانونه الداخلي وجود بعض هذه العناصر من أجل تقرير المسؤولية الجنائية ، كما تشير هذه المادة إلى ضرورة ألا يكون لجوء الشخص إلى هذه التصرفات بحق.

2- حيازة أي عنصر من العناصر المشار إليها في البندين (1/أ ، ب) بنية استخدامه في ارتكاب أي جريمة من الجرائم الواردة في المواد (2 : 5)

ويتبين من سياق هذه المادة أن الاتفاقية لم تكتفِ بالنص على تحديد الأفعال المجرمة والنص على كيفية مواجهتها ، والتي تمثل اعتداء على نظام المعالجة الآلية للبيانات ، وذلك لتوقيع العقاب ضد من يرتكب أياً من هذه الأفعال ، بل اتجهت هذه المادة إلى قفل الطرق التي قد تؤدي إلى ارتكاب الجرائم الإلكترونية بنصها على تجريم أي من الأفعال المحددة ، إذا كان الهدف منها هو ارتكاب الجرائم التي حددتها الاتفاقية بالتجريم والعقاب ، كالولوج غير المشروع أو الاعتراض الغير قانوني أو الاعتداء على سلامة البيانات وإعاقة النظام ، ولقد أراد الأعضاء بالاتفاقية استعمال وسائل وقائية للحيلولة دون وقوع الجريمة الإلكترونية ، وذلك بمنع حيازة أو إنتاج أو بيع أو شراء أو أي شكل من أشكال التصرف ، ويقصد بالنشر المشار إليه في هذه الاتفاقية هو نقل البيانات إلى الآخرين ، بينما يقصد بالوضع تحت التصرف هي وضع أجهزة على الخط المتصل بالشبكات المعلوماتية ليتم استخدامها بواسطة الغير.[76]

ويتبين لنا مما تقدم ، مدى لزومية وسائل تقنية المعلومات في الجرائم الإلكترونية ، فهو إما أن يكون أداة لارتكاب بعض الجرائم كجريمة الاحتيال المعلوماتي ، وجرائم القتل ، كما قد تكون وسائل تقنية المعلومات هدفا أو موضوعاً للجرائم الإلكترونية ، كما في حالة الدخول غير

---

[76] بلال أمين زين الدين ، مرجع سابق ، ص 367-368.

المصرح به والاعتراض غير القانوني ، والاعتداء على سلامة البيانات وإعاقة النظام ، كما قد تكون وسائل تقنية المعلومات بيئة للجريمة وذلك كما في حالة تخزين برامج القرصنة فيه أو في حالة استخدامه لنشر المواد غير القانونية أو استخدامه أداة اتصال لصفقات ترويج المخدرات، كما قد تكون وسائل تقنية المعلومات وسائل لكشف الجرائم الإلكترونية .

الفرع الثاني

فئات المجرمين المعلوماتيين

إن فكرة المجرم المعلوماتي[77] فكرة جديدة على الفقه الجنائي ، لأن المجرم المعلوماتي ليس كغيره من الجُناة التقليديين ، بل يتمتع بقدرات ودراية تقنية خاصة بكيفية تشغيل الحاسب الآلي ، كما يتمتع بالقدرة على اختراق الكودات السرية للبرامج والبيانات ، والمعلومات ، وبالتالي يمكننا تصنيف المجرمين المعلوماتيين إلى الفئات التالية :

أولاً . القراصنة :

يوجد نوعان من القراصنة هما :

أ) الفضوليين أو الهواة:

وهم من الشباب صغار السن والمراهقين المولعين بالمعلوماتية والحاسب الآلي الذين لديهم قدرة من المهارة في استخدام هذه التقنية العالية ، ويسعون عادةً إلى مجرد التسلية وإظهار مقدرتهم على تحدي النظام[78] ، وهؤلاء لايشكلون خطورةً على أنظمة المعلومات ، لأن الباعث لديهم في ارتكاب الجرائم الإلكترونيه لا يتعدى الرغبة في الاستطلاع والاستكشاف.[79]

ب) المحترفون :

ويقصد بهم ذوي النوايا الإجرامية في الإتلاف أو التخريب باستخدام الفيروسات ، وهم يتميزون بأنهم من أصحاب التخصصات العالية[80] ، حيث تهدف اعتداءاتهم بالأساس إلى تحقيق الكسب المالي لهم ، أو الجهات التي كلفتهم لارتكاب الجرائم الإلكترونيه ، كما تهدف اعتداءات بعضهم إلى تحقيق أغراض سياسية.[81]

---

[77] توجد عدة مصطلحات للمجرم المعلوماتي ، فتارةً يسمى بالهاكر (haker) وتارةً أخرى يسمى (cracker) وهو الهاكر سيء النية ، ويطلق عليه أيضاً تافهي العالم الافتراضي (cyber punks) وكذلك المجرم التقني أو مجرم الانترنت ، كما اطلق عليه ايضاً مصطلح القرصان (pirate) كما ارتبط ايضاً بمصطلح المخترق (رشدي محمد علي محمد عيد علي ، مرجع سابق ، ص72) .

[78] موسى مسعود أرحومة ، السياسة الجنائية في مواجهة جرائم الانترنت ، مرجع سابق ، ص86.

[79] محمد مسعود محمد خليفة ، مرجع سابق ، ص19.

[80] رشدي محمد علي محمد عيد علي ، المرجع السابق ، ص74.

[81] محمد مسعود خليفة ، المرجع السابق ، ص19.

ثانياً . المجرمون الحاقدون :

وهم الذين تحركهم لارتكاب جرائمهم الرغبة بالانتقام من أرباب الأعمال الذين يعملون عندهم ، ولا يتسم هؤلاء المجرمون بالمعرفة التقنية الاحترافية ، ومع ذلك لكي يقوم بارتكاب جريمته عليه الإلمام بكافة عناصر المعرفة المتعلقة بالفعل الذي ينوي ارتكابه ، وأن هذه الطائفة من المجرمين لا يتفاخرون بأنشطتهم بل يعمدون إلى إخفائها. [82]

ثالثاً . المحتالون :

ويتمتع هؤلاء بقدرات عالية من المهارة ، باعتبارهم عادةً من المختصين في مجال تقنية المعلومات ، وتنصب معظم جرائمهم على تحويل الأموال بإساءة استخدام بطاقات الائتمان ، ويمكنهم التلاعب بحسابات المصارف أو فواتير الكهرباء والهاتف ، أو ما شابه.

رابعاً . الجواسيس :

ويهدف هؤلاء إلى الحصول على بعض المعلومات والبيانات ، من خلال اقتحام النظم المعلوماتية لمصلحة دولهم ، أو لمصلحة بعض الدول الأخرى أو الجهات كالشركات التي تتنافس فيما بينهم[83] .

وعليه يمكن أن نقول بأن المجرم المعلوماتي ، قد يكون من المختصين الذين تتوافر لديهم قدرة ومهارة عالية في استخدام وسائل تقنية المعلومات لاقترافهم الجرائم ، كما قد يكون هؤلاء المجرمين من الذين ليس لديهم إلا قدر محدود من الدراية والمهارة بوسائل تقنية المعلومات لكي يقوموا بارتكاب جرائمهم .

---

[82] محمود أحمد طه ، مرجع سابق ، ص15.

[83] رامي متولي القاضي ، مرجع سابق ، ص54.

المبحث الثاني
ماهية الدليل الرقمي

نظراً للطبيعة الخاصة التي تتسم بها الجرائم الإلكترونية ، فإن إثبات هذا النوع من الجرائم يحيط به كثير من الصعوبات ، تتجلى في أن اكتشافها يحتاج إلى طرق أو وسائل إلكترونية تصلح لأن تكون أدلة إثبات لهذا النوع من الجرائم ذات الطبيعة الخاصة الفنية منها والعلمية ، وتدعى هذه الوسيلة بالدليل الرقمي باعتباره الوسيلة الوحيدة والرئيسية لإثبات هذه الجرائم لذا سنقسم هذا المبحث إلى مطلبين : نخصص المطلب الأول للتعريف بالدليل الجنائي بصفة عامة . ونكرس المطلب الثاني للتعريف بالدليل الرقمي.

المطلب الأول

التعريف بالدليل الجنائي

سنتناول في هذا المطلب تعريف الدليل الجنائي ، وبيان خصائصه وتقسيماته وذلك من خلال ثلاثة فروع : نخصص الفرع الأول لتعريف الدليل الجنائي . ونكرس الفرع الثاني لبيان خصائص الدليل الجنائي . ونفرد الفرع الثالث لتقسيمات الدليل الجنائي.

الفرع الأول

تعريف الدليل الجنائي

سنتناول في هذا الفرع تعريف الدليل لغةً واصطلاحاً وذلك على النحو الآتي :

أولاً ـ الدليل لغـةً :

الدليل جمع أدلة ، وهو ما يستدل به ، والدليل الدال أيضاً وهو (دلة) على الطريق يدله.[84]

ثانياً . الدليل في الإصطلاح القانوني :

هو ما يلزم من العلم به علم شيء آخر ، وغايته أن يتوصل العقل إلى التصديق اليقيني فيما كان يشك في مدى صحته ، أي أن يتوصل به إلى معرفة الحقيقة[85].

---

[84] محمد بن أبي بكر بن عبدالقادر الرازي ، مختار الصحاح ، الهيئة المصرية العامة للكتاب ، ص209.

[85] محمد الأمين البشرى "الأدلة الجنائية الرقمية مفهومها ودورها في الإثبات" المجلة العربية للدراسات الأمنية والتدريب ، المجلد 17 ، العدد 33 ، ص 104.

ثالثاً . الدليل إصطلاحا :

يقصد به "هو النشاط الإجرائي الحال والمباشر من أجل الحصول على اليقين القضائي وفقاً لمبدأ الحقيقة المادية وذلك عن طريق بحث أو تأكيد الاتهام أو نفيه"[86] .

كما يقصد بالدليل الجنائي هو "الوسيلة التي يستعين بها القاضي للوصول إلى الحقيقة التي ينشدها" ، والمقصود بالحقيقة في هذا الصدد هو كل ما يتعلق بالوقائع المعروضة عليه لإحكام القانون فيها[87] .

كما أن الدليل هو "كل واقعة مادية تعين في صحة إسناد الجريمة للمتهم ، وهذه الوقائع لا يقلل من أهمية توافرها أن يقرر المُشرّع للقاضي الجنائي بصلاحية وسلطة واسعة في الاقتناع[88] ، والقضاء بما يمليه عليه ضميره"[89]، أو هو كل إجراء معترف به قانوناً لإقناع القاضي بحقيقة الواقعة، كما يُعرف أيضاً بأنه "الواقعة التي يستمد منها القاضي البرهان على إثبات اقتناعه بالحكم الذي ينتهي إليه"[90] .

وكما هو ملاحظ من التعريفات السابقة ، نجد أن كلا منها ينظر إلى الدليل الجنائي من زاوية معينة ، وعلى ذلك نجد أن استخدام مصطلح الوسيلة أدق من مصطلح الواقعة لأن الواقعة تطلق على الجريمة نفسها ، أما الوسيلة فتطلق على ما يتوصل به إلى الشيء ، وهذا هو المراد من الدليل.

ولقد ذهب بعض الفقهاء ، إلى استعمال كلمة الإثبات كمرادف لكلمة الدليل ، غير أن الاثبات الجنائي بالمعنى العام يمكن أن يطلق على كل المراحل التي تمر بها العملية الإثباتية ، وعلى ذلك يمكن القول بأن الإثبات يهدف إلى البحث عن الدليل الذي يثبت به حدوث الواقعة الجنائية بغرض تقديمه وتقديره لاستخلاص السند القانوني للفصل في الدعوى ، أما الدليل فهو الوسيلة التي يستمد منها القاضي البرهان[91]، وفي هذا المعنى يبدو أن نطاق كلمة الإثبات أعم وأشمل من كلمة الدليل ، وبالتالي يكون لكل من الكلمتين مدلولهما الخاص.

---

[86] أحمد ضياء الدين محمد خليل ، قواعد الإجراءات الجنائية ومبادئها في القانون المصري ، الجزء الثاني ،كلية الشرطة 2004-2005 ، ص320.

[87] أحمد فتحي سرور ، الوسيط في قانون الإجراءات الجنائية ، الطبعة الثانية ، دار النهضة العربية ، القاهرة ، ، 1970 ، ص 331.

[88] **الإقتناع** : هو إذعان أو قبول نفس مبني على أدلة عقلية تسمح للمرء بقدر كافٍ من الرجحان والإحتمال بأن يوجه فكره نحو نقطة معينة ومن خصائص الإقتناع أنه يستند دائماً إلى أسباب فكرية وهو قلما يتكون نتيجة للتأثيرات الخارجية أو الإنطباعات الشخصية الموروثة أو المكتسبة ولعل هذا أهم ما يميز الإقتناع عن الأعتقاد ، وهو نوع من الأحكام الذهنية الجازمة التي تقبل التشكيك فيها ، أما **اليقين** : هو الإعتقاد الثابت الجازم وهو لحظة عقل منطقية قوامها إطمئنان النفس إلى الشيئ بأنه على صورة محدده وأنه لايمكن أن يكون إلا على هذه الصورة ، (د. أحمد الصادق الجهاني ، مقدمة في الإثبات الجنائي ، محاضرات قدمت لطلبة الدراسات العليا قسم القانون الجنائي ، كلية القانون ، جامعة قاريونس ، بنغازي ، ليبيا ، 2010ص8-10).

[89] أحمد العطار ، شرح قانون الإجراءات الجنائية المصري المحاكمة وطرق الطعن في الأحكام ، 2013 ، ص 18.

[90] محمد زكي أبو عامر ، الإجراءات الجنائية ، دار المطبوعات الجامعية ، الإسكندرية ، 1984 ، ص889.

[91] أبو العلا علي أبو العلا نمر ، الجديد في الإثبات الجنائي ، الطبعة الأولى ، دار النهضة العربية ، ص5-6.

ويعتبر جمع الدليل الجنائي من الصعوبات الرئيسية في الإجراءات الجنائية ، فبدون هذا الدليل لن تثبت الجريمة ولن تسند إلى المتهم ولن يطبق قانون العقوبات ، وقد تضاعفت أهمية الدليل الجنائي طبقاً للسياسة الجنائية الحديثة ، التي تهدف إلى تفريد الجزاء الجنائي طبقاً لشخصية المتهم ، فيتعين توافر الدليل لا من أجل إثبات الجريمة ونسبتها إلى المتهم فحسب ، وإنما أيضاً بقصد تحديد ملامح شخصية المتهم وخطورته الإجرامية ، كما تتضاعف أهمية الدليل الجنائي بأن القاضي يجب أن يصل إلى معرفة الحقيقة ليس فقط بما يقدمه الخصوم من أدلة كما هو الحال في الخصومة المدنية ، بل أن عليه دوراً في جمع الدليل وتقديره.[92]

وبناءً على ما تقدم يمكننا أن نقول بأن الدليل الجنائي هو الوسيلة التي يصل بها القاضي لإثبات صحة الشيء من عدمه بشأن الواقعة موضوع الدعوى ، كما أنه يمنح للمتهم الحماية بما يمكّنه من نفي الاتهام عن نفسه .

الفرع الثاني
خصائص الدليل الجنائي

يتسم الدليل الجنائي بعدة خصائص ، يتميز بها وهي خصائص عامة لأنواع الأدلة المختلفة ، سواء المادية أو الفنية أو المعنوية ، وسنتناول هذه الخصائص على النحو التالي:

أولاً ـ الجريمة تصنع أدلتها :

ويقصد بها أن الجريمة هي التي تصنع أدلتها ، التي تتشكل مقوماتها بمناسبة اقترافها لتستقر أصولها في قرار مادي أو معنوي نفسي بين معلوم ومجهول ، ظاهر أو خفي ، وما دور السلطات القضائية إلا دور كاشف لها من مصادرها من خلال قواعد إجرائية ، تستخدمها دون أن يكون لها دور في وجودها حتى ولو وضع الدليل المادي لمعاينة أو خبرة فنية ، للتعرف على دلالة هذا الدليل أو مغزاه ، هذا الدور الفني الذي يقوم به الخبراء باستخدام الوسائل العلمية في حين يعجز القاضي أو المحقق من معرفته بنفسه.

وإذا كان الجاني هو مرتكب الجريمة ، إلا أن هذا لا يعني أنه وحده المصدر البشري للدليل فيها ، ذلك لأن سلوك المجني عليه الذي واجه فيها سلوك الجاني كرد فعل يعتبر مصدراً بشرياً من مصادر الأدلة ، وذلك إذا قاوم المجني عليه الجاني بعدم تمكينه من إتمام جريمته .

فعناصر الأدلة تختلف بصورة طبيعية بمناسبة ارتكاب الجريمة ، فهي تمثل عين الحقيقة بحيث يكون دور السلطات القضائية هو الدور الكاشف لها حيثما وجدت ظاهرة كانت أو خفية.

---

[92] أحمد فتحي سرور ، مرجع سابق ، ص 332-333.

ثانياً . استظهار عناصر الأدلة يتوقف على الكفاءة الشخصية لرجال الضبط القضائي وسلطات التحقيق :

إن القدرة على استظهار عناصر الأدلة ، تتفاوت بتفاوت كفاءة وقدرة رجال الضبط القضائي وسلطات التحقيق التي تباشر الإجراءات ، في التعامل مع عناصر الجريمة وأطرافها واستخلاص أدلتها سواء كان ذلك في مرحلة جمع الاستدلالات أو مرحلة التحقيق الابتدائي أومرحلة التحقيق النهائي ، أثناء المحاكمة ، غير أن استظهار عناصر الأدلة يتطلب كشفها بالطرق الصحيحة ، من خلال الوعي الإجرائي الكافي ، ليستخلص المحقق استخلاصاً سائغاً من مصادرها الشرعية ، فتخرج معبره عن الحقيقة الواقعية التي تصلح أساساً للحكم الجنائي العادل. [93]

ثالثاً . يتميز الدليل الجنائي بصعوبة استخلاصه :

يختلف الإثبات في المواد الجنائية عنه في المواد المدنية، حيث أن القاضي الجنائي يحكم في وقائع مادية قد وقعت وانتهت في الماضي ، ويصعب إلى حد كبير إعادة تصويرها بالكيفية التي وقعت بها ، بحيث لا يكون لتدخل السلطات القضائية التي يقع عليها عبء الإثبات إلا تدخلاً لاحقاً بعد علمها بوقوع الجريمة والذي قد يتراخى لأيام أو أشهر تكون عناصر الجريمة قد اندثرت معالمها حسب الظروف التي تتعرض لها ، أو ينصب الإثبات على أمور معينة موجودة في شخص الجاني ، وهو ما يعبر عنه بالقصد الجنائي الذي يمثل الركن المعنوي في الجريمة ، بينما نظيره القاضي المدني فهو يحكم في وقائع قانونية ثابتة يمكن إعادة تصويرها بصورة يسيرة وسهلة ، بل أن عملية إعادة تصويرها أمام القاضي هي الوسيلة الوحيدة لإثباتها[94]، فالإثبات في المواد المدنية غالباً ما يكون محله حقوق والتزامات[95]، ناشئة عن عقود أو أن تكون ناشئة عن التزامات بمقتضى مراكز قانونية أو أحوال شخصية ثابتة مترتبة على قيام علاقة زوجية كالتزام الزوج بالنفقة على زوجته وأولاده.

وهذا يعني أن الإثبات في المواد الجنائية ، يتطلب بذل أقصى جهد للتنقيب والبحث عن أدلة الجريمة التي لم يكن لها وجود مسبق قبل ارتكاب الجريمة وكشف عناصرها وإثبات صحتها.

رابعاً . الدليل الجنائي هو الوسيلة الوحيدة الذي ينقل أحداث الجريمة إلى علم القاضي :

تعتبر الصلة التي تربط بين وقائع الجريمة ، وبين علم القاضي منقطعة تماماً من الوجهة القانونية ، وذلك نظراً للتفاوت من الناحية الزمنية ، الذي يتمثل في الانقضاء بين كشف وقوع الجريمة وإحالة موضوع الدعوى الجنائية الناشئة عنها ، إلى القاضي المعني بنظر القضية

---

[93] برهامي أبوبكر عزمي ، الشرعية الإجرائية للأدلة العلمية دراسة تحليلية لأعمال الخبرة ، دار النهضة العربية ، القاهرة ، 2006 ، ص 110-111-112-113 .

[94] أحمد الصادق الجهاني ، مرجع سابق ، ص6.

[95] محمد محي الدين عوض ، الإثبات بين الازدواج والوحدة في الجنائي والمدني في السودان ، مطبوعات جامعة القاهرة ، الخرطوم ، 1974 ، ص13 .

والفصل فيها ، ونظراً لعدم وقوف القاضي بنفسه على معالم الجريمة بعد اكتشافها ، فلا مناص من أن تكون الأدلة الجنائية هي الوسيلة الوحيدة لنقل هذه الوقائع إلى علم القاضي فإذا شاب هذه الوسيلة الناقلة قصور أو عدم أمانة في النقل خلال التحقيقات النهائية التي يجريها القاضي خلال جلسات المحاكمة وجب على القاضي أن يصدر حكمه ببراءة المتهم استناداً إلى قرينة البراءة التي يتمتع بها عندما تخلو ساحة الإثبات من أدلة قطعية الدلالة في الإدانة ، ويطمئن إلى صحتها على وجه اليقين.

غير أن القاضي الجنائي قد يعلم بتفاصيل الجريمة الخاصة بالدعوى التي ينظر فيها وذلك عن طريق وسائل الإعلام وسرعة تواجدها في مكان وقوع الحدث لنقله مباشرةً أوالكتابة عنه بطريقة غالباً ما تكون مجردة ومحايدة ، يكون من الصعب تحصين القاضي ضد تأثيرها عليه ، إلا أن هذه الوسيلة الناقلة غير قضائية ولا يمكن أن يعتدّ بها كحجة قضائية[1].

خامساً . قطعية الدليل :

الأصل في الإنسان البراءة ، وعلى من يدعي العكس أن يقيم الدليل على صحة ما يدعيه ومؤدى ذلك أنه لا يصح الحكم بإدانة شخص إلا إذا قام الدليل القاطع على انتفاء براءته، أما الحكم بالبراءة فلا يلزم بناؤه على القطع والجزم ، بل يصح بناؤه على الشك في ثبوت الإدانة ومن ذلك أن الحكم بالبراءة يصح أن يبنى إما على أدلة قاطعة تنفي الاتهام أو على عدم وجود أدلة قاطعة تثبت صحة الاتهام ، ذلك أن الحكم بالإدانة لا سبيل إليه إلا إذا قام الدليل القاطع على وقوع الجريمة ونسبتها إلى المتهم[2] .

---

[1] برهامي أبوبكر عزمي ، مرجع سابق ، ص 115 وما بعدها .

[2] عوض محمد عوض ، قانون الإجراءات الجنائية ، الجزء الثاني ، 1995 ، ص 142.

سادساً . الدليل الجنائي يخضع لتقدير سلطة المحكمة :

ويقصد به أن القاضي الجنائي حر في انتقاء الأدلة ذات الأثر في تكوين عقيدته ، وطرح ما عداها دون بيان العلة ، إلا أنها متى أفصحت عن الأسباب التي من أجلها أخذت بها الأدلة أو طرحتها ، فإنه يلزم أن يكون ما أوردته واستدلت به مؤدياً لما رتبه عليه من نتائج من غير تعسف في الاستنتاج ، ولا تناقض في حكم العقل والمنطق[96]

سابعاً . يتميز الدليل الجنائي بتساند مع الأدلة الأخرى :

ويقصد بتساند الأدلة هي أن الأدلة التي يذكرها الحكم في أسبابه تساند بعضها البعض ، ويكمل بعضها البعض لتدعيم النتيجة التي خلصت إليها المحكمة من حكمها وتكونت على أساسها عقيدتها[97]

فإذا سقط أحد هذه الأدلة أو أستبعد تعذر التعرف على الدليل الباطل ذي الأثر في الرأي الذي انتهت إليه المحكمة ، أو الوقوف على ما كانت تنتهي إليه المحكمة من نتيجة لو أنها انتبهت إلى أن هذا الدليل غير قائم ، لذا جرت المحكمة على أنها إذا أبطلت دليلاً من الأدلة الجوهرية ، ألغت الحكم برمته باعتباره معيباً لما شابه من فساد في الاستدلال ، أو أن الإجراءات ليس لها أصل في الأوراق أو الخطأ في الإسناد ، وهذا مما يقتضي إعادة النظر في الأدلة الصحيحة لدعم الإدانة.

لكن إذا كان الدليل الذي أبطلته المحكمة أو استبعدته ، ليس من شأنه أن يؤثر على عقيدة محكمة الموضوع لو أنها انتبهت إلى بطلان الدليل ، فإن مثل هذا الدليل يعتبر غير جوهري ، ومن ثم لا يهوّن من قوة الأدلة الأخرى ، بحيث أنها تكتفي بذاتها وبما بينها من تساند أن تثبت الواقعة موضوع الدعوى وإدانة مرتكبها[98]

والقاضي إن كان حراً في تكوين عقيدته إلا أنه ملزم ببيان كيفية اقتناعه عن طريق تسبيب الأحكام وهو في هذا خاضع لرقابة المحكمة العليا[99]

---

[96] محمد زكي أبوعامر ، الإثبات في المواد الجنائية ، دار الجامعة الجديدة ، الإسكندرية ، 2011، ص161.

[97] مأمون محمد سلامة ، الإجراءات الجنائية في التشريع المصري ، الجزء الثاني ، دار الفكر العربي ، مطبعة جامعة القاهرة والكتاب الجامعي ، ص 264.

[98] رؤوف عبيد ، مبادئ الإجراءات الجنائية ، دار الجبل للطباعة ، القاهرة ، ص792-793.

[99] مأمون محمد سلامه ، المرجع السابق ، ص 265.

الفرع الثالث
تقسيمات الدليل الجنائي

يوجد هناك العديد من المحاولات الفقهية لتقسيم الدليل الجنائي وهي كالآتي :

أولاً . تقسيم الأدلة من حيث قوتها في الإثبات :

تقسم الأدلة من حيث قوتها في الإثبات إلى أدلة كاملة أو تامة ، وأدلة ناقصة أو شبه أدله ، وأدلة ضعيفة أو الخفيفة ، وسنعرّف كل منها على النحو التالي :

أ) الأدلة الكاملة أو التامة :

وهذا النوع من الأدلة يكفي بذاته لإقناع القاضي ويجب عليه إذا ما توافرت ، أن يرتب عليها أثارها مهما كان اقتناعه الشخصي[100]، والمثال على هذا النوع من الأدلة شهادة الشهود والدليل الكتابي ، والاعتراف.

ب) الأدلة الناقصة أو شبه أدلة :

والمثال على هذا النوع هو القرائن التي لا يجوز الحكم بمقتضاها في الحالات المعاقب عليها بالإعدام إلا إذا توافر جانبها دليل كامل.

ومع هذا يجوز في بعض التشريعات الحكم بهذه الأدلة إذا ساندتها أدلة أخرى حتى ولو كانت غير تامة كاعتراف المتهم الناتج عن التعذيب.[101]

ج) الأدلة الضعيفة أو الخفيفة :

ويقصد بهذه الأدلة أنها تجعل المتهم في وضع الاشتباه ، أي لا يمكن أن يحكم عليه بالإدانة ولا بالبراءة ، وإنما يحكم بتوسطها ، فهذا الاشتباه يفتح باب التحقيق ، ولكن من الممكن أن تكون أدلة مكملة لغيرها تخول القاضي الاستناد إليها في الحكم بالإدانة.[102]

ثانياً ـ تقسيم الأدلة من حيث علاقة الدليل بالواقعة المراد إثباتها :

تقسم الأدلة من حيث علاقة الدليل بالواقعة المراد إثباتها ، إلى أدلة مباشرة ، وأدلة غير مباشرة .

---

[100] موسى مسعود أرحومة ، حرية القاضي الجنائي في تكوين عقيدته ، الطبعة الأولى ، الدار الجماهيرية للنشر والتوزيع والإعلان ، ليبيا ، 1988 ، ص 21-22.

[101] أحمد الصادق الجهاني ، مرجع سابق ، ص 1.

[102] محمود محمود مصطفى ، الاثبات في المواد الجنائية (النظرية العامة) ، الجزء الاول ، الطبعة الاولى ، مطبعة جامعة القاهرة 1977 ، ص9 .

أ) الأدلة المباشرة :

ويقصد بهذا النوع من الأدلة إذا كان الدليل ينصب على الواقعة المراد إثباتها كان الدليل مباشراً ، ومثال ذلك شهادة الشهود ، والاعتراف ، والمحررات[103].

ب) الأدلة غير المباشرة :

ويقصد بها إذا كان الدليل ينصب مباشرةً على واقعة أخرى ، والتي تفيد أو تؤدي إلى استخلاص قرار معين بالنسبة للواقعة المراد إثباتها ، وعلى القاضي أن يعمل ذهنه فيستنبط الواقعة التي أنصب الدليل عليها الواقعة الأخرى التي يراد إثباتها ، ويعني ذلك أنه لا يكفي القاضي لفهم الدليل غير المباشر مجرد الملاحظة الحسية أو الاستيعاب ، وإنما عليه أن يطبق العملية الذهنية التي قوامها الاستنباط فيستخلص مما ورد عليه الدليل واقعة لم يرد عليها مباشرةً دليل ، والمثال على هذا النوع القرائن[104] .

ثالثاً . تقسيم الأدلة من حيث وظيفتها :

تقسم الأدلة من حيث وظيفتها إلى أدلة إثبات وأدلة نفي وسوف نعرّف كلاً منها على النحو الآتي :

أ) أدلة الإثبات :

وهي الأدلة التي توجه نحو إدانة المتهم ، أو تشديد العقوبة عليه ، وذلك عن طريق إثبات وقوع الجريمة ونسبتها إلى فاعلها ، فضلاً عما يحيط بها من ظروف مشددة .

ب) أدلة النفي :

وهي الأدلة التي تهدف إلى إثبات براءة المتهم ، أو تخفيف العقوبة عليه ، وذلك عن طريق نفي وقوع الجريمة ونسبتها إلى المتهم ، وإثبات توافر الظروف المخففة[105] .

والجامع بين أدلة الإثبات وأدلة النفي ، هو أن كلاً منها يسعى إلى كشف الحقيقة وهي الغاية من الإثبات[106] .

ويلاحظ على هذا التقسيم ، أن أدلة الإثبات ليست جميعها على درجة واحدة من حيث الأهمية ، فبعضها يكفي لمجرد رفع الدعوى الجنائية ، وهو ما يكفي فيه الترجيح وتسمى بأدلة الاتهام ، وبعضها يصل إلى حد اليقين وتسمى بأدلة الإدانة[107] .

---

[103] مأمون محمد سلامة ، مرجع سابق ، ص 168.
[104] محمود نجيب حسني ، شرح قانون الإجراءات الجنائية ، دار النهضة العربية ، القاهرة ،1982 ، ص452.
[105] أحمد فتحي سرور ، مرجع سابق ، ص337- 338 .
[106] عوض محمد عوض ، مرجع سابق ، ص143.
[107] أحمد فتحي سرور ، المرجع السابق ، ص338.

أما أدلة النفي فهي لا تشترط ، أن تصل إلى حد القطع بعدم وقوع الجريمة أو نسبتها إلى فاعلها ، لأن الأصل في الإنسان البراءة ، كما أن الشك يفسر لمصلحة المتهم ، ومن ثم يجب أن تؤدي هذه الأدلة إلى إثارة الشك في ذهن القاضي حول قيمة أدلة الإثبات ، دون أن يصل الأمر إلى حد نفيها كُلياً وبهذا القدر وحده تنجح أدلة النفي في أداء مهمتها.

رابعاً . تقسيم الأدلة من حيث مصدرها :

تقسم الأدلة من حيث مصدرها إلى أدلة مادية ، أدلة فنية ، أدلة قولية ، أدلة قانونية

أ) الدليل المادي : وهو الدليل الذي يعبر بنفسه عن الحقيقة ، التي تؤثر في عقيدة القاضي ومثال ذلك ، الأثر المادي الذي يتركه الجاني في مكان الحادث مثل البصمة التي تدل على صاحبها ويتم الحصول عليها عن طريق المعاينة أو التفتيش أو الضبط.[108]

ب) الدليل الفني : أو كما يطلق عليه بعض الفقهاء بالدليل العلمي[109] ، ويقصد بهذا النوع من الأدلة هو ما يستخلصه أهل الخبرة من استنتاجات بناءً على تطبيقات علمية أو فنية أعقبت عدة مشاهدات وملاحظات حسية ، التي تمكن من خلالها الوصول إلى الاستنتاجات الفنية عن طريق الاستنباط العقلي وبحكم العلم ونظرياته[110].

ج) الدليل القولي : وهو الدليل الذي ينبعث من عناصر شخصية ، تتمثل فيما يصدر من الغير من أقوال وتؤثر في إقناع القاضي بطريقة غير مباشرة ، من خلال تأكده من صدق هذه لأقوال[111] . وهذا النوع من الأدلة يختلف عن الأدلة المادية حيث أن القاضي يكون اقتناعه من الأدلة المادية بطريقة مباشرة[112]، ومن مصادر الأدلة القولية الشهادة ، والاعتراف ، والاستجواب.

د) الدليل القانوني : ويقصد بهذا النوع من الأدلة ، هي التي يحددها القانون مسبقاً للقاضي لإثبات جريمة معينة ، وحدد شروط كل دليل وقوته القانونية ، بحيث لا يمكنه الاعتماد على غيرها ، فإذا قام الدليل وأستوفى شروطه ألتزم القاضي به ، ووجب عليه أن يحكم بالإدانة[113] حتى ولو كانت قناعته الوجدانية مخالفة ومغايرة تماماً لما سيضمنه في منطوق الحكم[114]، وإذا

---

[108] شعبان محمود محمد الهواري ، أدلة الإثبات الجنائي ، الطبعة الأولى ، دار الفكر والقانون للنشر والتوزيع ، المنصورة ، 2013 ، ص 32.

[109] أحمد العطار ، مرجع سابق ، ص 20.

[110] عبدالحكم فوده ، حجية الدليل الفني في المواد الجنائية والمدنية ، دار الفكر الجامعي ، الإسكندرية ، 2014 ، ص7.

[111] هشام عبدالحميد الجميلي ، المرجع الحديث في الإثبات الجنائي والدفوع الجنائية في ضوء مختلف الآراء وأحكام النقض ، حيدر جروب للنشر والتوزيع ، دار علام للإصدارات القانونية ،2014 ، ص 9.

[112] أحمد فتحي سرور ، مرجع سابق ، ص337.

[113] عوض محمد عوض مرجع سابق ، ص139.

[114] أحمد الصادق الجهاني ، مرجع سابق ، ص1.

تخلف الدليل أو شروطه وجب على القاضي أن يحكم بالبراءة ، أو بمعنى آخر يقتصر دور القاضي على مجرد التحقق من مدى توافر الدليل أو شروطه[115].

والدليل القانوني يطبق أصلاً في المواد المدنية ، أما في المسائل الجنائية فيحكم القاضي في الدعوى حسب عقيدته التي تكونت لديه بكامل حريته ، أي بمعنى أن الأدلة غير محصورة في الدعوى الجنائية ، غير أن حرية القاضي الجنائي تتقيد حيث تتبع المحاكم الجنائية في المسائل غير الجنائية ، التي تفصل فيها تبعاً للدعوى الجنائية طرق الإثبات المقررة في القانون الخاص بتلك المسائل ، فإثبات عقد الأمانة يجب أن يكون بالكتابة ، إذا زادت قيمته عن عشرة جنيهات ما لم يجيز القانون المدني إثباته بالبينة ، غير أنه يشترط للتقيد بطرق الإثبات في المسائل غير الجنائية أن يكون محل الواقعة المدنية عنصراً لازماً لقيام الجريمة[116].

المطلب الثاني
التعريف بالدليل الرقمي

بعد أن تناولنا التعريف بالدليل الجنائي بصورة عامة من حيث تعريفه لغةً واصطلاحاً ، وبيان خصائصه وتقسيماته ، بات علينا أن نعرف الدليل الجنائي الرقمي باعتباره نوعاً متميزاً من أنواع الدليل الجنائي ، وذلك من حيث بيان تعريفه وخصائصه وتقسيماته من خلال ثلاثة فروع : نخصص الفرع الأول لتعريف الدليل الرقمي . ونكرس الفرع الثاني لدراسة خصائص الدليل الرقمي . ونفرد الفرع الثالث لتقسيمات الدليل الرقمي .

الفرع الأول
تعريف الدليل الرقمي

نظراً للجهود التي بذلت لتعريف الدليل الرقمي ، نشير إلى وجود اتجاهين أحدهما يضيق من تعريف الدليل الرقمي ، والثاني يوسع من تعريف الدليل الرقمي ، ولذا سنبين هذين الاتجاهين على النحو الآتي :

---

[115] موسى مسعود أرحومة ، حرية القاضي الجنائي في تكوين عقيدته ، مرجع سابق ، ص 20.

[116] محمود مصطفى ، شرح قانون الإجراءات الجنائية ، الطبعة الثامنة ، الإتحاد القومي ، دار ومطابع الشعب ، 1962- 1963 ، ص 364-367.

أولاً . الاتجاه المضيق لتعريف الدليل الرقمي :

يذهب البعض إلى تعريف الدليل الرقمي بأنه "الدليل المأخوذ من أجهزة الحاسب الآلي في شكل مجالات ونبضات مغناطيسية أو كهربائية ، ممكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة ، ويتم تقديمها في شكل دليل يمكن اعتماده أمام القضاء"[117]وهو مكون رقمي لتقديم معلومات في أشكال متنوعة مثل (الصور ، والأصوات والنصوص المكتوبة)[118].

وكما هو ملاحظ من ذلك التعريف نجد أنه لا يخلو من القصور في تحديد مفهوم الدليل الرقمي ، وذلك بتصنيف دائرة الأدلة الرقمية ، وجعلها مقصورة على الأدلة المستخلصة من أجهزة الحاسب الآلي فقط .

وبالرغم من الآثار المعلوماتية المستخلصة من أجهزة الحاسب الآلي من الممكن أن تكون ثرية جداً ، بما تحتويه من معلومات مثل صفحات المواقع المختلفة "WebPages" والبريد الإلكتروني "Email" والفيديو الرقمي "Digital video" والصوت الرقمي وغرف الدردشة والكيان المادي والمعنوي للحاسب الآلي[119] إلا أن هذا التعريف غير جامع للأدلة الرقمية بأكملها ، ذلك لأن هناك مصادر أخرى للأدلة الرقمية لم يشر إليها في هذا التعريف ، مثل جهاز التصوير الرقمي والهاتف المحمول ، وغير ذلك من شبكات الإتصال والأجهزة التي تعتمد على التقنية الرقمية في تشغيلها يمكن أن تكون مصدراً للدليل الرقمي.

---

[117] مفتاح أبوبكر المطردي ، "الجريمة الإلكترونية والتغلب على تحدياتها" ورقة عمل مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية المنعقد بالسودان في 23-2012/9/25 ، ص 33.

[118] **تتنوع أشكال الدليل الرقمي إلى** : أ. **صورة رقمية** : يقصد بها تجسيد الحقائق المرئية حول الجريمة ، أما في شكل ورقي أو مرئي باستخدام الشاشة الرئيسية ، والواقع أن الصورة الرقمية تمثل تكنولوجيا يذيله للصورة الفوتوغرافية التقليدية ب. **الأصوات** : وهي التسجيلات التي يتم ضبطها وتخزينها بواسطة الآلة الرقمية وتتمثل في المكالمات الصوتية على الإنترنت والهاتف النقال ، ج.النصوص المكتوبة : ويقصد بها النصوص التي يتم كتابتها بواسطة الآلة الرقمية ، وتتمثل في رسائل البريد الإلكتروني ورسائل الهاتف النقال .....الخ . (طارق محمد الجملي ، الدليل الرقمي في مجال الإثبات الجنائي ، بدون ترقيم صفحات ، بحث منشور على الإنترنت.Http//www.startimes.com . lfaspx?t=30245909) .

[119] ممدوح عبدالحميد ، الادلة الرقمية والتحقيق الجنائي في جرائم الكمبيوتر ، بدون ترقيم صفحات ، بحث منشور على الانترنت: Http//:www.drmamdooh.com/images/lectures/152fb.ppt

ثانياً . الاتجاه الموسع لتعريف الدليل الرقمي :

إن أنصار هذا الاتجاه يعرف الدليل الرقمي بأنه "أي معلومات مخزنة أو منقولة بشكل رقمي وتعد جزء من قضية ما وقد تستخدم كإثبات "[120] ، أو هو "الدليل الذي يجد له أساساً في العالم الافتراضي[121]، ويقود إلى الواقعة غير المشروعة ومرتكبها "[122] .

كما يعرف أيضاً بأنه " الدليل المشتق من أو بواسطة النظم البرامجية المعلوماتية الحاسوبية ، وأجهزة ومعدات وأدوات الحاسب الآلي ، وشبكات الاتصال من خلال إجراءات قانونية وفنية لتقديمها للقضاء بعد تحليلها علمياً أو تفسيرها في شكل نصوص مكتوبة أو رسومات أو صور وأشكال وأصوات لإثبات وقوع الجريمة ولتقرير البراءة أوالإدانة فيها".[123]

ويلاحظ على التعريفات المتقدمة ، أنها تمتاز بالطابع العمومي ، فهي لم تقتصر مصدر الدليل الرقمي على جهاز الحاسوب فقط ، بل أن المفهوم من تلك التعريفات أن مصدر الأدلة الرقمية ، قد تكون شبكات الاتصال وغير ذلك من الأجهزة الرقمية ، كالهاتف النقال وجهاز التصوير الرقمي .

وتجدر الإشارة إلى أن الدليل الرقمي ، كما يصلح لإثبات الجرائم الإلكترونية المستحدثة فهو يصلح لإثبات الجرائم الإلكترونية التقليدية ، إذا أستعمل جهاز الحاسب الآلي أو شبكة الإنترنت أو الآلة بصفة عامة ، كوسيلة لارتكاب الجريمة التقليدية مثل استخدامه في غسل الأموال أو تهريب المخدرات.[124]

وتأسيساً على ما تقدم يمكننا وضع تعريف للدليل الرقمي بأنه "المعلومات أو البيانات المخزنة في جهاز الحاسب الآلي وملحقاته ، كالطابعات وغيرها من شبكات الاتصال ووسائلها ، كالإنترنت ، والهاتف النقال ، وتشمل كذلك أي جهاز يعتمد على التقنية الرقمية كجهاز التصوير الرقمي ، بحيث يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات خاصة بهدف إثبات وقوع الجريمة ونسبتها إلى فاعلها".

---

[120] فواز دليم الحربي ، الأدلة الجنائية الحاسوبية مبادئ ومفاهيم وتقنيات ، بدون ترقيم صفحات ، بحث منشور على الانترنت : Http//lexpertarabs.com.lar chives.1127.

[121] **العالم الافتراضي** : "هو العالم الذي يصنعه الحاسب الآلي بحيث يمكن الإنسان التفاعل معه بنفس الأسلوب الذي يتفاعل به مع العالم الحقيقي" المنظومة الحصرية للتكنولوجيا التعليمية ، مفهوم الواقع الافتراضي ، بحث منشور على الانترنت : Http//techm31omat2012.blogspot.com/2012/12/virtual.reality.html

[122] عمر محمد بن يونس ، الدليل الرقمي ، الطبعة الأولى ، الجمعية العربية لقانون الإنترنت ، 2007 ، ص25.

[123] عبدالناصر محمد محمود فرغلي ، ود. عبيد سيف سعيد المسماري ، مرجع سابق ، ص13.

[124] طارق محمد الجملي ، الدليل الرقمي في مجال الإثبات الجنائي ، مرجع سابق ، بدون ترقيم صفحات .

الفرع الثاني
خصائص الدليل الرقمي

يتميز الدليل الرقمي عن الدليل الجنائي التقليدي بعدة خصائص وهي كالآتي :

أولاً . الدليل الرقمي دليل علمي :

يتكون الدليل الرقمي من دوائر مغناطيسية ونبضات كهربائية غير ملموسة ، ولايدركها الرجل العادي بالحواس الطبيعية للإنسان ، فإذا كان الدليل الرقمي هو الذي يثبت الواقعة الإجرامية التي تحدث في البيئة الإلكترونية ، وهي واقعة أساسها علمي من حيث أن أساس العالم الافتراضي ، هو أساس علمي شيده العلماء والتقنيين ، وتفيد هذه الخاصية أنه لا يمكن الحصول على الدليل الرقمي أو الإطلاع على محتواه ، إلا بالاستعانة بأساليب علمية تتمثل في الأجهزة والأدوات التقنية ، كجهاز الحاسب الآلي ، واستخدام برامج وتطبيقات خاصة ، كما تفيد هذه الخاصية أيضاً حين تقوم الأجهزة الأمنية والقضائية بالتعامل مع الدليل الرقمي بهدف إثبات وقوع الجريمة ونسبتها إلى مرتكبها ، حيث يجب أن تبنى عملية البحث هنا على أسس علمية.[125]

ثانياً . الدليل الرقمي دليل تقني :

وهي الخاصية الثانية التي يتمتع بها الدليل الرقمي ، فهو مشتق من البيئة التي يعيش فيها ، وهي البيئة الرقمية أو التقنية "العالم الافتراضي" وتتمثل هذه الأخيرة في إطار الجرائم الإلكترونيه في العالم الرقمي ، وهذا العالم يكمن في أجهزة الحاسب الآلي وشبكات الاتصال بمختلف أنواعها ، فالدليل الرقمي ليس مثل الدليل العادي ، فلا تنتج التقنية سكيناً يتم به اكتشاف القاتل أو اعترافاً مكتوباً أو مالاً في جريمة الرشوة أو بصمه أصابع[126]، وإنما تنتج التقنية نبضات كهربائية غير ملموسة تصل إلى درجة التخيلية في شكلها وحجمها ومكان تواجدها غير المعلن.[127]

ولكي يجب فهم مضمون أو محتوى الدليل الرقمي ، أن يتطلب اعتماده على أجهزة خاصة تقوم بتجميع وتحليل محتواه ، ولذلك فكل ما لا يمكن تحليل محتواه بواسطة تلك الأجهزة لا يمكن اعتباره دليلاً رقمياً ، وذلك لعدم إمكانية الاستدلال به على معلومة مما يعدم قوته التدليلية في إثبات وقوع الجريمة ونسبتها إلى مرتكبها.[128]

---

(125) عمر محمد بن يونس ، الدليل الرقمي ، مرجع سابق ، ص42 .

(126) عمر محمد يونس ، الإثبات الجنائي عبر الإنترنت ، بحث منشور على الإنترنت :
Http//www.ituarabis.org.coe/coe/2006E.crime/Dociu.ARAdo.ppt

(127) عبدالناصر محمد محمود فرغلي و د. عبيد سيف سعيد المسماري ، مرجع سابق ، ص14 .

(128) طارق محمد الجملي ، مرجع سابق ، بدون ترقيم صفحات .

ثالثاً . الدليل الرقمي يسهل التخلص منه :

يتميز الدليل الرقمي عن الدليل الجنائي التقليدي ، بسهولة التخلص منه وذلك لأن محل الدليل الرقمي هي البيانات أو المعلومات المخزنة بوسائل تقنية المعلومات التي يسهل إتلافها أو تدميرها بواسطة برامج فيروسية ، غير أن هناك العديد من البرامج الحاسوبية التي وظيفتها استعادة البيانات التي تم حذفها أو إلغاؤها مثل برامج معالجة الملفات "xtreeprobold" وهو برنامج يمكّن المحقق من العثور على الملفات في أي مكان على الشبكة أو على القرص الصلب.[129] ويستخدم لتقييم محتويات القرص الصلب الخاص بالمتهم أو الأقراص المرنة[130] المطبوعة أو يستخدم لقراءة البرامج في صورتها الأصلية كما يمكن البحث عن كلمات معينة أو عن أسماء ملفات أو غيرها.[131] .

رابعاً . إن نشاط الجاني لمحو الدليل الرقمي يسجل عليه كدليل أيضاً ، حيث أن نسخه من هذا الفعل ، الذي قام به الجاني لمحو الدليل يتم تسجيله في جهاز الحاسوب أو البيئة الرقمية بصفة عامة ، بحيث يمكن استخلاصه لاحقاً لاستخدامها كدليل إدانة ضده.[132] .

خامساً . الدليل الرقمي قابل للنسخ :

يمكن استخراج نسخة من الدليل الرقمي مطابقاً للأصل ، بحيث تقل أو تعدم تقريباً مخاطر إتلاف الدليل الأصلي ، حيث تتطابق طريقة النسخ مع طريقة الإنشاء ، وهذه لاتتوافر في أنواع الأدلة الجنائية التقليدية.[133]

سادساً . الاتساع العالي لمسرح الدليل الرقمي ، بحيث يمكّن مستغلي الدليل الرقمي من تبادل المعرفة الرقمية بسرعة عالية ، وبمناطق مختلفة من العالم ، مما يساهم في الاستدلال على الجُناة أو أفعالهم بسرعة أقل نسبياً[134] .

---

[129] الأقراص الصلبة (hard disk) : وهو قرص معدني رقيق ومغطى بمادة قابلة للمغنطة ، وهو من أكثر وحدات التخزين استخداماً لسرعتها وكفاءتها العالية ، وهي مفيدة للتطبيقات التي تحتاج إلى مخازن ذات سعات تخزينية كبيرة مثل برامج معالجة النصوص لكتابة الرسائل أو تأليف الكتب ، وثبت القرص الصلب بالجهاز داخل حافظة تمنعه من وصول الأتربة إليه ، ويتميز القرص الصلب بعدم تحريكه من مكانه ولذلك يطلق عليه أحياناً بالقرص الثابت .

[130] الأقراص المرنة (floppy disk) :- وتستخدم لتخزين الملفات ، وهي أقل سعة من القرص الصلب ، لأن حجم تخزينه قليل وهذا القرص لأنه مرن يجب المحافظة عليه بكل عناية سواء من الأتربة أو من أشعة الشمس ، بوضعها في غلاف بلاستيكي.(خيرت علي محرز ، التحقيق في جرائم الحاسب الآلي ، دار الكتاب الحديث ، القاهرة ، 2012 ، ص21 .
ـ بشير على القائد ، المرجع السابق ، ص 79-80 .) .

[131] توجد طرق أخرى تساهم في جمع الأدلة الرقمية : وهي قرص بدء تشغيل الكمبيوتر.Do fable Diskette وبرنامج إذن تفتيش "computer scorch" وبرنامج النسخ "top link" وبرامج كشف الدسك "view AmA Disk" وبرامج الإتصالات "Lahtastic" (جمانه كاظم علي الخليفة ، تقنيات الأدلة الجنائية الإلكترونية ،بدون ترقيم صفحات ، بحث منشور على الإنترنت : (Http//coeia.ksu.edu.say

[132] ممدوح عبدالحميد ، مرجع سابق ، بدون ترقيم صفحات.

[133] عبدالناصر محمد محمود فرغلي و د. عبيد سيف سعيد المسماري ، مرجع سابق ، ص15.
ومثل هذا الأمر لاحظه المُشرّع البلجيكي فقام بمقتضى قانون 28 نوفمبر 2000 بتعديل قانون التحقيق الجنائي بإضافة المادة (39bis) التي سمحت بضبط الأدلة الرقمية مثل نسخ المواد المخزنة في نظم المعالجة الآلية للبيانات بقصد عرضها على الجهات القضائية. (عمر محمد بن يونس ، الدليل الرقمي ، مرجع سابق ، ص 43.) .

[134] إياد علي الدرة " الأدلة الجنائية الإلكترونية" مجلة معلوماتية ، العدد 72 ، ص 292 ، بحث منشور على الإنترنت :
Infomag.News.sy//indexphp?ine=issues/showarticles2 aid=1363.

سابعاً . الدليل الرقمي يمتاز بالسعة التخزينية العالية ، فآلة الفيديو الرقمية يمكن أن يخزن فيها مئات الصور[135] .

ثامناً . يمتاز الدليل الرقمي برصد معلومات عن الجاني ، وتحليلها في ذات الوقت فالدليل الرقمي يمكنه أن يسجل تحركات الفرد ، كما أنه يسجل عاداته وأخلاقياته وبعض الأمور الشخصية عنه ، لذا فإن سلطات الاستدلال والتحقيق قد تجد غايتها بسهولة أيسر من الدليل الجنائي المادي.

الفرع الثالث
تقسيمات الدليل الرقمي

لقد بينا فيما سبق أن الدليل الرقمي له طبيعة خاصة تميزه عن الدليل الجنائي التقليدي مما يتطلب منا تحديد تقسيمات الدليل الرقمي ، وسنقسم هذا الفرع إلى فقرتين : نخصص الفقرة الأولى لدراسة تقسيم الدليل الرقمي من منظور وزارة العدل الأمريكية . ونكرس الفقرة الثانية لتحديد تقسيم الدليل الرقمي من منظور فقهي.

أولاً . تقسيم الدليل الرقمي من منظور وزارة العدل الأمريكية :

وفقاً لما قررته وزارة العدل الأمريكية سنة (2002) فإن الدليل الرقمي يمكن تقسيمه إلى ثلاثة أقسام[136] ، وهي كالتالي :

أ) السجلات المحفوظة في جهاز الحاسب الآلي ، وهي الوثائق المكتوبة والمحفوظة مثل البريد الإلكتروني ، وملفات برامج معالجة الكلمات ، ورسائل غرف المحادثات على الإنترنت.

ب) السجلات التي تم إنشاؤها بواسطة جهاز الحاسب الآلي ، وتعتبر هذه السجلات من مخرجات جهاز الحاسوب ، التي لم يساهم الإنسان في إنشائها مثل فواتير أجهزة الحاسب الآلي .

ج) السجلات التي جزء منها تم حفظه ، وجزء تم إنشاؤه بواسطة جهاز الحاسب الالي ، ومن أمثلة ذلك البيانات التي يتم إدخالها إلى جهاز الحاسوب ، ويتم معالجتها من خلال برنامج خاص كإجراءات العملية الحسابية على تلك البيانات .

ويلاحظ على هذا التقسيم أنه لم يشمل كل أشكال الدليل الرقمي ، وهي الصور والأصوات ، بل اقتصرت على سجلات الحاسوب ، بالرغم من أن مصدر الدليل الرقمي ليس محصوراً فقط في جهاز الحاسوب ، بل توجد وسائل تقنية معلومات كثيرة كالهاتف النقال وغيرها .

---

[135] ممدوح عبدالحميد ، مرجع سابق ، بدون ترقيم صفحات .

[136] مفتاح ابوبكر المطردي ، مرجع سابق ، ص36.

ثانياً . تقسيم الدليل الرقمي من منظور فقهي :

لقد حاول بعض الفقهاء تقسيم الدليل الرقمي إلى أربعة أقسام[137] ، وهي كالآتي :

أ) الأدلة الرقمية الخاصة بأجهزة الكمبيوتر وشبكاتها .

ب) الأدلة الرقمية الخاصة بالإنترنت .

ج) الأدلة الرقمية الخاصة ببروتوكولات تبادل المعلومات بين أجهزة الشبكة العالمية للمعلومات.

د) الأدلة الرقمية الخاصة بالشبكة العالمية للمعلومات.

وإن هذا التقسيم يتطابق مع التقسيم الفقهي للجريمة عبر الكمبيوتر الذي قام بتقسيمها إلى أربعة أنواع :

1- <u>جرائم الكمبيوتر :</u> وهي سلوك صادر عن الإنسان يهدف إلى تنفيذ عمل غير مشروع قانوناً يقع على أجهزة الحاسب الآلي ، سواء وقع هذا التصرف غير مشروع على الكيان المادي أو المعنوي لجهاز الحاسب الآلي ، ومن أمثلتها تخريب الكيان المادي للجهاز كالشاشات أو الطابعة أو أقراص التخزين المرنة أو الصلبة ، كذلك الفيروسات التي تؤدي إلى تعديل أو محو البيانات الرئيسية.

2- <u>جرائم الإنترنت</u> : وهي تصرف إنساني يشكل فعلاً غير مشروع قانوناً حيث يقع على آلية نقل المعلومات ، بين مستخدمي الشبكة العالمية للمعلومات ومن أمثلة هذه الجرائم ، جرائم الولوج غير المشروع لمواقع غير مصرح بها واستخدام عناوين "IP" غير حقيقية أو زائفة إلى الشبكة العالمية للمعلومات ويقصد بعنوان "IP" هو عندما يتحول مستخدم الإنترنت في حوار إنترنت ، يترك آثار ما قام به في كل مكان يزوره ، فالموقع الذي يمر به يفتح سجلاً خاصاً به يتضمن عنوان الموقع الذي جاء منه ، نوع الكمبيوتر والمتصفح الذي يستخدمه ، وعنوان رقم "IP" الدائم ، ويتم ذلك عبر البروكسي[138] ، أو تقنيات الحماية firewall الخاصة بالجهات المتصلة بالشبكة وغيرها.

3- <u>جرائم الشبكة العالمية</u> : ويقصد بها أي سلوك صادر عن الإنسان ، يشكل فعلاً غير مشروع قانوناً ، ويقع على أي مستند مكتوب أو صوت أو صورة بالشبكة ومن أمثلتها قرصنة المعلومات ، وسرقة أرقام بطاقات الائتمان وغيرها ، وأن هذه الجرائم تتطلب الاتصال بالإنترنت على خلاف جرائم الكمبيوتر ، التي تحدث سواء كان هناك اتصال بالإنترنت أم لا .

4- <u>جرائم عبر الكمبيوتر</u> : ويقصد بهذا النوع من الجرائم ، أنه لا يعتبر استخدام الكمبيوتر والإنترنت والشبكة العالمية للمعلومات من طبيعة الفعل الإجرامي ، مثل الجرائم التي يتم فيها

---

(137) عبدالناصر محمد محمود فرغلي ود. عبيد سيف سعيد المسماري ، مرجع سابق ، ص14 .

(138) **بوركسي " Proxy "** حيث تقوم مزودات البروكسي بدور الوسيط ، بين المشتركين لدى إحدى شركات تقديم خدمة إنترنت ، وبين المواقع الموجودة على الشبكة العالمية ، وبدور الوكيل عن هؤلاء المشتركين في طلب المعلومات من تلك المواقع. (ممدوح عبدالحميد ، مرجع سابق ، بدون ترقيم صفحات) .

استخدام الكمبيوتر أو الإنترنت أو الشبكة العالمية للمعلومات في عمليات غسل الأموال أو نقل المخدرات من مكان لآخر ، فالكمبيوتر والإنترنت ، والشبكة العالمية للمعلومات ، تعتبر هنا كوسيلة يعتد بها الجاني لارتكاب جريمته[139].

أما البعض الآخر [140] ، فقد قسم الدليل الرقمي إلى ثلاثة أقسام :

أ) السجلات التي تم إنشاؤها بواسطة الآلة تلقائياً ، وتعتبر هذه السجلات من مخرجات الآلة[141] التي لم يساهم الإنسان في إنشائها مثل سجلات الهاتف وفواتير أجهزة الحاسب الآلي.

ب) السجلات التي جزء منها تم حفظه بالإدخال ، وجزء تم إنشاؤه بواسطة الآلة ومن أمثلة ذلك البيانات التي تم إدخالها إلى الآلة ، ثم معالجتها من خلال برنامج خاص ، بإجراء العملية الحسابية على تلك البيانات ، ويتميز هذا النوع من الأدلة بسهولة الحصول عليه .

ج) وهناك نوع من الأدلة لم ينشأ بإرادة الشخص ، أي ما يتركه الجاني دون أن يكون راغباً في وجوده ، وهي تتكون في الآثار التي يتركها مستخدم الشبكة المعلوماتية بين تسجيل الرسائل المرسلة من أو التي يستقبلها[142]، ويتميز هذا النوع من الأدلة بأنه لم يُعدّ أصلاً كدليل ليكون أثراً لمن صدر عنه ، ولهذا سيضمن معلومات تفيد في كشف الحقيقة عن الجريمة ومرتكبها ، ويتم الحصول على هذه الأدلة بإتباع تكنولوجيا خاصة لا تخلو من صعوبة وتعقيد.

وكما هو ملاحظ من هذا التقسيم الأخير ، وإن كان يتفق مع التقسيم الذي وضعته وزارة العدل الأمريكية ، من حيث أنه مقتصر على السجلات المكتوبة دون باقي أشكال الدليل الرقمي ، كالأصوات والصور ، إلا أنه يختلف عن التقسيم بوزارة العدل الأمريكية بأنه لم يربط السجلات بتلك التي يتم إخراجها من جهاز الحاسب الآلي فقط ، بل إن استخدام مصطلح الآلة في هذا التقسيم الأخير هو مصطلح فضفاض بحيث يمكن أن يشمل جهاز الحاسب الآلي ، وكذلك الهاتف النقال ، وغير ذلك من الأجهزة التي تعتمد على التقنية الرقمية.

والسؤال الذي يطرح نفسه في هذا المقام هو أين تقع الأدلة الرقمية من بين تقسيمات الدليل الجنائي العام ؟ أي بمعنى آخر هل تعتبر الأدلة الرقمية من قبيل الأدلة المادية باعتبارها منبعثة من عناصر مادية ملموسة ؟ أم أنها تعتبر من الأدلة الفنية أو العلمية باعتبارها ناتجة من رأي خبير فني ؟

---

(139) ممدوح عبدالحميد ، مرجع سابق ، بدون ترقيم صفحات .

(140) مفتاح أبوبكر المطردي ، مرجع سابق ، ص36.

(141) مخرجات الآلة : ويقصد بها مخرجات الكمبيوتر ، ليست فقط الورق الذي يخرج من الطابعة ، ولكن أيضاً البيانات التي يسجلها الكمبيوتر على مختلف الوسائل ، مثل الاسطوانات الممغنطه أو ذاكرة الجهاز نفسه . (شيماء عبدالغني ، مرجع سابق ، ص385) .
وتنقسم مخرجات الكمبيوتر إلى ثلاثة أنواع :
- المخرجات الورقية : هي التي تسجل فيها المعلومات على الورق باستخدام الطابعات .
- المخرجات الإلكترونية : هي التي تسجل فيها المعلومات على الأشرطة والأقراص الممغنطة .
- مخرجات معالجة البيانات المعروضة بواسطة الشاشات أو وحدة العرض المرئي : وهي تعتبر من أهم أجزاء الحاسب إستخداماً إذ عن طريقها يتم استعراض أي بيانات أو معلومات تكتب على لوحة المفاتيح بواسطة المستخدم .(هلالي عبداللاه أحمد ، حجية المخرجات الكمبيوترية في المواد الجنائية ، 1999 ، ص 16 وما بعدها).

(142) مفتاح أبوبكر المطردي ، المرجع السابق ، ص 36.

للإجابة عن هذا التساؤل يوجد هناك اتجاهان[143] ، لتحديد مكان الأدلة الرقمية من الأدلة الجنائية التقليدية بصفة عامة.

الاتجاه الأول : يرى مؤيدو هذا الاتجاه ، أن الأدلة الرقمية ما هي إلا مرحلة متقدمة من الأدلة المادية المحسوسة ، التي يمكن إدراكها بإحدى حواس الإنسان الطبيعية ، إلى الاستعانة بجميع ما يبتكره العلم من أجهزة مخبرية ، ووسائل التقنية المعلوماتية ، ومنها الحاسوب باعتباره أساس الأدلة الرقمية ، فالأدلة الرقمية في نظر أصحاب هذا الاتجاه لا تختلف عن آثار الأسلحة والبصمات أو البصمة الوراثية DNA .[144]

الاتجاه الثاني : يعتبر هذا الاتجاه مخالفاً ومغايراً تماماً للاتجاه الأول حيث يرى مؤيدو هذا الاتجاه ، أن الأدلة الرقمية هي نوع متميز من وسائل الإثبات ، ولها من الخصائص العلمية والمواصفات القانونية ما يجعلها تقدم إضافة جديدة لأقسام الأدلة الجنائية التقليدية .

ومن خلال الموازنة بين الاتجاهين نؤيد الاتجاه الثاني ، وذلك لأن الأدلة الرقمية تتميز بخصائص معينة باعتبارها أدلة علمية تقنية قابلة للنسخ إلى غير ذلك من الخصائص السابق ذكرها ، فضلاً عن أن البيئة الرقمية أو الإلكترونية التي تحدث فيها الواقعة الإجرامية ويستمد منها الدليل الرقمي ، هي ذات طابع معنوي غير ملموس ، وهو ما يختلف عن الأدلة الجنائية التقليدية الأخرى .

---

(143) محمد الأمين البشري ، مرجع سابق ، ص 110-111.

(144) **البصمة الوراثية (DNA)** : هي مجموعة من المعلومات الجزيئية التي تكون الحمض النووي ، والتي تدل على شخصية الفرد وتميزه عن غيره ، والتي يمكن الاستدلال بها على إثبات أو نفي النسب ، والتحقق من الشخصية في المجال الجنائي. (إيناس هاشم رشيد "تحليل البصمة الوراثية ومدى حجيتها القانونية في مسائل الإثبات القانوني" مجلة رسالة الحقوق ، السنة الرابعة ، العدد الثاني، 2012 ، ص 214).

الفصل الثاني

إجراءات جمع الدليل الرقمي

لا شك أن كل جريمة لا يمكن إثباتها إلا بدليل يتم الحصول عليه بالإجراءات التي نص عليها القانون ، وبما أن الجرائم الإلكترونية تختلف عن الجرائم الأخرى من حيث طبيعتها الخاصة فإن ذلك سيؤدي إلى تغيير المفاهيم السائدة حول إجراءات الحصول على هذا الدليل .

وبناءً على ما تقدم سنقسم هذا الفصل إلى مبحثين : نخصص المبحث الأول لدراسة الإجراءات التقليدية لجمع الدليل الرقمي . ونكرس المبحث الثاني لدراسة الإجراءات الحديثة لجمع الدليل الرقمي .

المبحث الأول

الإجراءات التقليدية لجمع الدليل الرقمي

حدّد المشرّع الليبي الطرق التي يتم الحصول بها على الدليل من خلال إجراءات معينة ، وأهم هذه الإجراءات ، المعاينة والتفتيش ، وضبط الأشياء ، سماع الشهود ، وندب الخبراء ، وعلى ذلك سنقسم هذا المبحث إلى خمسة مطالب : نخصص المطلب الأول لدراسة المعاينة . ونكرس المطلب الثاني لدراسة التفتيش . ونخصص المطلب الثالث لدراسة ضبط الأشياء . ونكرس المطلب الرابع لدراسة سماع الشهود . ونفرد المطلب الخامس لدراسة الخبرة .

المطلب الأول

المعاينة في مسرح الجرائم الإلكترونية

سنتناول في هذا المطلب تعريف المعاينة وأهميتها ، والإجراءات التي يتم إتباعها في معاينة مسرح الجرائم الالكترونية لذلك سنقسم هذا المطلب إلى فرعين : نخصص الفرع الأول لتعريف المعاينة وأهميتها . ونكرس الفرع الثاني لبيان إجراءات المعاينة في مسرح الجرائم الالكترونية .

الفرع الأول

تعريف المعاينة وأهميتها

أولاً . تعريف المعاينة :

يذهب جانب من الفقه إلى تعريف المعاينة بأنها " مشاهدة وإثبات الحالة القائمة في مكان الجريمة ، والأشياء التي تتعلق بها ، وتفيد في كشف الحقيقة ، وإثبات حالة الأشخاص

الذين لهم صلة بها كالمجني عليه فيها "[145] ، وقد عرفها البعض الآخر بأنها "إثبات حالة الشيء أو شخص معين ، وهي تقتضي الانتقال إلى مكان وجود هذا الشيء أو الشخص لفحصه والتحقق منه "[146].

والمعاينة قد تكون مكانية كما قد تكون شخصية ، كما قد تكون عينية أو مادية[147] .

وكما هو ملاحظ من التعريفات المتقدمة ، أن المعاينة تتطلب سرعة الانتقال إلى مكان الحادثة التي وقعت فيها الجريمة ، وذلك لإثبات حالته وضبط الأشياء التي تفيد في كشف الحقيقة ، لإثبات وقوع الجريمة ونسبتها إلى مرتكبها .

ثانياً . أهمية المعاينة :

تكمن أهمية المعاينة في أنها من أهم الإجراءات في التحقيقات المتعلقة بالدعوى الجنائية فهي عصب التحقيق ودعامته ، من حيث تعبيرها عن ما يدور في الواقع ، تعبيراً صادقاً ، لا يشوبه الكذب والخداع[148] ، فهي توضح الصورة الحقيقية للجريمة ، ذلك أن إجراء المعاينة ، وخاصة التي يقوم بها مأمور الضبط القضائي[149] ، أو سلطة التحقيق[150] أو المحكمة[151] تساعد على وضوح الرواية عن كيفية ارتكاب الجريمة منذ لحظة وقوعها حتى نهايتها أمام المحكمة لكي تتبين حقيقة الواقعة وما يثار فيها من غموض[152].

ويستهدف إجراء المعاينة أمرين ، الأول : جمع الأدلة التي تخلفت عن الجريمة كرفع البصمات ، وتحليل الدماء ، وجميع ما يفيد في كشف الحقيقة سواءً كان هذا الدليل استخدم في أحداث ارتكاب الجريمة أو تخلف عنها[153].

---

[145] فوزية عبدالستار : شرح قانون الإجراءات الجنائية ، دار النهضة العربية ، القاهرة ، 1986 ، ص526.

[146] أحمد فتحي سرور : مرجع سابق ، ص587.

[147] مأمون محمد سلامة ، مرجع سابق ، ص523 - 524 .

[148] شعبان محمود محمد الهواري ، مرجع سابق ، ص137 .

[149] المادة (14) إجراءات ليبي "يجب على مأموري الضبط القضائي أن يقبلوا التبليغات والشكاوي التي ترد إليهم بشأن الجرائم ، وأن يبعثوا بها فوراً إلى النيابة العامة ، ويجب عليهم وعلى مرؤسيهم أن يحصلوا على جميع الايضاحات ويجروا المعاينات اللازمة لتسهيل تحقيق الوقائع التي تبلغ إليهم أو التي يعلمون بها بأي كيفية كانت ، وعليهم أن يتخذوا جميع الوسائل التحفظية اللازمة للمحافظة على ادلة الجريمة ، ويجب أن تثبت جميع الإجراءات التي يقوم مأمور الضبط القضائي في محاضر موقع عليها منهم يبين فيها وقت اتخاذ الاجراء ومكان حصوله....."

- المادة (21) إجراءات ليبي "يجب على مأمور الضبط القضائي في حالة التلبس بالجناية أو الجنحة أن ينتقل فوراً إلى محل الواقعة ، ويعاين الأثار المادية للجريمة ويحافظ عليها ، ويثبت حالة الاماكن والاشخاص وكل مايفيد في كشف الحقيقة ، ويسمع أقوال من كان حاضراً أو من يمكن الحصول منه على إيضاحات في شأن الواقعة ومرتكبها ، ويجب عليه أن يخطر النيابة العامة فور انتقاله ، ويجب على النيابة العامة بمجرد اخطارها بجناية المتلبس بها الانتقال فوراً إلى محل الواقعة"

[150] المادة (74) إجراءات ليبي "ينتقل المحقق إلى أي مكان كلما رأى ذلك ليثبت حالة الأمكنة والأشياء والأشخاص ووجود الجريمة مادياً وكل ما يلزم اثبات حالته "

[151] المادة (267) إجراءات ليبي "إذا تعذر تحقيق دليل أمام المحكمة جاز لها أن تندب أحد اعضائها أو قاضياً آخر لتحقيقه" ، مجموعة التشريعات الجنائية ، الجزء الثاني ، الإجراءات الجنائية ، إعداد الإدارة العامة للقانون ، ليبيا ، الهيئة العامة لشئون القضاء ، 1987 م . ويقابل ذلك المواد (24 – 31 – 294) من قانون الإجراءات الجنائية المصري والقوانين المكملة لها وفقاً لأحدث التعديلات ، إعداد ومراجعة أسامة أنور ، دار العربي ، 2014.

[152] هشام عبدالحميد الجميلي ، مرجع سابق ، ص445 .

[153] محمد زكي أبو عامر ، الإجراءات الجنائية ، مرجع سابق ، ص680 .

أما الثاني : هو إعطاء سلطة التحقيق فرصة المشاهدة بنفسها للصورة الحقيقية والصحيحة لمكان حدوث الواقعة الإجرامية ، وما فيها من ماديات وآثار للجاني أو الجناة.[154]

ومع التسليم بأهمية المعاينة في ظهور حقيقة الكثير من الجرائم التقليدية فيما عدا الجرائم التي لا تجدي فيها المعاينة نفعاً ، كجرائم الرشوة والتزوير والسب[155] ، إلا أن المعاينة في مجال إظهار حقيقة الجرائم الإلكترونية لا تصل إلى نفس الدرجة من الأهمية التي تلعبها في مجال الجريمة التقليدية ، ويرجع ذلك إلى أمرين هما[156]:

أ) أن الجرائم الإلكترونية قلما يترتب على اقترافها آثار مادية محسوسة .

ب) إن الأعداد الكبيرة من الأشخاص الذين قد يترددون على مسرح الجريمة خلال المدة الزمنية التي غالباً ما تكون طويلة ، وذلك بين اقتراف الجريمة والكشف عنها ، الأمر الذي يؤدي إلى حدوث تغيير أو عبث بالآثار المادية أو إتلافها ، وهذا ما سيقود إلى نوع من الشك على الدليل المتحصل من المعاينة ، وبذلك يستلزم ضرورة توخي الحذر حال إجراء المعاينة في مسرح الجرائم الإلكترونية .

الفرع الثاني

إجراءات المعاينة في مسرح الجرائم الإلكترونية

يشير الفقه الجنائي إلى أهمية التمييز في ما يتعلق بمعاينة مسرح الجرائم الإلكترونية ، حسب موضوع الجريمة بين أمرين[157]، وهما على النحو الآتي :

أولاً. وقوع الجريمة على الكيان المادي للحاسب الآلي :

إن الجرائم التي تقع على الكيان المادي للحاسب الآلي تتمثل في أشرطة الحاسوب ، والأقراص ، والكابلات ، وشاشات العرض الخاصة به ، ومفاتيح التشغيل ، وهذه المكونات ذات طبيعة مادية ملموسة لا تثير أي صعوبة لمعاينتها من قِبل مأمور الضبط القضائي أو سلطة التحقيق ، والتحفظ على الأشياء ، وضبط كل ما استعمل في ارتكاب الجريمة التي تعتبر أدلة مادية تدل على وقوع الجريمة ونسبتها إلى مرتكبها .

---

[154] شعبان محمود محمد الهواري ، مرجع سابق ، ص137.

[155] محمد زكي أبو عامر ، الإجراءات الجنائية ، مرجع سابق ، ص680 .

[156] مصطفى محمد موسى ، التحقيق الجنائي في الجرائم الإلكترونية ، الطبعة الاولى ، مطابع الشرطة ، القاهرة ، 2009 ، ص172 .

[157] رامي متولي القاضي ، مرجع سابق ، ص108 .

ثانياً . وقوع الجريمة على الكيان المعنوي المنطقي أو الغير مادي أو بواسطة جهاز الحاسب الآلي :

تتمثل الجرائم التي تقع على الكيان المعنوي للحاسب الآلي في الجرائم الواقعة على برامج الحاسب الآلي وبياناته أو بواسطتها التي لا يترتب عليها آثار مادية ملموسة ، وحتى تصبح معاينة مسرح الجرائم الإلكترونية لها فائدة في كشف الحقيقة عنها وعن مرتكبها ، فإنه يجب اتخاذ العديد من القواعد حال إجراء المعاينة في مسرح الجرائم الإلكترونية ، وتتمثل هذه القواعد في الإجراءات التالية :

أ) تصوير جهاز الحاسب الآلي ، والأجهزة الطرفية المتصلة به ، والمحتويات والأوضاع العامة بالمكان ، مع التركيز بوجه خاص على تصوير الأجزاء الخلفية للحاسب الآلي وملحقاته ، ومراعاة زمان ومكان التقاط كل صورة[158] .

ب) العناية بملاحظة الطريقة التي تم بها إعداد النظام[159] ، والآثار الإلكترونية الخاصة بالتسجيلات الإلكترونية التي تتزود بها شبكات المعلومات بموافقة موقع الاتصال ، ونوع الجهاز الذي تم عن طريقه الدخول إلى النظام أو الموقع[160] .

ج) ملاحظة وإثبات حالة التوصيلات والكوابل المتصلة بكل مكونات النظام ، وذلك حتى يتسنى القيام بعملية المقارنة والتحليل لها عند عرض الموضوع على المحكمة .

د) التأكد عند نقل أي مادة رقمية من مكان وقوع الجريمة ، وذلك من خلال إجراء الاختبارات من عدم وجود أي مجالات مغناطيسية في المحيط الخارجي ، يمكن أن يترتب عليها إتلاف البيانات المخزنة[161] .

هـ)التحفظ على محتويات سلة المهملات من الأوراق الملقاة أو الممزقة والشرائط والأقراص الممغنطة (CD) ، ورفع ما يوجد بها من بصمات لها علاقة بالجريمة المرتكبة[162] .

و) التحفظ على مستندات الإدخال والمخرجات الورقية للحاسب الآلي المتعلقة بالجريمة لرفع ما قد يوجد عليها من بصمات[163] .

---

(158) مصطفى محمد موسى ، مرجع سابق ، ص172 .

(159) Htt//www.press.maroc.com/t3438 topic

(160) حسين بن سعيد الغافري ، السياسة الجنائية في مواجهة جرائم الانترنت ، دار النهضة العربية ، القاهرة ، 2009 ، ص457.

(161) عبدالله حسين علي محمود ، "إجراءات جمع الأدلة في مجال جريمة سرقة المعلومات" ، ورقة عمل مقدمة إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية بأكاديمية الشرطة المنعقد بدبي بالامارات العربية المتحدة ، 2003/4/26 ، بدون ترقيم صفحات ، منشور على الانترنت Http//www.flaw.Net/threads/11338

(162) Http//www.press.maroc.com/t3438 . topic

(163) مصطفى محمد موسى ، المرجع السابق ، ص172 .

ز) لا يسمح للمشتبه به بالتعامل مع وسائل تقنية المعلومات موضوع مسرح الجريمة ، وذلك لأن الأدلة الرقمية قد تتعرض للإتلاف لدى العمل على احدى هذه الوسائل .

ح) إعداد نسخة احتياطية عن وسائط تخزين المعلومات الموجودة في مسرح الجريمة ، لضمان المحافظة على الدليل الأصلي .

ط) توثيق جميع نشاطات التحقيق منذ لحظة فتح القضية إلى لحظة إغلاقها بحيث يجب توثيق كل ما يفعله المحقق ، بالوقت والتاريخ ، ويمكن استخدام جهاز المحمول (كمبيوتر) ، ومن المهم حفظ المعلومات المسجلة بواسطة كلمة السر مثلاً واستخدام التشفير ، ويجب الاحتفاظ بملفات منفصلة لكل عمل[164] .

ي) إعداد خطة واضحة بالرسومات ، ويتم مراجعتها مع أعضاء الفريق وذلك للهجوم ، مع إخطار الفريق الذي سيتولى المعاينة قبل موعدها بوقت كافٍ لكي يتم تنفيذها على الوجه الأكمل.[165]

ق) حصر مباشرة المعاينة على مأموري الضبط القضائي والمحققين ، ممن تتوافر فيهم الخبرة الفنية والكفاءة العلمية في مجال الحاسب الآلي.[166]

ل) السيطرة على الأماكن المحيطة بمسرح الجريمة ، وذلك عن طريق قفل الطرق والمداخل والتحفظ على الأشخاص .

م) وضع حراسات كافية لمراقبة التحركات داخل الأماكن المحيطة بمسرح الجريمة ورصد الاتصالات الهاتفية من وإلى مكان مسرح الجريمة .

ن) حصر أجهزة الحاسب الآلي الموجودة في مسرح الجريمة بأسرع وقت وفي حالة وجود شبكات الاتصالات يجب البحث عن خادم الملف fileserver لتعطيل حركة الاتصالات ، وكذلك يجب وضع حرس على كل جهاز حتى لا يتمكن أحد المتهمين من إتلاف المعلومات من على البعد ، أو من جهاز آخر داخل المبنى .

ي) اختيار مكان لمقابلة المتهمين والشهود على أن يكون المكان بعيداً عن أجهزة الحاسب الآلي[167] .

---

[164] كمال أحمد الكركي ، " التحقيق في جرائم الإنترنت " ، ورقة عمل مقدمة إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية بأكاديمية الشرطة ، المنعقد بدبي بالإمارات العربية المتحدة ، 26/4/2003 ، بدون ترقيم صفحات منشور على الإنترنت Http//almohokmoonalarab. Ahlamontada.com/t100 topic

[165] عبدالناصر محمد محمود فرغلي ، وعبيد سيف سعيد المسماري ، مرجع سابق ، ص17 .

[166] Http//www.press.maroc.com/t3438 . topic

[167]. عبدالله حسين علي محمود ، مرجع سابق ، بدون ترقيم صفحات .

ونلاحظ مما تقدم أن المعاينة لها أهميتها في مسرح الجرائم التقليدية ، فيما عدا بعض الجرائم الاستثنائية ، إلا أنها في مسرح الجرائم الإلكترونية لا تجدي المعاينة نفعاً سواءً اتخذت هذه الجرائم صورة الجرائم التقليدية التي ترتكب عبر الحاسب الآلي أو شبكة الإنترنت كجريمة الاستيلاء على الأموال عن طريق النصب المعلوماتي ، أم اتخذت صورة هذه الجرائم الإلكترونية المستحدثة كجريمة الولوج في الأنظمة المعلوماتية بطريقة غير مشروعة ، إذ تستلزم كشف هذه الجرائم قواعد إجرائية ذات طابع خاص تختلف عن القواعد الإجرائية التقليدية .

المطلب الثاني
التفتيش في مسرح الجرائم الإلكترونية

سنتناول في هذا المطلب الضوابط العامة للتفتيش[168] في مسرح الجرائم الإلكترونية من الناحية الموضوعية والشكلية .

وعليه سنقسم هذا المطلب إلى فرعين : نخصص الفرع الأول لبيان الضوابط الموضوعية للتفتيش . ونكرس الفرع الثاني لبيان الضوابط الشكلية للتفتيش .

الفرع الأول
الضوابط الموضوعية لتفتيش مسرح الجرائم الإلكترونية

يكمن تحديد الضوابط الموضوعية لتفتيش مسرح الجرائم الإلكترونية في السبب والمحل والسلطة المختصة ، وسنعرض كلاً منها في الفقرات التالية :

أولاً . سبب تفتيش مسرح الجرائم الإلكترونية :

من المتفق عليه أن سبب التفتيش بوصفه إجراءً من إجراءات التحقيق إنما يعني السعي نحو الحصول على دليل في تحقيق قائم من أجل الوصول إلى حقيقة الحدث فيتطلب سبب

---

(168) هو " البحث عن شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبها "

(عوض محمد عوض ، المبادئ العامة في قانون الاجراءات الجنائية ، دار المطبوعات الجامعية ، الاسكندرية ، 1999 ، ص 377.) .

وقد عرف المجلس الأوربي إجراء التفتيش في الجرائم الرقمية بأنه هو " الإجراء الذي يسمح بجمع الأدلة المخزنة أو المسجلة بشكل إلكتروني " وهو الإجراء الذي يسمح باستخدام الوسائل الإلكترونية للبحث في أي مكان عن البيانات والأدلة المطلوبة.

(محمد ابوالعلا عقيدة ، التحقيق وجمع الادلة في مجال الجرائم الإلكترونية ، ص9 ، بحث منشور على الانترنت

www.osamabahar.com)

التفتيش وقوع جناية أو جنحة ، واتهام شخص أو عدة أشخاص بارتكابها ، وتوافر إمارات قوية أو قرائن على وجود أشياء تفيد في إظهار الحقيقة لدى المتهم أو غيره.[169]

وسنبحث هذه الشروط فيما يلي :

أ) أن يكون بصدد جريمة إلكترونية واقعة بالفعل سواءً كانت جناية أو جنحة :

لا شك في أنه لابد لصحة إجراء التفتيش في مسرح الجرائم الإلكترونية أن تكون بصدد جريمة من الجرائم الإلكترونية واقعة بالفعل ، سواءً كانت جناية أو جنحة[170] ، وقد سبق لنا بيان أنه لايوجد تعريف محدد ومتفق عليه بين الفقهاء حول تعريف الجرائم الإلكترونية إذ منهم من قد وسع ومنهم من ضيق هذا التعريف ، وإن كنا انتهينا إلى تبني تعريف مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين ، حيث عرف الجرائم الإلكترونية بأنها "أي جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوب وتشمل الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في البيئة الالكترونية" .

فلا يجوز الأمر بالتفتيش لضبط أدلة في جريمة مستقبلية ولو قامت التحريات والدلائل الجدية على أنها ستقع بالفعل.[171]

ولإمكانية تطبيق القواعد العامة على تفتيش مسرح الجرائم الإلكترونية ، لابد للمشرع أن ينص صراحة على الأفعال التي تشكل جرائم إلكترونية ، وذلك تطبيقاً لمبدأ شرعية الجرائم والعقوبات ، وذلك ما فعلته الكثير من التشريعات المقارنة ، كقانون جرائم أنظمة المعلومات الأردني رقم (30 – لسنة 2010) ، وكذلك قانون جرائم المعلوماتية السوداني الصادر في2007/6/20 وكذلك قانون العقوبات القطري رقم (11 – لسنة 2004) والمتضمن فصل خاص بعنوان جرائم الحاسب الآلي .

ب) اتهام شخص أو أشخاص معينين بارتكاب الجريمة الإلكترونية أو المشاركة فيها :

يشترط لجواز إصدار أمر بتفتيش مسرح الجرائم الإلكترونية ، أن يكون هناك اتهام ضد شخص ساهم في ارتكاب الجريمة سواء بصفته فاعلاً أصلياً أو شريكاً فيها ، وهذا المفهوم من نص المادة (75) إج ليبي حيث نصت على أنه " تفتيش المنازل عمل من أعمال التحقيق ، ولا

---

[169] قدري عبدالفتاح الشهاوي ، ضوابط التفتيش في التشريع المصري والمقارن ، منشأة المعارف ، الاسكندرية ، 2005 ، ص53 .

[170] المادة (75، 36) إ ج ليبي ، حيث نصت المادة (75) إ ج ليبي على أنه "تفتيش المنازل عمل من اعمال التحقيق ، ولايجوز الالتجاء إليه إلا في تحقيق مفتوح وبناء على تهمة موجهة إلى شخص مقيم في المنزل المراد تفتيشه ، بارتكاب جناية أو جنحة أو باشتراكه في ارتكابها أو إذا وجدت قرائن على أنه حائز لاشياء تتعلق بالجريمة"، والمادة (36) إ ج ليبي على أنه "لمأمور الضبط القضائي في حالة التلبس بجناية أو جنحة أن يفتش منزل المتهم ويضبط فيه الاشياء والاوراق التي تفيد في كشف الحقيقة إذا اتضح له امارات قوية أنها موجودة فيه" .

[171] رؤوف عبيد ، مرجع سابق ، ص417 .

يجوز الالتجاء إليه إلا في تحقيق مفتوح وبناء على تهمة موجهة إلى شخص مقيم في المنزل المراد تفتيشه بارتكاب جناية أو جنحة أو باشتراكه في ارتكابها ..... " .

ج) توافر إمارات قوية أو قرائن على وجود معدات أو معلومات أو أجهزة معلوماتية تتعلق بالجريمة وتفيد في إظهار الحقيقة لدى المتهم المعلوماتي أو غيره :

لا يتم التفتيش إلا إذا توافرت لدى السلطة القائمة بالتفتيش أسباب كافية على أنه يوجد في المكان ، أو لدى الشخص المراد تفتيشه أدوات استعملت في الجريمة الإلكترونية أو مستندات إلكترونية ، أو أشياء متحصلة من الجريمة يحتمل أن يكون لها فائدة في استجلاء الحقيقة لدى المتهم المعلوماتي أو غيره ، وبالتالي فإن مجرد وقوع الجريمة سواءً كانت جناية أو جنحة ، واتهام شخص معين بارتكابها أو المساهمة فيها ، لا يكفي لحث سلطة التحقيق إلى إصدار قرارها بمباشرة التفتيش[172] ، ولكي يتم إصدار الإذن بالتفتيش يجب أن يكون الاتهام جدياً بحيث قامت عليه من الدلائل ما يكفي لإنتهاك حق الخصوصية لديه ، وتفتيش حاسوبه الشخصي وبرامجه الخاصة[173] ، ويمكن الاستناد على ذلك من نص المادة (38) إج ليبي حيث نصت بأنه " إذا قامت أثناء تفتيش منزل المتهم قرائن قوية ضد المتهم أو شخص موجود فيه على أنه يخفي أشياء تفيد في كشف الحقيقة جاز لمأمور الضبط القضائي أن يفتشه ".

ولم تتعرض قوانين الإجراءات الجنائية لتعريف الدلائل الكافية[174] ، إلا أن الفقه حدد مفهومها حيث عرف الدلائل الكافية في مجال الجرائم الإلكترونية بأنها " مجموعة من المظاهر أو الأمارات المعينة التي تنهض على السياق العقلي والمنطقي لملابسات الواقعة ، وكذلك على خبرة وحرفية القائم بالتفتيش والتي تؤيد نسبة الجريمة الإلكترونية إلى شخص معين سواءً بوصفه فاعلاً أو شريكاً "[175].

ومن تطبيقات الدلائل الكافية التي يلزم أن يستند الأذن بالتفتيش المعلومات عليها ارتباط عنوان انترنت بروتوكول المتعلق بجهاز الحاسوب الذي يحتوي على صور فاضحة مع رقم حساب المتهم لدى مزود الخدمات ووجود رقمين للهاتف لديه يستخدمان في ذلك[176] .

وتقدير هذه الأدلة متروك للسلطة التي تصدر الأذن بالتفتيش ، بشرط أن يكون تقديرها منطقياً ومتفقاً مع الواقع ، بحيث تظهر هذه الدلائل بجدية عن وقوع الجريمة محل التفتيش ، وأن

---

[172] هلالي عبداللاه أحمد ، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي ، الطبعة الثانية ، دار النهضة العربية ، القاهرة 2008 ، ص122 .

[173] علي حسن محمد الطوالبة ، التفتيش الجنائي على نظم الحاسوب والإنترنت ، 2010 ، ص75 .

[174] انظر المواد (24، 115 ، 134) من قانون الاجراءات الجنائية الليبي.

[175] هلالي عبداللاه أحمد ، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي ، المرجع السابق ، ص121 .

[176] شيماء عبدالغني عطا الله ، مرجع سابق ، ص281-282 .

هناك فاعلاً تنسب إليه[177]، كما لها أن تعتبر التفتيش باطلاً وتلتفت عن الدليل المستمد منه[178].

ثانياً . محل تفتيش مسرح الجرائم الإلكترونية :

يقصد بمحل التفتيش هو المستودع الذي يحتفظ فيه الشخص بالأشياء المادية التي تتضمن سره ، فالسر الذي يحميه القانون ، هو ذلك الذي يستودع في محل له حرمة[179] ، ومن ثم فإن التفتيش قد يقع على مسكن أو يقع على شخص ، وقد يكون محله الرسائل أو السيارات فهذه هي المحال التي يستودع المرء فيها سره عادةً ولها حرمة القانون ، ويشترط في محل التفتيش كعمل إجرائي ، أن يكون محل التفتيش معيناً ، وأن يكون قابلاً للتعامل فيه أي قابليته لأن يكون محلاً للعمل الإجرائي من الناحية القانونية ، أي أن يكون جائز وقوع التفتيش فيه[180] .

ومحل التفتيش في الجرائم الإلكترونية ، هو وسائل تقنية المعلومات بمكوناته المادية والمعنوية ، وشبكات الاتصال الخاصة بها وبناءً على ما تقدم سنبين مدى خضوع مكونات وسائل تقنية المعلومات المادية والمعنوية وشبكات الاتصال الخاصة بها للتفتيش، وذلك على النحو التالي:

أ) <u>تفتيش المكونات المادية لوسائل تقنية المعلومات :</u>

الواقع أن تفتيش المكونات المادية لوسائل تقنية المعلومات بأوعيتها المختلفة بحثاً عن شيء يتصل بجريمة وقعت ، وتفيد في كشف الحقيقة عنها وعن مرتكبيها ، يدخل في نطاق التفتيش طالما تم طبقاً للإجراءات القانونية المقررة ، بمعنى أن حكم تلك المكونات يتوقف على طبيعة المكان الموجودة فيه سواءً من الأماكن العامة أو الأماكن الخاصة ، إذ أن لصفة المكان أهمية خاصة في مجال التفتيش ، فإذا كانت موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته كان لها حكمه ، فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكنه وبنفس الضمانات المقررة قانوناً ، أما بالنسبة للأماكن العامة فإذا وجد شخص وهو يحمل مكونات الحاسب

---

(177) حسين بن سعيد الغافري ، السياسة الجنائية في مواجهة جرائم الانترنت ، مرجع سابق ، ص489 .

(178) علي حسن محمد الطوالية ، مرجع سابق ، ص75-76 .

(179) قدري عبدالفتاح الشهاوي ، مرجع سابق ، ص111 .

(180) محمد محمود الشركسي ، أحكام التفتيش في قانون الاجراءات الجنائية الليبي ، الطبعة الأولى ، دار النهضة العربية ، القاهرة ، 2012 ، ص130 .

الآلي المادية ، أو حائز لها فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص بنفس الضمانات المقررة قانوناً[181].

ويتضح أن التفتيش الواقع على مكونات وسائل تقنية المعلومات المادية لا توجد فيها مشكلة في التنفيذ لإمكانية ذلك وسهولته مع الأخذ بعين الاعتبار الإجراءات الخاصة بضبط هذه الأجهزة لحساسيتها وذلك في حالة سرقتها أو إتلافها أو محوها بسهولة ، لذا يقتضي القيام بهذا الإجراء من قِبل مختص في مجال تقنية المعلومات [182] .

ب) تفتيش المكونات المعنوية لوسائل تقنية المعلومات :

انطلاقاً من نص المادة (39) إج ليبي " لا يجوز التفتيش إلا للبحث عن الأشياء الخاصة بالجريمة الجاري جمع الاستدلالات أو حصول التحقيق بشأنها..... " ، والمفهوم من نص المادة أن التفتيش هو وسيلة للإثبات المادي لا غاية في حد ذاته ، فهو إجراء يسعى إلى ضبط الأدلة المادية المتعلقة بالجريمة لتقديمها إلى المحكمة المختصة كدليل إدانة ، ولكن الشك والتساؤل يثور حول إمكانية اعتبار البحث عن أدلة الجرائم الإلكترونية في نطاق نظم الحاسوب نوعاً من التفتيش باعتبار أن البيانات الإلكترونية أو البرامج في حد ذاتها ليس لها مظهر محسوس ، وقد اختلف الفقه في مدى جواز تفتيش المكونات المعنوية للحاسب الآلي إلى اتجاهين :

الاتجاه الأول : يذهب أنصار هذا الاتجاه إلى جواز تفتيش مسرح الجرائم الإلكترونية بصفة عامة فهو لا يقتصر على الأشياء بمفهومها المادي ، لأن الغاية من التفتيش هي البحث عن دليل بشأن جريمة وقعت ، وهذا مستخلص من نص المادة (39) إج ليبي التي نصت على مصطلح الأشياء ، فمن خلال تفسير ضبط الأشياء ، فإنها تشمل مكونات الحاسوب المادية وغير المادية وذلك إعمالاً بقواعد التفسير المنطقي التي تجعل من الكيانات المنطقية مما يجوز تفتيشها وضبط ما بها من محتويات .

ووصولاً لذات النتيجة يرى البعض أن كلمة شيء أو مادة يجب أن يرجح في شأنه إلى مدلول هذه الكلمة في العلوم الطبيعية ، حيث تعني كل ما يشغل حيزاً مادياً في فراغ معين.

ولما كانت المكونات المعنوية للحاسوب تشغل حيزاً مادياً في ذاكرة الحاسب الآلي ، ويمكن قياسها بمقياس معين وهي أيضاً تأخذ شكل نبضات إلكترونية تمثل الرقمين صفر أو واحد فإنها ذات كيان مادي وتتشابه مع التيار الكهربائي الذي اعتبره الفقه والقضاء في فرنسا ومصر من قبيل الأشياء المادية[183].

---

[181] أسامة بن غانم العبيدي ، " التفتيش عن الدليل في الجرائم المعلوماتية " ، المجلة العربية للدراسات الأمنية والتدريب ، المجلد التاسع والعشرون ، العدد الثامن والخمسون ، 2013 ، ص89 .

[182] علي حسن محمد الطوالبة ، مرجع سابق ، ص36 .

[183] علي محمود علي حمودة ، مرجع سابق بدون ترقيم صفحات .

وهذا الرأي أخذ به الفقه في كل من فرنسا وإنجلترا وأمريكا ، وقد أخذت بعض التشريعات بهذا الرأي الفقهي ، حيث نص قانون الإجراءات الجنائية الفرنسي في المادة (1/57) المضافة بالقانون 2003–239 الصادر في (18 – مارس – لسنة 2003) ، تجيز لمأمور الضبط القضائي التفتيش عن المعلومات في الأماكن التي يجري فيها التحقيق سواءً كانت معلومات مخزنة في النظام المعلوماتي للمتهم أو كانت مخزنة في نظام معلوماتي آخر طالما أن هذه المعلومات تم الوصول إليها من النظام الأساسي أو المتاح الوصول إليها بواسطة هذا النظام الأساسي[184].

الاتجاه الثاني : وعلى نقيض الاتجاه الأول ، يرى أنصار هذا الاتجاه أن المقصود بلفظ الشيء والأشياء هو ما كان مادياً أي ملموساً ، ولذا فإن المفهوم المادي لا ينطبق على بيانات الحاسب الآلي غير المحسوسة أو الملموسة ، ويقترح أصحاب هذا الرأي مواجهة هذا القصور التشريعي بإضافة عبارة إلى القوانين ذات العلاقة وإلى مذكرات التفتيش (المواد المعالجة عن طريق الحاسب الآلي أو بيانات الحاسب الآلي) وبذلك تصبح الغاية الجديدة من التفتيش بعد هذا التطور التقني الحديث ، هي البحث عن الأدلة المادية أو أي مادة معالجة بواسطة الحاسب[185].

ويرى بعض الفقهاء في فرنسا أن النبضات الإلكترونية أو الإشارات الإلكترونية الممغنطة لا تعد من قبيل الأشياء المحسوسة ، وبالتالي لا تعتبر شيئاً مادياً بالمعنى المألوف للمصطلح ولذا لا يمكن ضبطه[186].

وفي الولايات المتحدة الأمريكية تم تعديل القاعدة رقم 34 من القواعد الفدرالية الخاصة بالإجراءات الجنائية عام 1970 ، لتنص على السماح بتفتيش أجهزة الكمبيوتر والكشف عن الوسائط الإلكترونية ، بما في ذلك البريد الإلكتروني والبريد الصوتي والبريد المنقول وعن طريق الفاكس[187] .

ومن خلال الموازنة بين الاتجاهين السابقين نرجح ونؤيد الاتجاه الأول وهو ما يتفق مع سياسة المشرّع الليبي ، وهو المفهوم من نص المادة (32) من القانون رقم (2– لسنة 1979 بشأن الجرائم الاقتصادية) ، حيث اعتبر شتى أنواع الطاقة مالاً من الممكن أن يكون محلاً لجريمة

---

(184) بكري يوسف بكري ، التفتيش عن المعلومات في وسائل التقنية الحديثة ، الطبعة الأولى ، دار الفكر الجامعي ، الاسكندرية 2011 ، ص73 .
- محمد أبو العلا عقيدة ، مرجع سابق ، ص9.

(185) سليمان أحمد فضل ، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الإنترنت) ، دار النهضة العربية ، القاهرة ، 2013 ، ص302 .
- هلالي عبداللاه أحمد ، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي ، مرجع سابق ، ص83-84.

(186) عبدالله حسين علي محمود ، سرقة المعلومات المخزنة في الحاسب الآلي ، الطبعة الرابعة ، دار النهضة العربية ، القاهرة ، 2011 ، ص365 .

(187) أسامة بن غانم العبيدي ، مرجع سابق ، ص90 .
- سليمان أحمد فضل ، مرجع سابق ، ص302.

السرقة ، فاعتبار الطاقة مالاً يؤكد أن المشرّع لا يميز بين الأشياء المادية والمعنوية في تطبيق أحكامه متى كانت الغاية من تطبيق النص متوافرة.[188]

بل أن بعض النصوص الخاصة بالتفتيش في القانون الليبي تؤيد هذا الاتجاه ، حيث تنص المادة (2/75) إج ليبي على أنه " للمحقق أن يفتش أي مكان ويضبط فيه الأوراق والأسلحة والآلات وكل ما يحتمل أنه استعمل في ارتكاب الجريمة أو نتج عنها أو وقعت عليه وكل ما يفيد في كشف الحقيقة " ، فهذا النص يجيز للمحقق أن يباشر التفتيش في أي مكان ، وهذا يسمح باعتبار المكونات المعنوية لوسائل تقنية المعلومات مكاناً مفهوماً بالمعنى الواسع للكلمة ، وعلى ذلك فإن المكونات المعنوية لوسائل تقنية المعلومات من الممكن أن تكون محلاً للتفتيش ، غير أنه ينبغي تحويل المكونات المعنوية لوسائل تقنية المعلومات إلى صور أو تسجيلات أو نصوص عن طريق وحدات الإخراج الخاصة بالكمبيوتر حتى يمكن تفتيشها [189].أو عن طريق وسائط الحفظ أو التخزين الإلكترونية ، كالأسطوانات والأقراص الممغنطة [190] .

ج) مدى خضوع شبكات الحاسوب للتفتيش :

1- اتصال حاسوب متهم بجهاز آلي آخر موجود في مكان آخر داخل الدولة :

يرى الفقه الألماني بشأن مدى إمكانية امتداد الحق في التفتيش إذا تبين أن الحاسب أو النهاية الطرفية في منزل المتهم متصلة بجهاز أو طرفية في مكان آخر مملوك لشخص غير المتهم أنه يمكن أن يمتد التفتيش في هذه الحالة إلى سجلات البيانات التي تكون في موقع آخر استناداً إلى مقتضيات القسم (103) إج ألماني[191].

وقد نص مشروع قانون جريمة الحاسوب الهولندي الذي نص في المادة (125) على أن " تفتيش المسكن يمكن أن يمتد إلى تفتيش نظام آلي موجود في مكان آخر بغية التوصل إلى بيانات يمكن أن تفيد بشكل معقول في كشف الحقيقة ، وإذا ما وجدت هذه البيانات يجب تسجيلها "[192].

---

[188] علي محمود علي حمودة ، مرجع سابق ، بدون ترقيم صفحات .

[189] بكري يوسف بكري ، مرجع سابق ، ص72 .

[190] رامي متولي القاضي ، مرجع سابق ، ص115 .

[191] أسامة بن غانم العبيدي ، مرجع سابق ، ص91.

[192] علي حسن محمد الطوالبة ، مرجع سابق ، ص50 .

- سليمان أحمد فضل ، مرجع سابق ، ص304 .

كما نصت المادة (88) إج بلجيكي على أنه " إذا أمر قاضي التحقيق بالتفتيش في نظام معلوماتي ، أو في جزء منه فإن هذا البحث يمكن أن يمتد إلى نظام معلوماتي آخر يوجد في مكان آخر غير مكان البحث الأصلي ويتم هذا الامتداد وفقاً لضابطين :

– إذا كان ضرورياً لكشف الحقيقة بشأن الجريمة محل البحث .

– إذا وجدت مخاطر تتعلق بضياع بعض الأدلة نظراً لسهولة عملية محو أو إتلاف أو نقل البيانات محل البحث[193].

وباستقراء نص المادة (2/55) إج ليبي التي تنص " للمندوب أن يجري أي عمل آخر من أعمال التحقيق أو أن يستجوب المتهم في الأحوال التي يخشى فيها فوات الوقت متى كان متصلاً بالعمل المندوب له ولازماً في كشف الحقيقة " ، وفي مقابل ذلك يستطيع مأمور الضبط القضائي اتخاذ الإجراءات التحفظية اللازمة حتى يتم استصدار أذن تفتيش من الجهة المطلوبة المادة (14) إج ليبي إلا أن ذلك لا يتماشى مع خصائص الدليل الرقمي ذلك أنه أثناء تحضير أذن تفتيش جديد بإمكان هذا الدليل أن يتلاشى من قبل المتهم ومن ثم يخفي آثار جرمه ، وهذا ما يؤدي إلى إفلات الجناة من يد العدالة .

وباعتقادنا أن جواز تفتيش أي جهاز آلي في إقليم بشرط ألا يكون في دولة أخرى لايمكن هنا إعماله بإطلاق في ضوء القانون الليبي ، لأن هذا النوع من التفتيش ينطوي في الحقيقة على معنى تفتيش غير المتهم ولذلك فإنه لا يجوز إعماله إلا في الأحوال التي يجوز فيها للقائم بتفتيش غير المتهم أو منزله[194] .

2– اتصال الحاسب الآلي للمتهم بحاسب آلي موجود في مكان آخر خارج الدولة :

من المشكلات الإجرائية التي تعيق أجهزة العدالة ، حالة إجراء التفتيش في الجرائم الإلكترونيه العابرة للحدود ، فالأصل في الجرائم الإلكترونية قد تتم عبر شبكات الحواسب الآلية ، والتي تربط العديد من أجهزة الحاسب الآلي في العديد من الدول المختلفة ، وعليه تثير إجراء التفتيش مشكلة إجرائه على جهاز حاسب آلي خارج النطاق الجغرافي للدولة التي أصدرت الأذن بالتفتيش وبالتالي تثور مشكلة شرعية هذا الإجراء ومساسه بسيادة الدولة الأخرى[195].

---

[193] محمد أبو العلا عقيدة ، مرجع سابق ، ص10 .

[194] المادة (78) من قانون الاجراءات الجنائية الليبي " لقاضي التحقيق أن يفتش المتهم وله أن يفتش غيرالمتهم إذا تضح من أمارات قويه أنه يخفي أشياء تفيد في كشف الحقيقة ويراعى في التفتيش حكم الفقرة الثانية من المادة (35) " .
المادة (180) من قانون الاجراءات الجنائية الليبي " لا يجوز للنيابة العامة في التحقيق الذي تجريه تفتيش غير المتهمين أو منازل غير المتهمين أو ضبط خطابات والرسائل في الحالة المشارإليها في المادة (79) إلابناءً على أذن من القاضي الجزئي " .

[195] رامي متولي القاضي ، مرجع سابق ، ص118-119.

وللتعامل مع هذا الاحتمال نصت المادة (17) فقرة (2) من القانون الفرنسي المتعلق بالأمن الداخلي رقم (239– لسنة 2003) على أنه "إذا كانت البيانات المخزنة في نظام معلوماتي تقع في خارج إقليم الدولة فإنه يجوز لرجال الضبط القضائي الدخول إلى هذه البيانات مع مراعاة الشروط المنصوص عليها في المعاهدات الدولية"[196] ، والمفهوم من نص هذه المادة ، أنه لرجال الضبط القضائي أن يقوموا بتفتيش الأنظمة المتصلة حتى ولو تواجدت في خارج الإقليم مع مراعاة الشروط المنصوص عليها في المعاهدات الدولية التي هي طرف فيها .

ويرى جانب من الفقه ، بأن تفتيش الجرائم الإلكترونية العابرة للحدود ، لابد وأن يتم في إطار اتفاقيات تعاون خاصة ثنائية أو دولية ، تسمح بهذا الامتداد يتم إبرامها مع الدولة المعنية وبالتالي فإنه لا يجوز القيام بذلك التفتيش العابر للحدود في ظل عدم وجود مثل هذه الاتفاقيات أو كحد أدنى الحصول على موافقة الدولة الأخرى ، وهذا يؤكد على أهمية التعاون الدولي في مجال مكافحة الجرائم الإلكترونية [197] .

وقد أجازت المادة (32) من الاتفاقية الأوربية بشأن مكافحة الجرائم المعلوماتية الموقعة عام 2001 في بودابست ، إمكانية الدخول في أجهزة أو شبكات تابعة لدولة أخرى بغرض التفتيش والضبط دون أذنها في حالتين :

- **الأولى** : إذا تعلق التفتيش بمعلومات أو بيانات مباحة للجمهور .
- **الثانية** : إذا رضي صاحب أو حائز هذه البيانات بهذا التفتيش[198] .

والمثال على ماتقدم والذي أيده القضاء الألماني في أحد جرائم الغش المعلوماتي ، حيث أسفر البحث عن وجود اتصال بين جهاز حاسب آلي موجود في ألمانيا مرتبط بشبكة الاتصالات في سويسرا ، حيث يتم تخزين بيانات المشروعات فيها ، وعندما أرادت سلطات التحقيق الألمانية الحصول على البيانات لم تتمكن من ذلك إلا عن طريق طلب المساعدة المتبادلة من سويسرا[199] .

ثالثاً . السلطة المختصة بالتفتيش في مسرح الجرائم الإلكترونية :

سنتناول في هذه الفقرة إجراء التفتيش في مسرح الجرائم الإلكترونية بمعرفة سلطة التحقيق الأصلية ، وبمعرفة مأمور الضبط القضائي ، وذلك على النحو التالي :

---

[196] شيماء عبدالغني ، مرجع سابق ، ص301-302.

[197] محمد أبو العلا عقيدة ، مرجع سابق ، ص81 .

[198] رامي متولي القاضي ، مرجع سابق ، ص119 .

[199] حسين بن سعيد الغافري ، السياسة الجنائية في مواجهة جرائم الانترنت ، مرجع سابق ، ص484 - 485 .

أ) إجراء تفتيش مسرح الجرائم الإلكترونية بمعرفة سلطة التحقيق الأصلية :

حدد المشرّع الليبي السلطة الأصلية المختصة بالتحقيق ضمناً ، حيث وصف التفتيش بأنه عمل من أعمال التحقيق ، بموجب نص المادة (75) من قانون الاجراءات الجنائية الليبي فمؤدى ذلك أن السلطة المختصة به هي سلطة التحقيق ، فالتفتيش إجراء خطير ولذلك يتطلب المشرّع فيمن يأمر به أن تتوافر فيه ضمانات ، وقدر المشرّع أن هذه الضمانات لا تتوافر إلا في سلطة التحقيق الأصلية[200]، وسلطات التحقيق الأصلية هي النيابة العامة بصفة أصلية وقاضي التحقيق في حالات خاصة ، المادة (172) من قانون الاجراءات الجنائية الليبي حيث نصت على أنه " فيما عدا الجرائم التي يختص قاضي التحقيق بتحقيقها وفقاً لأحكام المادة (51) إج ليبي تباشر النيابة العامة التحقيق في مواد الجنح والجنايات طبقاً للأحكام المقررة لقاضي التحقيق مع مراعاة ما هو منصوص عليه في المواد التالية" (52،53) حيث نصتا بأن قاضي التحقيق هو مختص غير أنه لا يباشر ذلك إلا بناءً على طلب من النيابة العامة أو بناءً على إحالته إليه من الجهات الأخرى .

والتفتيش جائز لسلطة التحقيق سواءً انصب على شخص المتهم أو منزله أو شخص غير المتهم أو منزله ، ويتميز قاضي التحقيق عن النيابة العامة بسلطته في تفتيش شخص غير المتهم أو منزله[201] ، في حين أن النيابة العامة لا تملك تلك السلطة إلا بعد الحصول على أمر مسبب بذلك من القاضي الجزئي[202] ، ولا يكفي توافر صفة التحقيق أو عضو النيابة العامة لكي يقوم بهذا الإجراء في جميع الحالات ، بل لابد أن يكون مختصاً أصلاً بالتحقيق في الجريمة ويتحدد الاختصاص بالتحقيق بمحل الواقعة أو المكان الذي قبض فيه على المتهم أو المحل الذي يقيم فيه المتهم.[203]

ب) إجراء التفتيش في مسرح الجرائم الإلكترونية بمعرفة مأمور الضبط القضائي :

ينبغي هنا أن نفرق بين صورتين من التفتيش الأولى التفتيش بناءً على حالة التلبس ، والثانية التفتيش بناءً على غير حالة التلبس .

---

[200] محمود نجيب حسني ، مرجع سابق ، ص675.

[201] أنظر المادة (78) من قانون الإجراءات الجنائية الليبي .

[202] المادة (180) إج ليبي " لا يجوز للنيابة العامة في التحقيق الذي تجريه تفتيش غير المتهمين أو منازل غير المتهمين أو ضبط الخطابات والرسائل في الحالة المشار إليها في المادة (79) إلا بناءً على أذن من القاضي الجزئي".

[203] المادة (190) إج ليبي " يتعين الاختصاص بالمكان الذي وقعت فيه الجريمة أو الذي يقيم فيه المتهم أو الذي يقبض عليه فيه " .

1- التفتيش بناءً على حالة التلبس :

يجيز المشرّع الليبي لمأموري الضبط القضائي تفتيش الأشخاص بناءً على حالة التلبس دون الحصول على أذن بذلك من سلطة التحقيق ، وهذا ما تؤكده المادة (35) إج ليبي التي تنص على أنه " في الأحوال التي يجوز فيها القبض قانوناً على المتهم يجوز لمأمور الضبط القضائي أن يفتشه..." ، ويقابل ذلك المادة (46) من قانون الاجراءات الجنائية المصري.

إلا أنه ينبغي أن يقع التفتيش بمعرفة مأمور الضبط القضائي دون غيرهم من معاونيه إذا لم يحصل تحت إشرافه.[204] .

وإجازة تفتيش المتهم المقبوض عليه مقصورة على شخصه ، فلا يملك مأمور الضبط القضائي تفتيش منزله لمجرد أن القبض عليه وقع صحيحاً ، كما لم يستوجب القانون حضور شاهدين عند تفتيش شخص المتهم بمعرفة مأمور الضبط القضائي على نحو ما هو مقرر عند تفتيش منزل المتهم .

وتحدد المادة (24) إج ليبي الحالات التي يجوز فيها القبض استناداً لحالة التلبس بقولها " لمأمور الضبط القضائي أن يأمر بالقبض على المتهم الحاضر الذي توجد دلائل كافية لاتهامه في الجنايات ، وفي أحوال التلبس بالجريمة إذا كان القانون يعاقب عليها بالحبس مدة تزيد على ثلاثة أشهر " ويقابل ذلك المادة (34) من قانون الاجراءات الجنائية المصري.

كذلك يجوز لمأمور الضبط القضائي أن يفتش منزل المتهم في حالة التلبس بموجب نص المادة (36) إج ليبي التي تنص " لمأمور الضبط القضائي في حالة التلبس بجناية أو جنحة أن يفتش منزل المتهم ، ويضبط فيه الأشياء والأوراق التي تفيد في كشف الحقيقة ، إذا اتضح له من أمارات قوية أنها موجودة فيها " .

أما فيما يتعلق بتفتيش مسرح الجرائم الإلكترونية بناءً على التلبس بالجريمة وموقف قانون الإجراءات الجنائية من ذلك بأنه ينطلق من الاجتهاد في نطاق النصوص الإجرائية التقليدية في مواجهة هذا الفراغ التشريعي ، وعلى ذلك يمكن بأن نص المادة (24) من قانون الإجراءات الجنائية الليبي ، يتسع ليستوعب تفتيش مسرح الجرائم الإلكترونيه بناءً على حالة التلبس بالجريمة ، وفي هذا الخصوص نقول أن نص المادة (24) إج ليبي يعطي لمأمور الضبط القضائي في أحوال التلبس بالجنايات والجنح المعلوماتية التي يعاقب عليها بالحبس مدة تزيد على ثلاثة أشهر أن يأمر بالقبض على المتهم المعلوماتي الذي توجد دلائل كافية على اتهامه .

---

[204] نقض جنائي مصري ، 1938/12/19 ، مجموعة أحكام النقض ، س3 ، ص47 .

2- التفتيش بناءً على حالة غير التلبس :

إن سلطة التحقيق الأصلية غير مطالبة بإجراء التفتيش بنفسها في كل الحالات بل لها ندب أحد مأموري الضبط القضائي لإجرائه ، ويقصد بندب مأمور الضبط القضائي للتحقيق الابتدائي ، هو تكليفه من السلطة المختصة بالتحقيق بعمل محدد أو أكثر من أعمال التحقيق[205] ومن بينها التفتيش .

ويجد الندب في إجراء التفتيش سنده في قانون الإجراءات الجنائية الليبي في المادتين (54،174) ويقابل ذلك المادتين (200 ، 70) من قانون الإجراءات الجنائية المصري، حيث تنص المادة (54) إج ليبي على أنه " لقاضي التحقيق أن يكلف أحد أعضاء النيابة العامة أو أحد مأموري الضبط القضائي القيام بعمل معين أو أكثر من أعمال التحقيق عدا استجواب المتهم ..... " ، كما نصت المادة (174) إج ليبي " لكل من أعضاء النيابة العامة في حالة إجراء التحقيق بنفسه أن يكلف أي مأمور من مأموري الضبط القضائي ببعض الأعمال التي من اختصاصه " .

أما بالنسبة للندب في جرائم الحاسب الآلي أو الجرائم الإلكترونية على وجه الخصوص فنجد أن قانون إساءة استخدام الحاسب الآلي الانجليزي ، يشترط ضرورة الحصول على إذن قضائي للتفتيش بالنسبة للجرائم المدرجة في القسم الأول والخاصة بالدخول غير المصرح به على نظام الحاسب الآلي ، ولابد أن يبنى هذا الأذن على أسباب منطقية للاعتقاد بأن الجريمة قد وقعت أو يشتبه في وقوعها في أماكن خاصة ، وأن هناك أدلة متعلقة بهذه الجريمة يمكن الحصول عليها في هذه الأماكن .

كما نصت المادة (487) من القانون الجنائي الكندي ، على إعطاء سلطة إصدار إذن لتفتيش وضبط أي شيء بما في ذلك بيانات الحاسب طالما تتوافر أسس معقولة بأن الجريمة ارتكبت أو يشتبه في ارتكابها.[206]

ومن التشريعات العربية التي أجازت إجراء التفتيش في الجرائم الإلكترونيه قانون جرائم أنظمة المعلومات الأردني رقم (30) لسنة 2010 الذي نصت فيه المادة (1/13) على أنه " مع مراعاة الشروط والأحكام المقررة في التشريعات ذات العلاقة ، يجوز لموظفي الضابطية العدلية الدخول إلى أي مكان يشتبه باستخدامه لارتكاب أي من الجرائم المنصوص عليها في هذا

([205]) محمود نجيب حسني ، مرجع سابق ، ص614 .

([206]) هلالي عبداللاه أحمد ، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي ، مرجع سابق ، ص140 .

القانون ، كما يجوز لهم تفتيش الأجهزة والأدوات والبرامج والأنظمة والوسائل المشتبه في استخدامها لارتكاب أي من تلك الجرائم ..... " .

الفرع الثاني

الضوابط الشكلية لتفتيش مسرح الجرائم الإلكترونية

تتنوع هذه الضوابط الشكلية في الحضور الضروري لبعض الأشخاص أثناء إجراء التفتيش في مسرح الجرائم الإلكترونية ، ومحضر التفتيش ، والميقات الزمني لإجراء تفتيش مسرح الجرائم الإلكترونية ، وهذا ما سنبينه على النحو الآتي :

أولاً . الحضور الضروري لبعض الأشخاص أثناء إجراء التفتيش في مسرح الجرائم الإلكترونية :

يعتبر هذا الشرط من أهم الشروط الشكلية التي يستوجبها القانون خلال مباشرة التفتيش ، وذلك ضماناً لصحة الإجراء وصحة ما يسفر عنه من نتائج ، غير أن هذا الشرط لايستلزم عند تفتيش الأشخاص حيث لم تشترط التشريعات الإجرائية لصحة هذا الإجراء حضور شهود عند القيام بتفتيشهم ، وإنما حدد ذلك فيما يتعلق بتفتيش المساكن ، حيث نجد أن المشرّع الليبي قد حدد هذا الشرط وفقاً للشخص القائم ، حيث اشترط عند مباشرة التفتيش بمعرفة أحد مأموري الضبط القضائي أن يتم في حضور شاهدين ، ويكون هذان الشاهدان بقدر الإمكان من أقاربه البالغين أو من القاطنين معه بالمنزل أو من الجيران المادة (40) إج ليبي ويقابل ذلك المادة (51) إج مصري ، أما إذا كان القائم بتفتيش المساكن قاضي التحقيق أو النيابة العامة فإنه لا يشترط لصحة إجراء التفتيش حضور الشهود ، وإنما يشترط لصحة هذا الإجراء أن يتم بحضور المتهم أو من ينيبه عنه إن أمكن ذلك ، وذلك فيما يتعلق بمنزل المتهم أما إذا حصل التفتيش في منزل غير المتهم ، فإنه يستلزم حضور صاحب المنزل بنفسه أومن ينيبه عنه أن أمكن ذلك المادة (76) إج ليبي ويقابلها المادة (92) إج مصري .

ويلاحظ على نص المادة (76) إج ليبي أنه إذا لم يكن للسلطة عند إجراء التفتيش التمكن من استدعاء المتهم أو من ينيبه ، جاز لها أن تجري التفتيش بدون حضور أحد ، وذلك سواءً قام بالتفتيش النيابة العامة أو قاضي التحقيق ، بل يلتزم بذلك مأمور الضبط القضائي حين يجرى التفتيش بانتداب من سلطة التحقيق الأصلية.[207] .

ثانياً . الميقات الزمني لإجراء التفتيش في الجرائم الإلكترونية :

تحرص بعض التشريعات الإجرائية على حظر القيام بتفتيش المنازل وما في حكمها ليلاً إلا في حالات محددة وذلك حرصاً على تضييق نطاق الاعتداء على الحرية الشخصية وحرمة المسكن ومن هذه التشريعات ، حيث نصت المادة (333) من قانون الإجراءات الجنائية

---

(207) محمد محمود الشركسي ، مرجع سابق ، ص172 .

الايطالي على أنه " لا يجوز تفتيش المباني أو الأماكن المغلقة المتصلة بها بعد غروب الشمس وقبل شروقها فيما عدا حالة الاستعجال فيجوز للقاضي بأمر مكتوب أن يجري التفتيش ليلاً ".[208]

وأكد على ذلك قانون الإجراءات الجنائية الفرنسي في المادة (59) فقرة (1) حيث نصت على أنه " فيما عدا الاستغاثة الصادرة من داخل المنزل أو الاستثناءات المقررة بواسطة القانون فإن التفتيش ودخول المنازل لا يمكن أن يبدأ قبل الساعة السادسة صباحاً ولا بعد الساعة التاسعة مساءً ".[209]

ووفقاً لهذا النص فإن تفتيش المساكن والدخول إليها فيما عدا حالة المطالبة من الداخل كما في الاستغاثة أو الحريق أو الغرق ، إن الأحوال المنصوص عليها قانوناً لا يجوز أن يبدأ قبل الساعة السادسة صباحاً ولا بعد الساعة التاسعة مساءً .

أما بالنسبة لتفتيش مسرح الجرائم الإلكترونية الموجودة في المساكن وما في حكمها ، فلا توجد نصوص تشريعية تحدد وقتاً معيناً يتم فيه إجراء تفتيشها سواءً في ليبيا أو في القوانين المقارنة ، إلا أننا نرى عدم تحديد وقت معين لتنفيذ التفتيش وتركه لسلطة المحقق التقديرية فقط فيما يتعلق بتفتيش مسرح الجرائم الإلكترونية ذلك لأن الوقت الذي تكثر فيه الجرائم الإلكترونية هو ليلاً ولعدة أسباب منها سهولة الاتصال لسهولة الدخول إلى المواقع المراد التلاعب بها ، وذلك بسبب قلة المستخدمين في مثل هذا الوقت في المؤسسات والبنوك العامة والخاصة .

ثالثاً . تحرير محضر التفتيش في الجرائم الإلكترونية :

يشترط لصحة التفتيش الذي يعتبر عملاً من أعمال التحقيق ، أن يتم عن طريق تحرير محضر يثبت فيه ما تم من إجراءات ، وما أسفر عنه من أدلة ، حيث أن المشرّع الليبي لم يتطلب شكلاً معيناً في محضر التفتيش ، ومن ثم فإنه لا يشترط لصحته سوى ماتستوجبه القواعد العامة في المحاضر عموماً.[210] .

ومقتضى تلك القواعد العامة أن يكون المحضر مكتوباً باللغة الرسمية للدولة ، وأن يحمل تاريخ تحريره وتوقيع محرره ، كما ينبغي أن يتضمن كافة الإجراءات التي اتخذت بشأن

---

[208] بكري يوسف بكري ، مرجع سابق ، ص85 .

[209] محمد محمود الشركسي ، مرجع سابق ، ص194 .

[210] المادة (57) من قانون الإجراءات الجنائية الليبي التي تنص بأنه " يستصحب قاضي التحقيق في جميع إجراءاته كاتباً من كتاب المحكمة يوقع معه المحاضر وتحفظ هذه المحاضر مع الأوامر وباقي الأوراق في قلم كتاب المحكمة " .

الوقائع التي يثبتها[211]، لكي تكون حجة يعامل الموظفون الأمرون منهم والمؤتمرون بمقتضاها ، ولتكون أساساً صالحاً لما بني عليه من النتائج.[212] .

أما بالنسبة لمحضر التفتيش في الجرائم الإلكترونية ، فإنه لابد بالإضافة إلى ما سبق ذكره أن يكون قاضي التحقيق أو النيابة العامة أو مأمور الضبط القضائي لديه علم بثقافة تكنولوجيا المعلومات هذا من جانب ، ومن جانب آخر لابد وأن يستعين بشخص متخصص في مجال الحاسوب والإنترنت ، لصياغة محضر التفتيش بحيث تتم تغطية كل الجوانب الفنية أثناء القيام بعملية التفتيش والضبط ، بالإضافة إلى المحافظة على الأدلة المتحصل عليها من كل تلف أو مسح.[213] .

---

[211] قدري عبدالفتاح الشهاوي ، مرجع سابق ، ص160 .

[212] هشام عبدالحميد الجميلي ، مرجع سابق ، ص562 .

[213] حسين بن سعيد الغافري ، السياسة الجنائية في مواجهة جرائم الانترنت ، مرجع سابق ، ص495 .

- علي حسن محمد الطوالبة ، مرجع سابق ، ص60 .

المطلب الثالث

ضبط الدليل في الجرائم الإلكترونية

يهدف التفتيش إلى ضبط الأدلة المادية التي تفيد في كشف الحقيقة ، فالضبط[1] هو هدف التفتيش وغايته أي الأثر المباشر الذي ينتج عن هذا الإجراء[2] .

ولما كان الضبط هو الأثر المباشر للتفتيش ، وباعتباره أحد إجراءات التحقيق فتنطبق عليه القواعد التي تنطبق على التفتيش[3] ، ويقع الضبط في القواعد العامة على الأشياء المادية فقط مثل ضبط المنقولات والعقارات[4] ، ولا ينصب الضبط على الأشياء المعنوية لأنها لاتصلح محلاً لوضع اليد على الشيء[5] .

وبالتالي فإنه يثار التساؤل حول ضبط الكيانات المادية والمعنوية للحاسب الآلي وشبكة الإنترنت ، فهل تسري القواعد العامة للضبط على الكيانات المادية والمعنوية لجهاز الحاسب الآلي والإنترنت ؟ للإجابة على هذا التساؤل سنقسم هذا المطلب إلى فرعين : نخصص الفرع الأول لدراسة ضبط الكيانات المادية في الجرائم الإلكترونية . ونكرس الفرع الثاني لدراسة ضبط الكيانات المعنوية في الجرائم الإلكترونية .

الفرع الأول

ضبط الكيانات المادية في الجرائم الإلكترونية

يُقصد بالكيانات المادية في الجرائم الإلكترونية الأشياء المادية التي تفيد في إظهار الحقيقة عن الجريمة محل البحث أو الأشياء التي تتصل بهذه الجريمة من الناحية المادية ، وبما أن الضبط ينصب على الأشياء المادية التي قد تكون منقولة أو عقارية ، فعلية سنتناول في هذا الفرع دراسة ضبط المنقولات في الجرائم الإلكترونية . ووضع الأختام على العقارات في الجرائم الإلكترونية ، وذلك في الفقرتين التاليتين :

---

[1] الضبط : هو " وضع اليد على شيء يتعلق بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبها " .
(محمد زكي أبو عامر ، الاجراءات الجنائية ، مرجع سابق ، ص701).

[2] قدري عبدالفتاح الشهاوي ، مرجع سابق ، ص167 .

[3] محمود مصطفى ، شرح قانون الاجراءات الجنائية ، مرجع سابق ، ص248 .

[4] عوض محمد عوض ، المبادئ العامة في قانون الإجراءات الجنائية ، مرجع سابق ، ص395 .

[5] محمد زكي أبو عامر ، الاجراءات الجنائية ،المرجع السابق ، ص701 .

أولاً . ضبط المنقولات في الجرائم الإلكترونية :

نصت المادة (43) إج ليبي على أنه " لمأمور الضبط القضائي أن يضبط الأوراق والأسلحة والآلات ، وكل ما يحتمل أن يكون قد استعمل في ارتكاب الجريمة ، أو نتج عن ارتكابها ، أو ما وقعت عليه الجريمة وكل ما يفيد في كشف الحقيقة..... "[214] .

كما نصت المادة (2/75) إج ليبي على أنه " للمحقق أن يفتش أي مكان ويضبط فيه الأوراق والأسلحة والآلات وكل ما يحتمل انه استعمل في ارتكاب الجريمة أو نتج عنها أو وقعت عليه وكل ما يفيد في كشف الحقيقة "[215] .

وكما هو ملاحظ من هذين النصين ، أن المشرّع بعد أن عدد الأشياء التي يمكن أن تضبط ، واستخدامه مصطلح كل ما يفيد في كشف الحقيقة ، فهذا يعني أن التحديد السابق ورد على سبيل المثال لا الحصر ، فوجود صلة بين الجريمة والأشياء التي يتم ضبطها هو معيار الضبط[216] .

ويخضع ضبط المنقولات[217] لسلسلة من الإجراءات التي نصت عليها المواد (43 ، 44 ، 45) إج ليبي ، فيما يتعلق بالضبط الذي يباشره مأمور الضبط القضائي ، وأحالت المادة (82) إج ليبي بالضبط الذي يباشره قاضي التحقيق أو النيابة العامة إلى المادة (44) إج ليبي وباستقراء هذه المواد المذكورة ، يتبين أن هذه القواعد الشكلية تتمثل في وجوب عرض الأشياء المضبوطة على المتهم وإبداء ملاحظاته عليها ، وعمل محضر بذلك يوقع عليه المتهم أو يذكر امتناعه عن التوقيع ، كما تتطلب وجوب وضع الأشياء والأوراق المضبوطة في حرز مغلق ، وربطها كل ما أمكن ذلك ، وختمها وكتابة تاريخ المحضر المحرر لضبط تلك الأشياء داخلها ، والإشارة إلى موضوع الضبط ، كما لا تفض الأختام الموضوعة على الأحراز المغلقة طبقاً للمادة (44) إج ليبي[218] أو الموضوعة على الأماكن التي بها آثار أو أشياء تفيد في كشف الحقيقة طبقاً للمادة (42) إج ليبي إلا بحضور المتهم ، أو وكيله دون أن يستلزم حضورهما معاً وقت فض الأختام ، طبقاً للمادة (45) إج ليبي.

---

[214] ويقابل ذلك المادة (55) من قانون الإجراءات الجنائية المصري.

[215] ويقابل ذلك المادة (91) من قانون الإجراءات الجنائية المصري.

[216] محمود نجيب حسني ، مرجع سابق ، ص 683.

[217] يختلف مصطلح المنقول في القانون الجنائي ، عنه في القانون المدني ، فالمنقول في القانون المدني : هو الشيء الذي يمكن نقله من مكان لآخر دون تلف ، في حين أنه يشمل وفقاً لمفهومه في القانون الجنائي ، المنقول بطبيعته كالأوراق والأسلحة والأجهزة وما يُعد عقاراً بالتخصيص وهو منقول بطبيعته ، ولكنه مخصص لخدمة عقار أو الاستغلال له كالآلات الزراعية ومعدات المصنع والعقار بالاتصال وهو منقول بطبيعته ولكنه اتصل بالعقار فيأخذ حكمه فنوافذ وأبواب المنازل والأجزاء التي يمكن نزعها مع العقار بطبيعته كالأشجار المزروعة . (محمد رمضان باره ، جرائم الاعتداء على الأموال ، مرجع سابق ، ص97 - 98) .

[218] ويقابل ذلك المواد (55 ، 56 ، 57 ، 98) من قانون الإجراءات الجنائية المصري.

وإذا وجد مأمور الضبط القضائي في منزل المتهم أوراقاً مختومة أو مغلقة بأية طريقة فلا يجوز له فضها وفقاً لقانون الإجراءات الجنائية الليبي ، حيث حدد المشرّع الليبي اختصاص قاضي التحقيق بفض الأوراق والإطلاع عليها وله أن يكلف أحد أعضاء النيابة العامة بفرز الأوراق المادة (81) إج ليبي ، وقد قرر المشرّع الليبي استثناء من قواعد الضبط المذكورة حرم به على المحقق ، أن يضبط لدى المدافع عن المتهم أو الخبير الاستشاري ، الأوراق والمستندات التي سلمها المتهم لهما لأداء المهمة التي عهد إليهما بها والمراسلات المتبادلة بينهما في القضية المادة (80) إج ليبي[219] .

ويبرر هذا الاستثناء حرص المشرّع على كفالة حرية الدفاع للمتهم ، ويلاحظ أنه وإن كان المشرّع قد نص على عدم جواز ضبط الأوراق والمستندات لدى المدافع أو الخبير إلا أن حكمة الاستثناء توجب مد نطاقه إلى عدم ضبط هذه الأوراق والمستندات إينما وجدت ، أي سواءً لدى المدافع أو الخبير أو في مكاتب البريد أو التلغراف[220] ، بل أنها توجب مد نطاقه إلى المحادثات الهاتفية والأحاديث الخاصة التي تحدث بين المتهم والمدافع أو الخبير الاستشاري[221] كما أنه ليس للنيابة العامة ضبط الخطابات والرسائل إلا بناءً على أذن من القاضي الجزئي المادة (180) إج ليبي وعلة اشتراط أذن القاضي الجزئي فيما تجريه النيابة العامة من ضبط الرسائل ومراقبة المحادثات وإجراء التسجيلات تتعلق بها مصلحة لغير المتهم غير أن إصدار الأذن يخضع لتقدير القاضي الجزئي تحت إشراف قاضي الموضوع[222] .

أما فيما يتعلق بضبط المكونات المادية في الجرائم الإلكترونية ، لا يوجد خلاف بين فقهاء القانون في إمكانية ضبط هذه المكونات[223] ، وهي وحدات الإدخال مثل لوحة المفاتيح وشاشة اللمس والفأرة ، ووحدات الإخراج كالشاشة والطابعة والرسم ، وكوحدات التخزين الثانوية بما تشمله من أقراص صلبة ومرنة وأشرطة مغناطيسية .

كذلك مكونات جهاز الهاتف النقال المادية كالجسم الخارجي والسماعة والبطارية والميكروفون ومكونات كاميرا المراقبة المادية كالشاشة ، ووحدة الإرسال ووحدة الاستقبال ومكونات كاميرا التصوير ، والفيديو المادية ، كالجسم الخارجي والأشرطة الممغنطة والخاصة

---

[219] ويقابل ذلك المادة (96) من قانون الإجراءات الجنائية المصري .

[220] محمود مصطفى ، شرح قانون الاجراءات الجنائية ، مرجع سابق ، ص248 .

[221] فوزية عبدالستار ، مرجع سابق ، ص342 .

[222] جلال ثروت ، نظم الاجراءات الجنائية وفقاً لآخر التعديلات ، مطابع السعدني ، 2004 ، ص431 .

[223] أمير فرج يوسف ، مرجع سابق ، ص237 .

- هلالي عبداللاه أحمد ، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي ، مرجع سابق ، ص198 .

بالتصوير الصوتي والمرئي وأجهزة الاستقبال والمعالجة .فكل هذه المكونات المادية التي يمكن اعتبارها دليلاً في الجرائم الإلكترونية ، لا تثير أي صعوبة في ضبطها .

ومن التشريعات التي تجيز ضبط المكونات المادية في الجرائم الإلكترونية ، وذلك من خلال ما تمنحه لسلطة التحقيق من اتخاذ الإجراءات أو أي شيء لازم لجمع أدلة الجريمة والحفاظ عليها ، منها نص المادة (83) إج ليبي التي تنص أنه " لقاضي التحقيق أن يأمر لحائز الشيء يرى ضبطه أو الإطلاع عليه بتقديمه..... " .

وكذلك نصت المادة (75) إج ليبي التي نصت على أنه " للمحقق أن يفتش أي مكان ويضبط فيه الأوراق والأسلحة والآلات وكل ما يحتمل أنه استعمل في ارتكاب الجريمة أو نتج عنها أو وقعت وكل ما يفيد في كشف الحقيقة " ، وكما نصت المادة (43) إج ليبي على أنه "لمأموري الضبط القضائي أن يضبطوا الأوراق والأسلحة والآلات وكل ما يحتمل أن يكون قد استعمل في ارتكاب الجريمة أو نتج عن ارتكابها ، أو ما وقعت عليه الجريمة ، وكل ما يفيد في كشف الحقيقة..... "[224] .

ويُلاحظ من خلال المواد السابقة أنها قد منحت لسلطة التحقيق ولمأموري الضبط القضائي ضبط جميع الأشياء التي تفيد في كشف الحقيقة بما في ذلك الأوراق والأسلحة التي استعملت في ارتكاب الجريمة أو التي أعدت لاستعمالها ، وبناءً على ذلك يمكن أن يشمل مصطلح الأشياء المكونات المادية في الجرائم الإلكترونية ، سواءً وجدت عند المتهم أم عند غيره فاستخدام مصطلح الأشياء يمكن أن يتسع ليشمل مدخلات ومخرجات الحاسوب كلوحة المفاتيح وشاشة اللمس أو نظام الفأرة أو الماسح الضوئي (اسكنر) ، أو الطابعة التي تستخدم في ارتكاب الجرائم الإلكترونية ، فعلى سبيل المثال حصل المفتشون في قضية usv simpson على أذن بضبط قرص من Diskettes خاص بجهاز حاسب آلي المتهم بناءً على سبب معقول يعتقد أن حاسوب المتهم المذكور يحتوي على صور داعرة للأطفال ، وقام المفتشون بضبط الحاسب الآلي ، ثم قاموا بتفتيشه وهو في حوزة الشرطة ووجدوا فيه صوراً داعرة للأطفال[225] .

ثانياً . وضع الأختام على العقارات الموجود بها المنقولات في الجرائم الإلكترونية :

قلنا فيما سبق أن ضبط المكونات المادية لجهاز الحاسب الآلي وشبكة الإنترنت ، وغير ذلك من الوسائل التقنية ، التي تستخدم في ارتكاب الجرائم الإلكترونية ، يشمل بالإضافة المنقولات المادية التي سبق أن أشرنا إليها ، والتي لا تثير أي مشكلة فقهية أو قانونية ، لأنه يدخل

---

[224] ويقابل ذلك المواد (55 ، 91 ، 99) من قانون الاجراءات الجنائية المصري.

[225] عمر محمد بن يونس ، الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي ، المرشد الفيدرالي الأمريكي لتفتيش وضبط الحواسيب وصولاً إلى الدليل الإلكتروني في التحقيقات الجنائية ، الطبعة الأولى، 2005 ، ص254.

في مضمون التفتيش الذي تنص عليه التشريعات الإجرائية لمختلف الدول ، فإنها تشمل أيضاً العقارات الكائنة بها هذه المنقولات .

وفي هذا الخصوص تنص المادة (42) إج ليبي على أنه " لمأموري الضبط القضائي أن يضعوا الأختام على الأماكن التي بها أثار أو أشياء تفيد في كشف الحقيقة ، ولهم أن يقيموا حراساً عليها ، ويجب عليهم إخطار النيابة العامة بذلك في الحال ، وعلى النيابة العامة إذا رأت عدم ضرورة ذلك الإجراء أن تأمر بإزالة الأختام ، فإذا رأت إبقائها جاز لحائز العقار أن يتظلم أمام القاضي الجزئي بعريضة يقدمها إلى النيابة العامة ، وعليها رفع التظلم إلى القاضي فوراً "[226]

وعليه أن هذه الأحكام التقليدية المتعلقة بضبط العقارات هي التي تنطبق على ضبط العقارات الكائن بها جهاز الحاسب الآلي أو شبكة الإنترنت ، وغير ذلك من الوسائل التقنية الحديثة التي استخدمت في ارتكاب الجرائم الإلكترونية .

الفرع الثاني

ضبط الكيانات المعنوية في الجرائم الإلكترونية

اختلفت الاتجاهات الفقهية فيما يتعلق بضبط البيانات المعالجة بواسطة وسائل تقنية المعلومات إلى ثلاث اتجاهات .

الاتجاه الأول : يرى أنصار هذا الاتجاه أنه لا يمكن تصور إجراء الضبط على البيانات المعالجة إلكترونياً بواسطة جهاز الحاسب الآلي وشبكة الإنترنت لانتفاء الكيان المادي عنها ، ولا سبيل لضبطها إلا بعد نقلها على كيان مادي ملموس كطباعتها على الورق أو إفراغ بياناتها على الأقراص المرنة.[227] .

ومن التشريعات التي أخذت بهذا الاتجاه قانون الإجراءات الجنائية الألماني ، فقد حددت المادة (94) منه محل الضبط يقع على الأشياء المادية الملموسة ، ويفسر الفقه الألماني نص هذه المادة ، بأن البيانات المعالجة إلكترونياً لا يمكن ضبطها مجردة ، ذلك لأنها تفتقد الكيان المادي لكن عند تحويلها أو إضافتها إلى مكون مادي يمكن ضبطه مثل طباعة هذه البيانات على الورق كما يمكن ضبط البيانات أيضاً بالتصوير من الشاشة ، ومن ثم يمكن التعامل معها ضمن ما تنص عليه المادة (161) إج ألماني التي تجيز الحصول على البيانات المعروضة على شاشة الحاسوب عن طريق التصوير الفوتوغرافي أو بنقلها على دعامة مادية.[228]

---

[226] ويقابل ذلك المواد (53 ، 54) من قانون الإجراءات الجنائية المصري.

[227] محمد أبو العلا عقيدة ، مرجع سابق ، ص11 .

[228] أسامة بن غانم العبيدي ، مرجع سابق ، ص109

- سليمان أحمد فضل ، مرجع سابق ، ص321 – 322.

الاتجاه الثاني : يرى أصحاب هذا الاتجاه أنه لا مانع من أن يرد الضبط على البيانات والمعلومات الكائنة بالحاسب الآلي[229] ، غير أنه يميز أنصار هذا الاتجاه بين المعلومات والبيانات المعالجة إلكترونياً ، فينفي الطابع المادي عن أولها ، ويؤكد الثانية طابعاً مادياً على أساس أنها نبضات أو ذبذبات إلكترونية أو موجات كهرومغناطيسية قابلة لأن تسجل وتخزن على وسائط معينة ويمكن قياسها ، وبالتالي ينفون الطابع المعنوي لهذه البيانات مؤكدين أنها شيء يمكن لمسه في المحيط الخارجي وأنها كيان مادي لا يمكن إنكاره، مستندين في ذلك إلى حكم محكمة النقض الفرنسية حيث قضت بأنه " سرقة الأقراص المغناطيسية (الديسكات) يتضمن في الوقت ذاته سرقة محتوياتها المعلوماتية للفترة الزمنية التي تكون محملة بها وبناء على ذلك فإن ضبط الأدلة المتحصلة من التفتيش ، يمكن أن يقع على الكيانات المعنوية في الوسائل الإلكترونية ، ومثال ذلك يمكن ضبط البيانات الإلكترونية"[230] .

ومن التشريعات التي أخذت بهذا الاتجاه قانون الإجراءات الجنائية اليوناني في المادة (251) والتي تعطي سلطة التحقيق إجازة القيام (بأي شيء) وهذا يعني أن التحقيق يشمل ضبط البيانات المخزنة أو المعالجة إلكترونياً.[231]

ويجيز قانون الإجراءات الجنائية الكندي في المادة (421) ، 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 ينص قانون الإثبات الكندي في المادة (29) منه 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 المواد المكتوبة وينطبق هذا النص سواءً كانت السجلات 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 "[232] .

ومن التشريعات العربية التي أجازت ضبط الأشياء المتعلقة بالجرائم الإلكترونيه القانون الأردني حيث نصت المادة (13/ب) على أنه " مع مراعاة حقوق الآخرين ذوي النية الحسنة

---

[229] علي محمود علي حمودة ، مرجع سابق ، بدون ترقيم صفحات .
- رامي متولي القاضي ، مرجع سابق ، ص120.
- محمد أبو العلا عقيدة ، مرجع سابق ، ص11 .

[230] علي محمود علي حمودة ، المرجع السابق ، بدون ترقيم صفحات .

[231] هلالي عبداللاه أحمد ، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي ، مرجع سابق ، ص200 وما بعدها .

[232] أسامة بن غانم العبيدي ، مرجع سابق ، ص110 .

باستثناء المرخص لهم وفق أحكام قانون الاتصالات ممن لم يشتركوا بأي جريمة منصوص عليها في هذا القانون يجوز لموظفي الضابطية العدلية ضبط الأجهزة والأدوات والبرامج والأنظمة والوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها أو يشملها هذا القانون ، والأموال المتحصلة منها والتحفظ على المعلومات والبيانات المتعلقة بارتكاب أي منها " .

الاتجاه الثالث : ويأخذ أصحاب هذا الاتجاه الموقف الوسط ، وذلك بدعوتهم إلى ضرورة تدخل تشريعي لتوسيع دائرة الأشياء التي يمكن أن يرد عليها الضبط ، لتشمل إلى جانب الأشياء المادية البيانات المعالجة إلكترونياً.[233]

ومن خلال الموازنة بين تلك الاتجاهات نرجح ونؤيد الاتجاه الثالث لأنه لابد من تطوير النصوص الإجرائية المتعلقة بالضبط في الجرائم الإلكترونية لتشمل البيانات المعالجة إلكترونياً ، وإلا أدى ذلك إلى العديد من الصعوبات من الناحية التشريعية لعدم وجود نصوص خاصة بذلك ويتعين بعد ضبط البيانات الإلكترونية ، أن يتم تحريزها أو تأمينها فنياً، خاصة أمام عدم إلمام المحقق الجنائي أو مأمور الضبط القضائي بالثقافة المعلوماتية ، مما يؤدي بتلك الأدلة إلى الإتلاف ، مما يجب اتخاذ بعض الإجراءات الخاصة للحفاظ على تلك الأدلة من العبث[234] وذلك على النحو التالي :

أ) يجب حمل الأقراص من الجزء العلوي لها عند علامة الشركة وإدخالها أو إخراجها من مشغل الأقراص برفق للمحافظة على القرص والمشغل .

ب) عدم لمس الأجزاء المكشوفة من الأقراص ، حتى لا تتعرض البيانات المسجلة عليها إلى تلف .

ج) عدم وضع أشياء ثقيلة على القرص كالكتب مثلاً ، بالإضافة إلى إبعاد القرص عن أشعة الشمس .

د) ضبط الدعائم الأصلية للبيانات ، وعدم الاعتماد على ضبط نسخها .

هـ) الالتزام بالقواعد الفنية المتعلقة بطريقة نقل الأحراز المعلوماتية ، كعدم وضعها في أماكن متربة .

و) تأمين البرامج المضبوطة قبل تشغيلها فنياً ، وعمل نسخ منها سليمة .

---

(233) مفتاح أبوبكر المطردي ، مرجع سابق ، ص46-47.

(234) حسين بن سعيد الغافري ، السياسة الجنائية في مواجهة جرائم الانترنت ، مرجع سابق ، ص465-466.

- علي حسن محمد الطوالبة ، مرجع سابق ، ص167 وما بعدها .

- هلالي عبداللاه أحمد ، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي ، مرجع سابق ، ص209-210.

ن) إحكام الحلقات الإجرائية للضبط التي مرت بها المادة المعلوماتية لتأمين سلامتها من الإتلاف من لحظة اكتشافها وفي لحظة تقديمها للمحكمة .

ي) تمييز المادة المضبوطة بوضع علامة مادية خاصة بها من قِبل كل من كانت في حيازته.

المطلب الرابع

الشهادة في الجرائم الإلكترونية

سنتناول في هذا المطلب تعريف الشهادة وأهميتها وذلك في فرع أول . أما الفرع الثاني سنخصصه لدراسة التزامات الشاهد في الجرائم الإلكترونية ، وذلك على النحو التالي :

الفرع الأول

تعريف الشهادة وأهميتها

أولاً . تعريف الشهادة في الجرائم الإلكترونية :

يُقصد بالشهادة بوجه عام هي "إخبار شخص غير خصم في الدعوى الجنائية ، مقبولة شهادته أمام القضاء إثباتاً أو نفياً عما أدركه عن واقعة رؤية أو سماعاً"[235] أو هي " إثبات واقعة معينة من خلال ما يقوله أحد الأشخاص كما شاهده أو سمعه أو أدركه بحواسه من هذه الواقعة بطريقة مباشرة "[236] .

أما البعض الآخر من الفقه فقد عرفها بأنها " المعلومات التي وصلت إلى الشخص بأي حاسة من حواسه عن الواقعة محل الشهادة ، ومطابقة تلك الواقعة لحقيقتها التي يشهد بها سواءً في مرحلة الاستدلال أو في مرحلة التحقيق أو القضاء "[237]

أما تعريف الشاهد في الجرائم الإلكترونية فيقصد به " الفني صاحب الخبرة والتخصص في تقنية الحاسب الآلي وشبكات الاتصال ، الذي تكون لديه معلومات جوهرية أو هامة ، لازمة للولوج إلى نظام المعالجة الآلية للبيانات ، إذ كانت مصلحة التحقيق تقتضي التنقيب أو البحث عن أدلة الجريمة داخله "[238] ويختلف الشاهد في الجرائم الإلكترونية عن الشهادة الالكترونية حيث يقصد بهذه الأخيرة هي "الشهادة التي تتم عن طريق الاتصال بالشاهد عبر الوسائل والتقنيات الحديثة ، ومنها نظام الاتصال المرئي المسموح عبر الانترنت للادلاء بالشهادة"[239]، ويشمل الشاهد في الجرائم الإلكترونية عدة طوائف[240] أهمها:

---

[235] سعد حماد صالح القباتلي ، الشهادة أمام القضاء الجنائي (دراسة نظرية وتطبيقية مقارنة بالشريعة الاسلامية) ، الطبعة الأولى الدار العالمية للنشر والتوزيع ، الإسكندرية ، 2014 ، ص24.

[236] عاطف شعبان ، الإثبات الجنائي في مرحلة التحقيق النهائي في ضوء الفقه والقضاء ، الطبعة الثانية ، 1994 ، ص211 .

[237] أحمد يوسف سوليه ، الحماية الجنائية والأمنية للشاهد ، دار الفكر الجامعي ، الإسكندرية ، 2007 ، ص9 .

[238] هلالي عبداللاه أحمد ، التزام الشاهد بالإعلام في الجرائم المعلوماتية ، الطبعة الثانية ، دار النهضة العربية القاهرة ، 2008 ، ص23.

[239] أحمد محمود موافي ، الجرائم الالكترونية وشبكة الانترنت ، دار نور الاسلام للطباعة والنشر والتوزيع ، القاهرة ، ص85.

[240] حسين بن سعيد الغافري ، السياسة الجنائية في مواجهة جرائم الانترنت ، مرجع سابق ، ص 467 – 468 .
- مصطفى محمد موسى ، مرجع سابق ، ص 223 – 224.

أ) القائم على تشغيل جهاز الحاسب الآلي :

هو المختص بتشغيل جهاز الحاسب الآلي ومكوناته ، ولديه خبرة في قواعد كتابة البرامج واستخدام أدوات إدخال البيانات .

ب) المبرمجون :

وهم المختصون في كتابة أوامر البرامج ، سواءً كانت برامج النظم أو برامج التطبيقات فالمختص ببرامج النظم يقوم باختيار وتعديل وتصحيح برامج الحاسب الآلي الداخلية ، أي أنه يقوم بالوظائف الخاصة بتجهيز الحاسب الآلي بالبرامج والأجزاء الداخلية التي تتحكم في وحدات الإدخال والإخراج ، أما المختص بكتابة أوامر التطبيقات يعرف مواصفات النظام الإداري المطلوب من محلل النظم ثم يقوم بتحويل ذلك إلى برامج رقمية .

ج) المحللون :

هم الأشخاص الذين يحللون خطوات العمل ، ويقومون بتجميع بيانات معينة ، ودارستها وتحليلها وذلك بتقسيم النظام إلى وحدات ، كما يقومون بتتبع البيانات داخل النظام ، عن طريق ما يسمى بمخطط تدفق البيانات ، واستنتاج الأماكن التي يمكن ميكنتها بواسطة جهاز الحاسب الآلي .

د) مهندسو الصيانة والاتصالات :

وهم الأشخاص المسئولون عن صيانة جهاز الحاسب الآلي بمكوناته المادية والمعنوية وشبكة الإنترنت .

هـ) مدير النظام المعلوماتي :

وهو الذي يوكل له أعمال الإدارة من حيث تأمين عمل الشبكة وكذلك مراقبة الأمن وإصلاح الشبكة حال ظهور المشكلات.[241]

ثانياً . أهمية الشهادة في الجرائم الإلكترونية :

تعتبر شهادة الشهود بصفة عامة ، من الأدلة المهمة أمام سلطة التحقيق والقضاء ، ويحظى الدليل المستمد منها باهتمام المحقق أو القاضي ، فالشهود هم عيون المحكمة وأذانها كما أن الشهادة غالباً ما تقوم بدور الدليل في الدعوى ، دون أن يساندها دليل آخر ، ومن ثم فإن الشهادة الصادقة هي خير معين للقاضي في تكوين قناعته.[242]

---

[241] عمر محمد بن يونس ، الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي ، مرجع سابق ، ص95 .

[242] مأمون محمد سلامة ، الإجراءات الجنائية في التشريع المصري ،ج2 ، دار الفكر العربي ، القاهرة ، ص199 .

وللشهادة أهميتها العملية في الدعوى الجنائية ، حيث يتطلب الحال إثبات وقائع مادية لا يمكن الحصول مقدماً على أدلة عليها ، ولذا تعتبر الشهادة هي الوسيلة العادية لاكتشاف الحقيقة وإثباتها[243]، لأنها تنصب على الواقعة مباشرة ، باعتبارها دليل مباشر شفهي ، حيث أن الشاهد يدلي بشهادته شفهياً أمام السلطة المختصة[244]، ومن ثم لا يجوز الاستعانة بمذكرات مكتوبة إلا بإذن من المحكمة أو القاضي المنتدب[245] ، ذلك لأن القاعدة العامة تلزم الشاهد بالإدلاء بما يعلمه من معلومات بخصوص واقعة الجريمة والفاعلين فيها وكل ما يفيد في كشف الحقيقة من وقائع أخرى.[246]

فالشهادة في الجرائم الإلكترونية لا تقل أهمية عن باقي وسائل جمع الدليل الرقمي ، فطبقاً للقواعد العامة في الشهادة ، تقتضي بأنه لا يلتزم الشاهد إلا بذكر ما يعلمه ولا يجوز إكراهه على القيام بسلوك معين ، وهذا يؤكد أهمية وجود قواعد خاصة في هذا المجال لكي تفرض واجب التعاون مع الجهة القضائية في أثناء التحقيقات والمحاكمة على الشاهد .

- مصطفى مجدي هرجة ، شهادة الشهود في المجالين الجنائي والمدني وشهادة الزور واليمين الكاذبة ، دار محمود للنشر والتوزيع ، القاهرة ، ص21 - 22 .

[243] جندي عبدالملك ، الموسوعة الجنائية ، الجزء الأول ، دار إحياء التراث العربي ، بيروت ، لبنان ، 1976 ، ص124 .

[244] خالد عبدالعظيم أبو غابة وآخرون ، مدى حجية الشهادة والقرائن وضوابط مشروعيتها في الاثبات ، دراسة مقارنة بين النظم الاسلامية والانظمة الوضعية ، الطبعة الاولى ، دار الفكر الجامعي ، الاسكندرية ، 2013 ، ص 47.

[245] مصطفى يوسف ، مشروعية الدليل في المسائل الجنائية في ضوء الفقه والقضاء ، الطبعة الاولى ، 2010 ، ص106.

[246] المادة (93) من قانون الاجراءات الجنائية الليبي " يسمع قاضي التحقيق شهادة من يرى لزوم سماعه من الشهود عن الوقائع التي تثبت أو تؤدي إلى ثبوت الجريمة وظروفها وإسنادها إلى المتهم أو براءته منها " .

الفرع الثاني
التزامات الشاهد في الجرائم الإلكترونية

سنتناول في هذا الفرع دراسة التزامات الشاهد في الجرائم الإلكترونية ، من حيث التزام الشاهد بواجب الحضور ، وحلف اليمين القانونية ، وقول الحقيقة وذلك على النحو التالي :

أولاً . الحضور الضروري أمام الجهة القضائية التي استدعته :

يلتزم الشاهد بالحضور أمام الجهة القضائية التي استدعته في الموعد والمكان المحددين[247]. ويكون تكليف الشهود بالحضور بواسطة المحضرين أو بواسطة رجال السلطة العامة[248]. ويجب على الشاهد أن يحضر بناءً على الطلب المحرر إليه ، وإلا جاز للقاضي الحكم عليه بعد سماع أقوال النيابة العامة ، بدفع غرامة ، ويجوز له أن يصدر أمراً بتكليفه بالحضور ثانياً بمصاريف من طرفه ، أو أن يصدر أمراً بضبطه وإحضاره[249]، وإذا حضر الشاهد أمام الجهة القضائية التي استدعته بعد تكليفه بالحضور ثانياً أو من تلقاء نفسه وأبدى أعذاراً مقبولة جاز إعفاؤه من الغرامة بعد سماع أقوال النيابة العامة ، كما يجوز إعفاؤه بناءً على طلب يقدم منه إذا لم يستطع الحضور بنفسه.[250] .

وإذا لم يحضر الشاهد في المرة الثانية ، جاز الحكم عليه بغرامة لا تتجاوز ضعف الحد الأقصى المقررة في المادة (253) من قانون الإجراءات الجنائية الليبي.[251]

أما إذا كانت المحكمة هي التي تقوم بالتحقيق ، جاز لها إذا اعتذر الشاهد بأعذار مقبولة من عدم إمكانية الحضور ، أن تنتقل إليه وتسمع شهادته بعد إخطار النيابة العامة ، وباقي الخصوم ، وللخصوم أن يحضروا بأنفسهم أو بواسطة وكلائهم ، وأن يوجهوا للشاهد الأسئلة التي يرون لزوم توجيهها إليه[252] ، وقد قرر المشرّع هذا الإجراء حرصاً على الحيلولة دون إدعاء الشاهد المرض خلافاً للحقيقة.[253]

---

[247] عوض محمد عوض ، المبادئ العامة في قانون الإجراءات الجنائية ، مرجع سابق ، ص414 .

[248] المادة (94) من قانون الاجراءات الجنائية الليبي، ويقابل ذلك المادة(111)من قانون الاجراءات الجنائية المصري .

[249] أنظر المواد (99 ، 250 ، 252 ، 253) من قانون الاجراءات الجنائية الليبي ، ويقابل ذلك المادة (117-118) من قانون الاجراءات الجنائية المصري .

[250] المادة (100) من قانون الاجراءات الجنائية الليبي ، ويقابل ذلك المادة (118) من قانون الاجراءات الجنائية المصري.

[251] ويقابل ذلك المادة (2/280) من قانون الاجراءات الجنائية المصري.

[252] انظر المادة (254) من قانون الاجراءات الجنائية الليبي ، ويقابل ذلك المادة (279) من قانون الاجراءات الجنائية المصري.

[253] فوزية عبدالستار ، مرجع سابق ، ص350 .

ثانياً . قسم اليمين القانونية أمام الجهة القضائية التي استدعته :

يلزم المشرّع الليبي الشاهد أن يحلف اليمين قبل أدائه الشهادة سواء في مرحلة التحقيق الابتدائي أو في مرحلة المحاكمة[254] ، ذلك أن حلف اليمين يعني تنبيه شعور الشاهد بالمسئولية وإيقاظ ضميره ، بأن يتخذ الله رقيباً على صدق شهادته وأنه معرض لغضبه وانتقامه إن كذب فيها[255] ، ولا يجوز حلف الشهود اليمين في مرحلة جمع الاستدلالات إلا إذا خيف فيما بعد عدم استطاعة سماع الشهادة بيمين. [256]

ثالثاً . التزام الشاهد بقول الحقيقة أمام الجهة القضائية التي استدعته :

يلتزم الشاهد بذكر حقيقة ما يشهده أو ما يعلمه ، دون أن ينكر الحق أو أن يصمت عن بعض ما يعرفه ، وهذا يمنح للشهادة أن تؤدي دورها بوصفها دليل إثبات يتيح للقاضي تقديراً للوقائع بطريقة سليمة وصحيحة طبقاً للقانون.

فالكذب في الشهادة له خطورته ، إذ قد يترتب عليه تضليل القضاء في تطبيق العدالة ، وقد حرص المشرّع على ضمان صدق الشاهد بوسيلتين : الأولى : وسيلة معنوية تستهدف إيقاظ ضميره وإثارة خشيته من العقاب ، وهي إلزامه بأداء اليمين قبل الإدلاء بشهادته ، والثانية : وسيلة عقابية تستهدف إثارة خوفه من توقيع العقاب عليه ، وهي تقرير العقاب على الشهادة الكاذبة أي شهادة الزور[257]، ولا تتحقق ارتكاب جريمة شهادة الزور إلا إذا ارتكبت أمام المحكمة[258]، دون سلطة التحقيق إلا بعد أن تقرر المحكمة إقفال باب المرافعة إذ أنه إلى ذلك الوقت يجوز للشاهد أن يعدل عن شهادته ، وتعتبر شهادة الزور من جرائم الجلسات التي يجوز للقضاء الجنائي أن يحرك الدعوى الجنائية فيها بنفسه ، وتحكم على المتهم فيها بالعقوبة ولو حال انعقاد الجلسة[259] .

غير أن السؤال الذي يطرح نفسه هل يلتزم الشاهد المعلوماتي وفقاً للقواعد العامة لالتزامات الشاهد في قانون الإجراءات الجنائية ، بأن يقوم بطبع ملفات البيانات المخزنة في

---

[254] المادة (256) إج ليبي تنص " يجب على الشهود الذين بلغت سنهم أربعة عشر سنة أن يحلفوا يميناً قبل أداء الشهادة على أنهم يشهدون بالحق ولا يقولون إلا الحق وكل الحق ويجوز سماع الشهود الذين لم يبلغوا أربعة عشرة سنة كاملة بدون حلف اليمين على سبيل الاستدلال " .

[255] أحمد يوسف السوليه ، مرجع سابق ، ص61 - 86 .

[256] المادة (19) من قانون الاجراءات الجنائية الليبي ويقابل ذلك المادة (29) من قانون الإجراءات الجنائية المصري.

[257] فوزية عبدالستار ، مرجع سابق ، ص554 .

[258] المادة (266) عقوبات ليبي ، موسوعة التشريعات الجنائية ، قانون العقوبات ، منشور بالجريدة ، عدد خاص ، 1954.

[259] أحمد ضياء الدين محمد خليل ، مرجع سابق ، ص342 .

- رؤوف عبيد ، مرجع سابق ، ص707 .

ذاكرة الحاسب الآلي أو الإفصاح عن كلمات المرور والشفرات الخاصة بالبرامج؟ الإجابة على هذا التساؤل تتلخص في اتجاهين :

الاتجاه الأول : يرى أنصار هذا الاتجاه ، أنه ليس من واجب الشاهد طبقاً للالتزامات التقليدية للشهادة ، أن يقوم بطبع ملف البيانات أو الإفصاح عن كلمات المرور أو الشفرات الخاصة بالبرامج المختلفة ، ويميل إلى هذا الاتجاه الفقه الألماني حيث يرى عدم التزام الشاهد بطبع البيانات المخزنة في ذاكرة الحاسب على أساس أن الالتزام بأداء الشهادة لا يتضمن هذا الواجب.[260] .

الاتجاه الثاني : يرى أنصار هذا الاتجاه أن من بين الالتزامات التي تقع على الشاهد القيام بطبع ملفات البيانات أو الإفصاح عن كلمات المرور أو الشفرات الخاصة بالبرامج المختلفة حيث يرى البعض من الفقه الفرنسي أن القواعد العامة في مجال الإجراءات تحتفظ بسلطانها في مجال الإجراءات المعلوماتية ، ومن ثم يتعين على الشهود من حيث المبدأ الالتزام بتقديم شهادتهم المواد (62،109،438) إج فرنسي ، ومن ثم يجب عليهم الإفصاح عن كلمات المرور السرية التي يعلمونها ولا يعفيهم من هذا الالتزام سوى الاعتصام باحترام السر المهني.[261]

ومن خلال الموازنة بين الاتجاهين نرجح ونؤيد الاتجاه الأول الذي يقول بأنه ليس من واجب الشاهد طبقاً للالتزامات التقليدية الشهادة أن يقوم بطبع ملفات البيانات أو الإفصاح عن كلمات المرور أو الشفرات الخاصة بالبرامج المختلفة ، وذلك لأنه وفقاً للقواعد العامة في قانون الإجراءات الجنائية المتعلقة بالتزامات الشاهد ، لا تلزم الشاهد إلا بذكر ما يعلمه ، ولايجوز إجباره على القيام بسلوك معين ، وهذا مستفاد من نص المادة (257) من قانون الإجراءات الجنائية الليبي ، فالشاهد في الجرائم الإلكترونية متى كان حائزاً لمعلومات جوهرية لازمة للبحث عن أدلة تتطلبها مصلحة التحقيق ، فإنه يكون مطالباً بأن يعلم بها سلطات التحقيق ، والتحري على سبيل الاستدلال ، وإلا تعرض للعقوبات المقررة للامتناع عن الشهادة[262] .

---

[260] عبدالله حسين علي محمود ، سرقة المعلومات المخزنة في الحاسب الآلي ، مرجع سابق ، ص382 .
- سليمان أحمد فضل ، مرجع سابق ، ص335.

[261] هلالي عبداللاه أحمد ، التزام الشاهد بالإعلام في الجرائم المعلوماتية ، مرجع سابق ، ص53 – 54.

[262] حسين بن سعيد الغافري ، السياسة الجنائية في مواجهة جرائم الانترنت ، مرجع سابق ، ص469 .

المطلب الخامس

الخبرة في الجرائم الإلكترونية

قد يستعصى على سلطة التحقيق أو القضاء أو مأمور الضبط القضائي إظهار الحقيقة في الجريمة الإلكترونية ، مما يتطلب الأمر الاستعانة بخبراء فنيين في مجال الحاسب الآلي وغير ذلك من وسائل التقنية الحديثة ، وذلك من أجل كشف غموض الجريمة أو تجميع أدلتها والتحفظ عليها ، غير أن ذلك مشروط بمراعاة القواعد القانونية والفنية التي تحكم عمل الخبير في الجرائم الإلكترونية .

وبناءً على ما تقدم سنقسم هذا المطلب إلى فرعين : نخصص الفرع الأول لدراسة القواعد القانونية التي تحكم الخبرة في الجرائم الإلكترونية ، ونكرس الفرع الثاني لبيان القواعد الفنية التي تحكم عمل الخبير في الجرائم الإلكترونية .

الفرع الأول

القواعد القانونية التي تحكم الخبرة في الجرائم الإلكترونية

سنتناول في هذا الفرع تعريف الخبرة وأهميتها ، وشروط صحة عمل الخبير ، وذلك على النحو التالي :

أولاً . تعريف الخبرة وبيان أهميتها :

أ) تعريف الخبرة :

يعرفها البعض بأنها " وسيلة إثبات يلجأ إليها المحقق أو القاضي ، بتكليف أحد المختصين فيها لإبداء الرأي في وقائع ذات طبيعة فنية أو علمية لا تتوافر المعلومات اللازمة عنها لديه ، بهدف مساعدته في تكوين عقيدته بشأن تلك المسألة "[263]

كما تعرف أيضاً بأنها " تلك المعرفة المتخصصة في أي من مجالات العلم والعمل".[264] أما الخبير الإلكتروني فيعرفه البعض بأنه " الشخص الذي تعمق في دراسة عمل من الأعمال الإلكترونية ، وتخصص في أدائه فترة زمنية طويلة مما أكسبه خبرة عملية ، بحيث أصبح ملماً بتفصيلاته ، مما جعله متفوقاً على الشخص العادي ، وجعله قادراً على إبداء الرأي

---

[263] عبدالخالق محمد أحمد الصلوي ، حجية الخبرة في الإثبات الجنائي (دراسة مقارنة)، دار النهضة العربية ، القاهرة ، 2009 ، ص24 .

[264] حسين المحمدي بوادي ، الوسائل العلمية الحديثة في الإثبات الجنائي ، منشأة المعارف ، الإسكندرية ، 2008 ، ص6 .

الإلكتروني في الأمور المتصلة بهذا العمل ، ويشترط فيه أن يجمع بين المؤهل العلمي والخبرة العملية "[265]

ب) أهمية الاستعانة بالخبراء :

ازدادت أهمية الخبرة في الوقت الحاضر نظراً لتقدم العلوم والفنون التي تشمل دراستها الوقائع التي تتصل بوقوع الجريمة ، ونسبتها إلى فاعلها ، ودقة النتائج التي يمكن الوصول إليها عند الاستعانة بالمتخصصين في هذه العلوم والفنون ، مما يمثل عوناً للقضاء وسائر السلطات المختصة بالدعوى الجنائية في أداء رسالتها ، لذا فقد اهتم المشرّع الليبي بتنظيم أعمال الخبرة[266]. وأجاز لكل من مأموري الضبط القضائي والنيابة العامة وقاضي التحقيق الاستعانة بالخبراء كما يجوز للمحكمة أيضاً تعيين الخبراء سواءً من تلقاء نفسها أو بناءً على طلب الخصوم .

ومن ثم فإن مهمة الخبير هي المساهمة في كشف الحقيقة عن طريق الإثبات العلمي وتقديم الدليل العلمي ، وهي مهمة مكملة للتحقيق الجنائي[267] ، وإذا كان للخبرة تلك الأهمية في الجرائم التقليدية ، فإن أهميتها تزداد وتكون ضرورية في إثبات الجرائم الإلكترونية ، فالخبرة وسيلة من وسائل الإثبات التي تهدف إلى إظهار بعض الأدلة أو تحديد مدلولها بالاستعانة بالمعلومات العلمية[268]. غير أن الخبير لا يشترط فيه فقط توافر الكفاءة العلمية ، بل لابد من توافر الخبرة العملية في تحقيق الجرائم الإلكترونية ، كجرائم التلاعب في البيانات وتزوير المستندات ، أو كجرائم عرض صور أو أفلام مخلة بالآداب العامة.[269] .

ومن التشريعات التي نظمت أعمال الخبرة في مجال الجرائم الإلكترونية ، قانون نظام مكافحة الجرائم المعلوماتية السعودي ، الذي نص في المادة (14) على أنه " تتولى هيئة الاتصالات وتقنية المعلومات وفقاً لاختصاصها تقديم الدعم والمساندة الفنية للجهات الأمنية المختصة خلال مراحل ضبط هذه الجرائم والتحقيق فيها وأثناء المحاكمة " .

---

[265] مصطفى محمد موسى ، مرجع سابق ، ص221 .

[266] انظر المواد (19،69،70،71،72،73،265) من قانون الإجراءات الجنائية الليبي ، ويقابل ذلك المواد (29،85،86،87،88،89،292) من قانون الإجراءات الجنائية المصري.

[267] أبو العلا علي أبو العلا نمر ، مرجع سابق ، ص153.

[268] صغير يوسف ، مرجع سابق ، ص89 .

[269] محمد أبو العلا عقيدة ، مرجع سابق ، ص6 .

ثانياً . شروط صحة عمل الخبير :

يمكن إجمال هذه الشروط فيما يلي :

أ) يجب أن تتوافر شروط التعيين في وظيفة الخبرة ، حيث نص قانون رقم (1) لسنة 1371و.ر الخاص بتنظيم الخبرة القضائية في مادته رقم (5) التي تشترط في من يقيد أسمه في جدول الخبراء ما يلي :

1- أن يكون متمتعاً بالجنسية الليبية.

2- ألا يكون محكوم عليه في جناية أو جنحة مخلة بالشرف أو بعقوبة تأديبية .

3- أن يكون حاصلاً على المؤهلات الدراسية التخصصية مع خبرة عملية تحددها لجنة الخبراء

وتقدير ما إن كانت الدعوى تستلزم ندب خبير من عدمه ، هو أمر من شأن المحقق لذلك فهو ليس ملزماً بإجابة الخصوم لهذا الندب[270] .

والخبير قد يكون شخصاً طبيعياً أو معنوياً[271]، والشخص المعنوي يتجسد في المكاتب أو الشركات ، ونلاحظ أنه في مجال الجرائم الإلكترونية يتعين الاستعانة بالشركات أو المكاتب حيث تمتلك إمكانيات من أجهزة ومعدات فضلاً عن توافر الكفاءات البشرية المتخصصة من حيث الشهادة العلمية والخبرة العملية في مجال الحاسب الآلي وغير ذلك من وسائل تقنية المعلومات .

ب) حلف اليمين القانونية للخبير :

تنص المادة (70) إج ليبي على أنه " يجب على الخبراء أن يحلفوا أمام المحقق يميناً على أن يبدوا رأيهم بالأمانة والصدق ، وعليهم أن يقدموا تقريرهم كتابة "[272] ، هذا فيما يتعلق بمرحلة التحقيق الابتدائي ، أما عن مرحلة جمع الاستدلالات فالأصل أن الخبير لا يحلف اليمين[273] ، ومع ذلك يجوز لمأمور الضبط القضائي تحليف الخبير اليمين قياساً ، على جواز تحليف الشاهد إذا خيف ألا يستطاع فيما بعد تقديم خبرته[274]، ويتعين أن يكون حلف اليمين قبل أدائه مهمته ، وإذا أدى الخبير مهمته دون حلف يمين ، يبطل عمله ، ولكن يبقى صحيحاً

---

(270) www.aladel.gov.ly/main/madules/sections/item.php?itemid=13

(271) المادة الثانية من قانون تنظيم الخبرة القضائية رقم (1) لسنة 1371 ، التي تنص على أنه " يجوز أن تمارس أعمال الخبرة عن طريق المكاتب أو تشاركيات تؤسس لهذا الغرض ..... " (aladel.gov.ly/home/?P=1297)

(272) المادة (86) من قانون الاجراءات الجنائية المصري.

(273) المادة (19) من قانون الاجراءات الجنائية الليبي .

(274) شعبان محمود محمد الهواري ، مرجع سابق ، ص123 .

باعتباره عمل استدلال[275] ، وقد استقر الفقه على أن أداء الخبير اليمين يوم تسليمه للعمل يغني عن أداء اليمين عند مباشرة كل مأمورية[276] ، أما إذا كان الخبير من غير الخبراء المقيدين في الجدول ، يجب في هذه الحالة استحلافه اليمين بأن يؤدي عمله بالصدق والأمانة.[277]

ج) تقرير الخبرة :

عندما ينتهي الخبير من عمله ، فإن عليه أن يقدم تقريراً يشتمل على وصف ما قام به من أعمال ونتائجها ، لذلك أوجبت المادة (71) إج ليبي على أنه " يحدد المحقق ميعاداً للخبير ليقدم تقريره فيه ، وله أن يستبدل به خبيراً آخر ، إذا لم يقدم التقرير في الميعاد المحدد "[278] ، غير أن الفقه لم يوجب شكلاً معيناً في تقرير الخبير ، فقد يكون شفوياً أو مكتوباً وفقاً لما تحدده طبيعة المأمورية[279] ، إلا أن المشرّع أوجب إتباع شكل معين في تقرير الخبير بأن يكون مكتوباً وهو ما نصت عليه المادة (70) من قانون الاجراءات الجنائية الليبي " يجب على الخبراء أن يحلفوا أمام المحقق يميناً على أن يبدوا رأيهم بالأمانة والصدق ، وعليهم أن يقدموا تقريرهم كتابة "[280] .

وسلطة المحكمة في تقدير القوة التدليلية لعناصر الدعوى كاملة باعتبارها الخبير الأعلى في كل ما تستطيع الفصل فيه بنفسها ، كما هي غير ملزمة بندب خبير ولا بإعادة المهمة إلى ذات الخبير ، أو بإعادة مناقشته ما دام استنادها إلى الرأي لا يجافي العقل والقانون والمنطق.[281]

كما لها أن تأخذ برأي خبير دون آخر، وللمحكمة أن تفاضل بين تقارير الخبراء.[282] غير أنه إذا تعرضت لرأي الخبير الفني في مسألة فنية بحتة يتعين عليها أن تستند إلى تفنيده إلى أسباب فنية.[283] .

---

[275] محمود نجيب حسني ، مرجع سابق ، ص658 .

[276] محمد زكي أبو عامر ، الإجراءات الجنائية ، مرجع سابق ، ص681 .

- برهامي أبوبكر عزمي ، مرجع سابق ، ص382-383.

- مأمون محمد سلامة ، الإجراءات الجنائية في التشريع المصري ، ج1 ، مرجع سابق ، ص526 .

[277] محمد حسين منصور ، قانون الاثبات مبادئ الاثبات وطرقه ، منشأة المعارف ، الاسكندرية ، 1998 ، ص253.

[278] ويقابل ذلك المادة (87) من قانون الاجراءات الجنائية المصري .

[279] أبو العلا علي أبو العلا النمر ، مرجع سابق ، ص181 .

[280] ويقابل ذلك المادة (86) من قانون الاجراءات الجنائية المصري .

[281] المحكمة العليا نقض جنائي 1982/2/14 ، مجلة المحكمة العليا ، س1 ، عدد 19 ، ص218 .

- المحكمة العليا نقض جنائي 1994/2/6 ، مجلة المحكمة العليا ، س23 ، العدد 30 ، ص295.

[282] المحكمة العليا ، نقض جنائي 1981/12/22 ، مجلة المحكمة العليا ، س4 ، العدد 18 ، ص224.

- المحكمة العليا ، نقض جنائي 1984/6/12 ، مجلة المحكمة العليا ، س1 ، عدد 22 ، ص167.

[283] إيهاب عبدالمطلب ، الموسوعة الجنائية الحديثة في شرح قانون الإجراءات الجنائية ، الطبعة الاولى ، المجلد الثالث ، المركز القومي للإصدارات القانونية ، 2004 ، ص258.

- المحكمة العليا ، نقض جنائي 1985/9/24 ، مجلة المحكمة العليا ، س4 ، عدد 23 ، ص165.

الفرع الثاني
القواعد الفنية التي تحكم الخبرة في الجرائم الإلكترونية

نظراً للطبيعة الخاصة في الجرائم الإلكترونية ، فإنها تنفرد الخبرة الفنية فيها إلى قواعد فنية يستعين فيها بالخبير الإلكتروني .

وبناءً على ما تقدم سنتناول في هذا الفرع المسائل التي يستعين فيها بالخبير الإلكتروني ، وتحديد الإمكانيات الإلكترونية لمختبر الجرائم الإلكترونية وبيان خطوات استخلاص الدليل الرقمي بواسطة الخبير الفني وذلك على النحو التالي:

أولاً . المسائل التي يستعان فيها بالخبير الإلكتروني :

بالنظر إلى الطبيعة الفنية والعلمية للخبرة في مجال الجرائم الإلكترونية فإنه يمكن تحديد هذه الخبرة في الموضوعات الآتية :[284]

أ) وصف تركيب جهاز الحاسب الآلي وصناعته ونوعه ونوع نظام التشغيل ، بالإضافة إلى الأجهزة الملحقة به وكلمات المرور ونظام التشفير .

ب) وصف طبيعة بيئة جهاز الحاسب الآلي وبيئة شبكات التقنية الرقمية من حيث التنظيم ومن توزيع عمل المعالجة الآلية ونمط وسائط الاتصالات وتردد موجات البث وأمكنة اختزانها

ج) وصف الموضع المحتمل للأدلة والشكل أو الهيئة التي تكون عليها .

د) وصف أثر التحقيق من الوجهة المالية على المشاركين في استخدام النظام .

هـ) بيان كيفية عزل النظام المعلوماتي دون إتلاف الأدلة أو تدميرها أو إلحاق ضرر بالأجهزة .

و) بيان كيفية نقل أدلة الإثبات الإلكترونية في صورة مادية بنقلها إذا أمكن إلى أوعية ورقية يتاح للقاضي مطالعتها وفهمها مع إثبات أن المسطور على الورق مطابق للمسجل على جهاز الحاسب الآلي .

ثانياً . الإمكانيات الإلكترونية لمختبر الجرائم الإلكترونية :

يحتاج مختبر الجرائم الإلكترونية إلى الإمكانيات الإلكترونية التالية: [285]

---

[284] عبدالله حسين علي محمود ، جمع الأدلة في مجال جريمة سرقة المعلومات ، مرجع سابق ، بدون ترقيم صفحات.

[285] كمال أحمد الكركي ، التحقيق في جرائم الحاسوب ، بدون ترقيم صفحات ، بحث منشور على الإنترنت .
Http//www.f.law.Net/Law/threads/11337

أ) الأجهزة :

وتشتمل هذه الأجهزة على ما يلي :

1- أجهزة الحاسوب .

2- طابعات ملونة وأبيض وأسود .

3- ماسح ضوئي (سكنر) .

4- أجهزة حاسوب (لاب توب) مجهزة بالإضافات الحديثة ، وبطاقة شبكة الإنترنت ، ووصلات خارجية للربط مع أي شبكة ، ومزودة بعدة نظم تشغيل .

5- مجموعة فارغة من أقراص ذات سعة عالية .

6- تشكيلة للربط من أدوات التفكيك والمفكات .

ب) الأنظمة والبرامج :

1- أنظمة التشغيل ومنها على سبيل المثال (Dos mac.winme.winxp.Linux)

2- البرامج .

وتتمثل هذه البرامج فيما يلي :

- برامج معالجة الصور وعرضها وتحويلها وتصميمها مثل :

Acdsee.compupic.XNview.photoshop

- برامج نسخ الأقراص المدمجة مثل Ashampo Nero
- برامج نسخ الأقراص الصلبة Back Office
- برامج الاتصال بين أي من حواسيب المعمل الجنائي والكمبيوترات المضبوطة عبر الـports
- برامج التشفير وفك التشفير مثل pgp
- برامج التنصت على شبكة الإنترنت والوسائل الإلكترونية واختراق المواقع Simantic Forest
- برامج مكافحة البرامج الإلكترونية المتطفلة الضارة " الفيروسات " .
- برامج حماية الشبكات والأنظمة من الاختراق Fire walls
- برامج البحث الدقيق واستعادة الملفات المحذوفة مثل Disk.Searth . Nortonutl Lites
-

ثالثاً . خطوات استخلاص الدليل الرقمي بواسطة الخبير الالكتروني :

توجد هناك عدة خطوات من أجل استخلاص الدليل الرقمي وتتمثل هذه الخطوات في المراحل التالية[286] :

أ) خطوات ما قبل التشغيل والفحص :

1- التأكد من مطابقة محتويات أحراز المضبوطات لما هو مدون عليها .

2- التأكد من صلاحية وحدات النظام للتشغيل .

3- تسجيل بيانات الوحدات والمكونات المضبوطة كالنوع والصناعة والرقم المسلسل .

ب) خطوات التشغيل والفحص :

1- استكمال تسجيل باقي بيانات الوحدات من خلال قراءة الجهاز .

2- عمل نسخة من كل وسائط التخزين المضبوطة وعلى رأسها القرص الصلب .

3- تحديد أنواع وأسماء المجموعات البرامجية ذات دلالة بموضوع الجريمة كبرامج إنشاء ومعالجة الصور في جرائم دعارة الأطفال .

4- استرجاع الملفات التي تم محوها من الأصل .

5- إعداد قائمة يجرد فيها الخبير كل الأدلة الرقمية التي تم الحصول عليها في الديسك الخاص مع إجراء مراجعة لكل صورة محتفظ بها في الديسك في جهاز حاسب آلي آخر للتأكد من سلامة القائمة .

---

[286] عبدالناصر محمد فرغلي ، و عبيد سيف سعيد المسماري ، مرجع سابق ، ص35.

المبحث الثاني

الإجراءات الحديثة لجمع الدليل الرقمي

لقد تناولنا فيما سبق من خلال المبحث الأول ، الإجراءات التقليدية لجمع الدليل الرقمي ، وتبين لنا من خلال ذلك المبحث المعوقات التي تحيط بتلك الإجراءات ، وهذا ما يؤدي في الغالب إلى عرقلة سير العدالة الجنائية من خلال إفلات المجرمين من العقاب .

لذا من الضروري إنشاء قواعد قانونية إجرائية غير تقليدية تعاصر هذا التطور من الإجرام الحديث ، عن طريق الاعتماد على تقنية تكنولوجية المعلومات في جمع الدليل الرقمي . وقد بينت اتفاقية بودابست المتعلقة بالإجرام المعلوماتي الصادرة في 2001 هذه الإجراءات الحديثة من خلال التحفظ السريع على البيانات المخزنة وتجميعها ، والأمر بتقديم بيانات معلوماتية تتعلق بالمشترك ، وبيان اعتراض الاتصالات الإلكترونية .

وبناءً على ما تقدم سنقسم هذا المبحث إلى ثلاثة مطالب : نخصص المطلب الأول لدراسة التحفظ السريع على البيانات المخزنة وتجميعها . ونكرس المطلب الثاني لدراسة الأمر بتقديم بيانات معلوماتية متعلقة بالمشترك . ونفرد المطلب الثالث لبيان اعتراض الاتصالات الإلكترونية .

المطلب الأول

التحفظ السريع على البيانات المخزنة وتجميعها

يعتبر التحفظ السريع على البيانات المخزنة وتجميعها ، من الإجراءات الحديثة لجمع الأدلة الرقمية ، والتي تسهل مهمة سلطة التحقيق في كشف الجرائم الإلكترونية والبحث عن أدلتها وضبطها .

وبناء على ما تقدم سنقسم هذا المطلب إلى فرعين : نخصص الفرع الاول لدراسة التحفظ السريع على البيانات المعلوماتية المخزنة ، ونكرس الفرع الثاني لدراسة التجميع في الوقت الفعلي للبيانات المتعلقة بخط سير البيانات .

الفرع الأول

التحفظ السريع على البيانات المعلوماتية المخزنة

سنتناول في هذا الفرع تعريف التحفظ السريع على البيانات المعلوماتية المخزنة ، وتحديد إجراءات التحفظ السريع على مضمون البيانات المخزنة ، وذلك على النحو التالي:

أولاً . تعريف التحفظ السريع على البيانات المعلوماتية المخزنة :

ويُقصد به " توجيه السلطة المختصة لمزودي الخدمات[287]، الأمر بالتحفظ على بيانات معلوماتية مخزنة في حوزته ، أو تحت سيطرته في انتظار اتخاذ إجراءات قانونية أخرى كالتفتيش أو الأمر بتقديم بيانات معلوماتية "[288]

وكما هو ملاحظ من هذا التعريف أن التحفظ السريع على البيانات هو إجراء أولي تمهيدي ، الهدف منه هو محاولة الاحتفاظ بالبيانات قبل فقدانها .

غير أنه يوجد هناك فرق بين التحفظ على البيانات والاحتفاظ أو أرشفة البيانات ، حيث يقصد بالأول حفظ بيانات سبق وجودها في شكل مخزن ، وحمايتها من الإتلاف أو العبث ، أما الثاني فيقصد به تجميع البيانات والاحتفاظ بها في المستقبل بدون ضمان سلامتها وسريتها ، فهو عملية تخزين لا غير.[289]

ثانياً . إجراءات التحفظ السريع على مضمون البيانات المخزنة :

تتمثل إجراءات التحفظ السريع على مضمون البيانات المخزنة ، في إصدار أوامر إلى مزودي الخدمات في مجال الاتصالات الإلكترونية من أفراد أو شركات بالحفاظ على البيانات المخزنة بمنظومة الكمبيوتر والإنترنت لفترة زمنية معينة .

ويعتبر التحفظ على البيانات من إجراءات التحقيق ، التي يقوم بها مأمور الضبط القضائي تمهيداً لعرضها على النيابة العامة للتحقيق في الدعوى ، ولعضو النيابة أن يقوم بالإطلاع على المضبوطات والتحفظ عليها ، إذا كان يتصل بالجريمة التي يباشر التحقيق فيها[290].

---

[287] يقصد بمزود الخدمات هو " من يقدم خدمته إلى الجمهور بوجه عام في مجال الاتصالات الإلكترونية التي لا تقتصر في أدائها على طائفة معينة من المتعاملين معه بمقتضى عقد من العقود " ، (شيماء عبدالغني محمد عطا الله ، مرجع سابق ، ص209). كما أشار قانون حماية الحياة الخاصة في مجال الاتصالات الإلكترونية بالولايات المتحدة الأمريكية نوعين من مزودي الخدمات : النوع الأول : مزود خدمات الاتصالات الإلكترونية ويقصد به كل من يقدم خدمة إلى مستخدمي الشبكة والتي تتمثل في تسهيل إرسال واستقبال الاتصالات السلكية والإلكترونية ، (عمر محمد بن يونس ، الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي ، مرجع سابق ، ص281). أما النوع الثاني هو مزود الخدمات ومعالجة المعلومات عن بعد ، فيعرف حسب ما جاء في قانون خصوصية الاتصالات الإلكترونية الأمريكي بأنه " كل من يقدم للجمهور خدمة معالجة البيانات عن بعد بوسيلة من وسائل الاتصالات الإلكترونية " . (شيماء عبدالغني محمد عطا الله ، المرجع السابق ، ص210) .

[288] بوعناد قاطمة زهرة " مكافحة الجريمة الإلكترونية في التشريع الجزائري " ، مجلة الندوة للدراسات القانونية ، العدد الأول ، سنة 2013 ، ص72.

[289] هلالي عبداللاه أحمد ، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست الموقعة في 23 نوفمبر 2001 ، دار النهضة العربية ، القاهرة ، 2006 ، ص187 .

[290] ناير نبيل عمر ، الحماية الجنائية للمحل الإلكتروني في جرائم المعلوماتية ، دار الجامعة الجديدة ، الإسكندرية 2012 ، ص160 .

ومما تجدر الإشارة إليه أن التصرف في المضبوطات يشترط ألا تكون لازمة للسير في الدعوى ، وألا تكون محلاً للمصادرة[291]، أي أنه بمفهوم المخالفة ، فالتحفظ على البيانات أو المعلومات الإلكترونية لابد أن يكون ضرورياً للسير في الدعوى ، أو أن تكون تلك البيانات تحوي ما هو محل للمصادرة[292] .

وقد نصت اتفاقية بودابست على هذا الإجراء في المادة (16) حيث نصت على :

أ) يجب على كل طرف أن يتخذ الإجراءات التشريعية ، وأية إجراءات أخرى يرى أنها ضرورية من أجل السماح لسلطاته المختصة أن تأمر أو أن تفرض بطريقة أخرى التحفظ العاجل على البيانات المعلوماتية المخزنة ، وبما في ذلك البيانات المتعلقة بالمرور المخزنة بواسطة نظام معلوماتي ، وبالأخص عندما تكون هناك أسباب تدعو للاعتقاد بأن هذه البيانات على وجه الخصوص معرضة للفقد أو التغيير .

ب) عندما يقوم طرف بتطبيق الفقرة (1) أعلاه عن طريق أمر يصدر لشخص للتحفظ على البيانات المخزنة الموجود في حوزته أو تحت إشرافه ، فإن هذا الطرف يجب عليه اتخاذ الإجراءات التشريعية والإجراءات الأخرى التي يراها ضرورية من أجل إجبار هذا الشخص على التحفظ وحماية سلامة البيانات المذكورة لمدة طويلة من الزمن على قدر الضرورة بحد أقصى 90 يوماً بغرض السماح للسلطات المختصة بالكشف عنها ، كما يمكن لكل طرف أن يقرر تجديد هذا الأمر .

ويختلف إجراء التحفظ على البيانات المتعلقة بالمرور عن التحفظ على مضمون البيانات ، الذي نصت عليه المادة (16 الفقرة 1) من الاتفاقية ، في أن التحفظ على البيانات المتعلقة بالمرور ، يقتصر على البيانات المتعلقة بالاتصال من حيث مصدرها ووقتها ومرسلها ومن ساهم في نقلها ، ولا يشمل محتوى ما تتضمنه من معلومات[293] .

غير أننا نلاحظ أن هذا الإجراء يحتاج إلى تكنولوجيا عالية ، تمكن مزود الخدمة القيام به في وقت سريع ، بهدف إعطاء السلطة المختصة فرصة اتخاذ الإجراء اللازم .

وهذا ما أكدت عليه المادة (17 فقرة 1 ، 2) من اتفاقية بودابست حيث نصت على أنه " يجب على كل دولة طرف اتخاذ الإجراءات التشريعية وأية إجراءات أخرى يرى أنها ضرورية من أجل :

---

[291] عبدالفتاح بيومي حجازي ، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية ، الطبعة الأولى ، 2009 ، ص645 .

[292] ناير نبيل عمر ، مرجع سابق ، ص160 .

[293] هلالي عبداللاه أحمد ، الجرائم الموضوعية والإجرائية لجرائم المعلوماتية ، مرجع سابق ، ص205.

1- التأكد من أن التحفظ المعجل لهذه البيانات المتعلقة بالمرور متوافرة بغض النظر عما إذا كان هناك مقدم خدمة واحد أو عدة مقدمين للخدمة قد ساهموا في نقل الاتصال .

2- ضمان الإفشاء السريع للسلطة المختصة للطرف ، أو للشخص المعين من قبل هذه السلطة عن كمية بيانات مرور كافية تسمح بتحديد مزودي الخدمات والطريق الذي تم الاتصال من خلاله.

وكما هو ملاحظ من النص السابق ، أنه يحث على ضرورة تبني الدول تشريعات تكفل قيام مزودي الخدمات بالتحفظ السريع على البيانات المتعلقة بالمرور .

وتجدر الإشارة هنا إلى أن إجراء التحفظ على البيانات سواءً تلك المتعلقة بمضمون البيانات أو البيانات المتعلقة بالمرور ، يعد بالنسبة للمشرع الليبي سلطة قانونية جديدة ، فهو أداة تحقيق مستحدثة في إطار مكافحة الجرائم الإلكترونية ، فهو يتلاءم وطبيعة هذه البيئة الرقمية من حيث قابلية البيانات للإتلاف والضياع بسرعة .

الفرع الثاني

التجميع في الوقت الفعلي للبيانات المتعلقة بخط سير البيانات

ويقصد به تجميع أو التسجيل عن طريق وسائل معينة موجودة على أرض الدولة للبيانات المتعلقة بخط سير البيانات ، وذلك بإلزام مزود الخدمة في نطاق قدراته الفنية بجمع وتسجيل تلك البيانات في الوقت الصحيح .

ويهدف هذا الإجراء الخاص بالتجميع في الوقت الفعلي للبيانات المتعلقة بخط سير البيانات الذي تقوم به السلطة المختصة في الدولة ، أو ينفذه مزودو الخدمات بناءً على أوامر صادرة من السلطة المختصة بهذا الإجراء إلى تسهيل مهام الجهات القائمة بجمع الأدلة .

ويختلف إجراء التجميع في الوقت الفعلي للبيانات المتعلقة بخط سير البيانات ، عن إجراء التحفظ السريع على البيانات المعلوماتية الذي نصت عليه المادة (16) من اتفاقية بودابست في أن البيانات في حالة التحفظ موجوده لدى مزود الخدمات ، أي مخزنة بالنظام المعلوماتي للحاسب الآلي أو في دعامة تخزين ، بينما في حالة التجميع فالبيانات غير مخزنة.[294]

وتجدر الإشارة إلى أن هذه الإجراءات تهدف إلى تجميعها وقت مباشرة الاتصال ، فالبيانات المتعلقة بالاتصال التي يقوم مزود الخدمة بحفظها وتجميعها ، تعد ذات قيمة معلوماتية

---

[294] هلالي عبداللاه أحمد ، الجوانب الموضوعية والاجرائية لجرائم المعلوماتية ، مرجع سابق ، ص205 - 256 ومابعدها .

لرجال الضبط القضائي والتحقيق ، ويظهر فيها المستخدم ووقت بداية ونهاية الاتصال والرقم الكودي للمتصل والمواقع التي زارها ، والمعلومات التي طلبها والبيانات التي حصل عليها .

هذه المعلومات وغيرها تعد كلها بمثابة الآثار التي يرتكبها المستخدم ، وتعتبر بمثابة دليل عند ارتكاب الجرائم الإلكترونية [295] .

[295] وليد الكشباطي ، جرائم اختراق الأنظمة المعلوماتية ، بدون ترقيم صفحات ، بحث منشور على الإنترنت
Http//www.chawkitabib.info/spip.php? artict Leu 77

المطلب الثاني

الأمر بتقديم بيانات معلوماتية متعلقة بالمشترك

يقصد بالأمر تقديم بيانات متعلقة بالمشترك ، هي أن تصدر السلطة المختصة أمر إلى مزودي الخدمات أو أي شخص في حيازته أو تحت سيطرته بيانات معينة أن يقوم بتقديمها[296] وإذا كان الأصل يقول أن البيانات الشخصية المتعلقة بالمشترك ، تدخل في إطار الحق في الخصوصية ، وهذا ما نادت به العديد من الاتفاقيات الدولية ، كالإعلان العالمي لحقوق الإنسان الصادر عن الجمعية العامة للأمم المتحدة الصادر في 10 ديسمبر 1948 ، والمواثيق الدولية والإقليمية ، كالاتفاقية الأوربية لحقوق الإنسان والحريات الأساسية الصادرة عن المجلس الأوربي عام 1950م.[297]

أما موقف التشريعات العربية والأجنبية فهو مختلف بشأن الإفشاء بالبيانات المعلوماتية المتعلقة بالمشترك ، لذا سنقسم هذا المطلب إلى ثلاثة فروع : نخصص الفرع الأول لدراسة موقف التشريع الفرنسي . ونخصص الفرع الثاني لدراسة موقف التشريع الأمريكي . ونفرد الفرع الثالث لبيان موقف التشريع الليبي .

الفرع الأول

موقف التشريع الفرنسي

يسمح المشرع الفرنسي لرجال الضبط القضائي أن يأمروا الأشخاص تسليم ما تحت أيديهم من موضوعات ، والتي يطلب تقديمها كدليل ، ومن بينها البيانات المتعلقة بالمشترك التي يحوزها مزودو الخدمات .

وهو ما نصت عليه المادة (60–2) أج فرنسي المعدل بالقانون رقم (239 لسنة 2003) المعدلة بالقانون رقم (204 لسنة 2004) على أن العاملين بالجهات العامة والخاصة التي تعمل من خلال أنظمة الحاسب الآلي ، وبناءً على طلب من مأموري الضبط القضائي عليهم أن يقدموا ما لديهم من معلومات ، مع استثناء من منهم يكون ملتزماً بالمحافظة على سر المهنة ، ما دامت تلك المعلومات ضرورية لإظهار الحقيقة عن الجريمة.[298] .

---

[296] بوعناد فاطمة زهرة ، مرجع سابق ، ص71.

[297] محمد رشاد إبراهيم ، الحماية الجنائية للحق في حرمة الاتصالات الشخصية ، رسالة دكتوراه ، كلية الحقوق ، جامعة الاسكندرية ، 2009 ، ص 38 ومابعدها.

[298] علي حسن محمد الطوالبة ، مرجع سابق ، ص239 .

الفرع الثاني

موقف التشريع الأمريكي

يجيز المشرع الأمريكي من خلال قانون خصوصية الاتصالات الإلكترونية المعروف بـ (ECPA) ، لرجال الضبط القضائي الإطلاع في نطاق ما يقومون به من جمع الاستدلالات على البيانات الموجودة في حوزة مزودي الخدمات والتي تخص مستخدمي شبكة الإنترنت ، وهذه المعلومات تتمثل في ثلاث فئات :

أ) المعلومات الشخصية الخاصة بالمشترك مثل اسمه ورقم هاتفه وعنوانه .

ب) المعلومات الشخصية الخاصة بالتعامل مع المشترك (أي كل ما يتصل به أو يدخل معه في صفقة) .

ج) المعلومات المتعلقة بمحتوى الملفات (مضمون المحادثات – مضمون الملفات)[299]

([299]) شيماء عبدالغني محمد عطا الله ، مرجع سابق ، ص216 .

الفرع الثالث

موقف التشريع الليبي

لا يجيز المشرع الليبي أن يصدر رجال الضبط القضائي مثل هذا الأمر ، وإنما يُجيزه لسلطة التحقيق ، حيث تنص المادة (83) إج ليبي على أنه " لقاضي التحقيق أن يأمر الحائز لشيء يرى ضبطه أو الإطلاع عليه بتقديمه..... " ، ولا تختلف سلطة النيابة العامة في ذلك عن سلطة قاضي التحقيق ، كما أن للمحكمة أن تصدر مثل هذا الأمر وفقاً لنص المادة (264) إج ليبي التي تنص على أنه " للمحكمة أن تأمر ولو من تلقاء نفسها أثناء نظر الدعوى بتقديم أي دليل تراه لازماً لظهور الحقيقة " .

وكما هو ملاحظ من التشريعات السابقة ، أن المشرع الأمريكي والفرنسي قد أجاز لرجال الضبط القضائي إصدار أوامر إلى مزودي الخدمات لتقديم ما لديهم من معلومات ، غير أن المشرع الليبي لم يسمح لرجال الضبط القضائي إصدار مثل هذه الأوامر ، وبناء على ماتقدم نؤيد موقف المشرع الليبي ، لأن إصدار مثل هذا الأمر فيه اعتداء على حرمة الحياة الخاصة ، وهو إجراء خطير يجب أن تقوم به سلطة التحقيق أو المحكمة .

المطلب الثالث

اعتراض الاتصالات الإلكترونية المتعلقة بالمشترك

سنتناول في هذا المطلب تعريف اعتراض الاتصالات الإلكترونية وبيان اهميتها وذلك من خلال فرع أول . أما الفرع الثاني سنخصصه لدراسة الضمانات القانونية لمشروعية اعتراض الاتصالات الإلكترونية .

الفرع الأول

تعريف اعتراض الاتصالات الإلكترونية وأهميتها

سنتناول في هذا الفرع تعريف اعتراض الاتصالات الإلكترونية ، وبيان أهمية اعتراض الاتصالات الإلكترونية ، وذلك على النحو التالي :

أولاً . تعريف اعتراض الاتصالات الإلكترونية :

أغفل المشرع الليبي في قانون الإجراءات الجنائية تعريف الاعتراض التي نص عليها في المادتين (79 ، 180) ، أو كما يسميه البعض بـ"المراقبة" .

في حين عرف بعض الفقه المراقبة الإلكترونية بأنها " العمل الذي يقوم به المراقب باستخدام التقنية الإلكترونية ، لجمع بيانات ومعلومات عن المشتبه فيه سواءً كان شخصاً أو مكاناً ، أم شيئاً حسب طبيعته مرتبط بالزمن التاريخ والوقت ، لتحقيق غرض أمني أو لأي غرض آخر "[300] .

وقد عرف المشرع الكندي المراقبة من خلال قانون حماية الخصوصية الكندي الصادر سنة 1973 بأنها " الاستماع أو تسجيل أو اكتساب اتصالات أو اكتساب المادة التي تعنى أو يفهم منها ذلك ، ويجب أن تتم المراقبة عن طريق أجهزة إلكترونية أو سمعية أو ميكانيكية أو أي أجهزة أخرى " .

أما المشرع الأمريكي فقد عرف الاعتراض في المادة (4) من القانون الفيدرالي الأمريكي الصادر سنة 1968 بأنه " اكتساب سماعي عن طريق السمع لمحتويات أية أسلاك أو أية

---

[300] مصطفى محمد موسى ، المراقبة الإلكترونية عبر شبكة الإنترنت بين المراقبة الأمنية التقليدية والالكترونية ، الطبعة الأولى ،دار الكتب والوثائق المصرية ، 2003 ، ص192 .

اتصالات شفهية عن طريق استخدام جهاز إلكتروني أو ميكانيكي أو أي جهاز آخر"[301] . وقد قضى بأن المقصود بكلمة اكتساب أن يتم الالتقاط أو الاعتراض أثناء الاتصال نفسه.[302]

وتجدر الإشارة هنا إلى أن الاتصالات السلكية تختلف عن الاتصالات الإلكترونية ، حيث تعرف الاتصالات السلكية من قِبل قانون خصوصية الاتصالات الالكترونية الأمريكي بموجب القسم (1) (2510) بأنها "تعني أي تحويل سمعي أو شفهي يتم القيام به كلياً أو جزئياً باستخدام تسهيلات لبث اتصالات بمساعدة الأسلاك أو الكابل أو أي رابط آخر بين نقطة المصدر ونقطة الاستقبال ، وتشمل استخدام هذا الرابط في محطة التحويل يتم تزويدها أو عملها بواسطة أي شخص يقدم أو يشغل هذه التسهيلات "[303] .

ومن خلال هذا التعريف ، فإن الاتصالات السلكية تتطلب وجود صوت إنسان ، باعتباره عنصر أساسي يميز الاتصالات السلكية عن غيرها من الاتصالات الأخرى[304] .

أما الاتصالات الإلكترونية فيعرفها القسم (12– 2510) من القانون الأمريكي بأنها " أي تحويل لمؤشرات أو إشارات أو كتابة أو صور أو أصوات أو بيانات أو أي معلومات من أي نوع يتم بثها جزئياً أو كلياً بواسطة نظام سلكي أو لاسلكي أو كهرومغناطيسي أو كهروضوئي أو ضوئي بصري "[305] .

وكما هو ملاحظ من التعريفات السابقة ، أن الاعتراض يقتصر على الاتصالات التي يتم التقاطها أثناء البث ، دون أن تتطرق إلى بيان مصير الاتصالات الإلكترونية المخزنة ، فعلى سبيل المثال قد يمضي البريد الصوتي بعض الوقت في حالة تخزين إلكتروني قبل أن يتم استلامه بواسطة المرسل إليه .

غير أن المشرع الأمريكي اعتبر الاتصالات الإلكترونية المخزنة من قبيل البيانات التي تنطبق عليها كل الإجراءات ، التي تتلاءم مع هذا النوع من البيانات ، كالأمر بالتحفظ المعجل ، وأمر تقديم البيانات ، والدليل على ذلك أنه قام بتعديل القسم (2703) من قانون (ECPA) المتعلق

---

(301) سامح أحمد بلتاجي موسى ، الجوانب الإجرائية للحماية الجنائية شبكة الإنترنت ، رسالة دكتوراه ، كلية الحقوق ، جامعة الإسكندرية ، 2010 ، ص104- 105 .

(302) شيماء عبدالغني محمد عطا الله ، مرجع سابق ، ص305 .

(303) عمر محمد بن يونس ، الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي ، مرجع سابق ، ص362

(304) شيماء عبدالغني محمد عطا الله ، المرجع السابق ، ص265 .

(305) عمر محمد بن يونس ، الاجراءات الجنائية عبر الانترنت في القانون الامريكي ، المرجع السابق ، ص 365.

بخصوصية الاتصالات الإلكترونية ، ليشمل عبارة الاتصالات الإلكترونية المخزنة صراحة[306] ، كالبريد الإلكتروني مثلاً .

ثانياً . أهمية اعتراض الاتصالات الإلكترونية :

تكمن أهمية اعتراض الاتصالات الإلكترونية من خلال ما نص عليه المشرع الليبي في المادة (79) من قانون الإجراءات الجنائية الليبي حيث نصت " لقاضي التحقيق أن يضبط لدى مكاتب البريد كافة الخطابات والرسائل والجرائد والمطبوعات والطرود ولدى مكاتب تلغرافات كافة البرقيات كما يجوز له مراقبة المحادثات التليفونية متى كان لذلك فائدة في ظهور الحقيقة "، ويقابل ذلك نص المادة (95) من قانون الإجراءات الجنائية المصري.

وكما هو ملاحظ من نص هذه المادة ، أنه علق اعتراض الاتصالات بشرط أن تكون هناك فائدة في كشف الحقيقة ، وتكمن العلة من هذا الشرط في أن المراقبة إجراء استثنائي أملته الضرورة ، لأنه يعتبر تعدياً خطيراً على حق المرء في حياته الخاصة ، فسرية حديث الشخص مع غيره تُعد من الأمور المتعلقة بكيانه الشخصي ، ففي هذه الأحاديث يثق المتصل بشخص المتصل إليه فيتحدث دون خوف من أن يسمعه أحد غيره لثقته أنه في مأمن من استراق السمع[307] ، فيسمح استثناءاً اتخاذ مثل هذا الإجراء في حدود الفائدة المتعلقة بإظهار غموض الجريمة أو العمل على ضبط الجناة[308] ، لأن الجناة أصبحوا يتفننون في إخفاء جرائمهم مما يتطلب تزويد رجال الضبط القضائي بأحدث الوسائل التي تساعدهم على اكتشاف الجريمة وملاحقة مرتكبيها[309] ، وبالتالي فإنه لا مناص من تقرير شرعية مراقبة المحادثات التليفونية في الحدود المسموح بها قانوناً[310] .

وقد أيد القضاء الياباني مشروعية هذا الإجراء بالرغم من أن القانون الياباني لم ينص على السماح به بشكل صريح ، وذلك من خلال ما انتهت إليه محكمة مقاطعة Kofa سنة 1991 حيث أقرت مشروعية التنصت على شبكات الحاسب الآلي في سبيل البحث عن الدليل[311] .

---

(306) عمر محمد بن يونس ، الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي ، مرجع سابق ، ص365 - 370.

(307) محمد رشاد إبراهيم مفتاح ، مرجع سابق ، ص58 .

(308) محمد ابو العلا عقيدة ، مراقبة المحادثات التليفونية ، دار الفكر العربي ، 1994 ، ص192.

(309) سليمان عبدالمجيد ،" مراقبة المحادثات التليفونية " ، مجلة الأمن العام ، العدد 41 ، السنة 11 ذو القعدة 1968 ، ص23.

(310) محمد حلمي حسان ، الحماية الجنائية للمحادثات الهاتفية ، رسالة ماجستير ، كلية الحقوق ، جامعة الاسكندرية ، 2008 ، ص84 .

(311) موسى مسعود أرحومة ، " الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية " ، بحث مقدم إلى المؤتمر المغاربي الأول حول المعلوماتية والقانون الذي نظمته أكاديمية الدراسات العليا طرابلس خلال الفترة 28-2009/10/29 ، ص13 .

الفرع الثاني
الضمانات القانونية لمشروعية اعتراض الاتصالات الإلكترونية

لم ينص المشرع الليبي على هذه الضمانات ، وإنما نص عليها المشرع المصري بشأن مراقبة المحادثات التليفونية ، غير أنه لا تقتصر على هذا النوع من المحادثات الهاتفية فقط ، بل تمتد هذه الضمانات إلى الاتصالات الإلكترونية عبر الإنترنت ، لأن الغرض من وراء هذه الضمانات هي حماية الحياة الخاصة للإنسان المتعلقة بأسراره ، التي غالباً ما تكون أكثر انتهاكاً إذا ما استعملت الطرق الإلكترونية للتعرض إليها.[312]

ومن هذه الضمانات ضرورة صدور إذن من القاضي باعتراض الاتصالات الإلكترونية وأن يكون إذن القاضي باعتراض الاتصالات مسبباً ، وأن يكون اعتراض الاتصالات بصدد جريمة معينة وقعت فعلاً وأن تكون هناك مدة للاعتراض محددة قانوناً ، وهذا ما سنبينه في مايلي :

أولاً . ضرورة صدور إذن من القاضي باعتراض الاتصالات الإلكترونية:

يعتبر الحصول على إذن من القاضي باعتراض الاتصالات الإلكترونية من أهم الضمانات الضرورية لمشروعيتها ، فقد نصت المادة (95) من قانون الإجراءات الجنائية المصري " لقاضي التحقيق أن يأمر بضبط جميع الخطابات والرسائل والجرائد والمطبوعات والطرود لدى مكاتب البريد وجميع البرقيات لدى مكاتب البرق ، وأن يأمر بمراقبة المحادثات السلكية واللاسلكية ، أو إجراء تسجيلات لأحاديث جرت في مكان خاص متى كان لذلك فائدة في ظهور الحقيقة في جناية أو جنحة معاقب عليها بالحبس لمدة تزيد على ثلاثة أشهر ، وفي جميع الأحوال يجب أن يكون الضبط أو الإطلاع أو المراقبة أو التسجيل بناءً على أمر مسبب ولمدة لا تزيد عن ثلاثين يوماً قابلة للتجديد لمدة أو لمدد أخرى مماثلة."

ويلاحظ من خلال هذا النص أن قاضي التحقيق يختص بإصدار الإذن باعتراض المحادثات التليفونية ، إذا كان هو المباشر للتحقيق ، وإذا تولت النيابة العامة التحقيق فالقاضي الجزئي هو المختص بالإذن لها باعتراض المحادثات التليفونية[313] .

---

[312] علي محمود علي حمودة ، مرجع سابق ، بدون ترقيم صفحات

[313] المادة (180) من قانون الإجراءات الجنائية الليبي.

وسلطة قاض التحقيق في هذا المجال أوسع من السلطة المخولة للقاضي الجزئي ، فله أن يأمر باعتراض المحادثات التليفونية ويندب لتنفيذها أحد رجال الضبط القضائي[314] .

وإذا كانت النيابة العامة هي التي تتولى التحقيق ورأت ضرورة اعتراض المحادثات التليفونية الخاصة بالمتهم أو ببعض المتهمين ، فعليها أن تطلب من القاضي الجزئي الإذن بالاعتراض ، وبعد الحصول على الإذن يمكنها مباشرة الاعتراض بنفسها ، أو أن تقوم بانتداب أحد مأموري الضبط القضائي للقيام بها ، وللقاضي الجزئي مطلق الحرية في الإذن بالاعتراض أو رفضه ، ويخضع في هذا التقدير لإشراف قاضي الموضوع.[315]

غير أنه ذهب جانب من الفقه إلى أنه يجوز للنيابة العامة في حالة الضرورة أو الاستعجال صدور إذن بالاعتراض بشرط أن يحصل التصديق عليها فيما بعد من القاضي الجزئي[316].

إلا أننا نتفق لمن ينادي بضرورة الحصول مسبقاً على إذن من القاضي الجزئي الذي يكون رأيه على ضوء ما يقدم إليه من أوراق بخصوص إصدار الإذن بالاعتراض أو رفضه[317] ، ففي الولايات المتحدة الأمريكية مثلاً يجيز القانون اعتراض الاتصالات الإلكترونية بصفة عامة ، بما في ذلك شبكات الحاسب الآلي وذلك متى تم بإذن من المحكمة[318].

أما في إنجلترا فيجوز لوزير الداخلية أن يأذن لرجال الضبط القضائي باعتراض وضبط المكالمات والمراسلات ، على أساس أنه إجراء استثنائي يجب اتخاذ كل الحذر والحيطة قبل اتخاذه.[319]

وعلى نقيض ماسبق قام المشرع الأمريكي بتحديد الحالات التي يجوز فيها اعتراض الاتصالات الإلكترونية بطريقة مشروعة ودون صدور إذن من السلطة القضائية المختصة ، وذلك من خلال منح مزود الخدمات السلطة في اعتراض النظام دون إذن ، وذلك باستخدام طريقتين كالآتي :

---

(314) عوض محمد عوض ، المبادئ العامة في قانون الإجراءات الجنائية ، مرجع سابق ، ص406 .

(315) سليمان عبدالمجيد ، مرجع سابق ، ص26 -27 .

(316) جندي عبدالملك ، ج2 ، مرجع سابق ، ص266 .

(317) محمود نجيب حسني ، مرجع سابق ، ص685 - 686.

(318) موسى مسعود أرحومة ، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية ، مرجع سابق ، ص13 .

(319) محمد حلمي محمد حسان ، مرجع سابق ، ص63 .

أ) الاعتراض بطريقة معتادة لعمل الشبكة من قِبل مزودي الخدمات :

قرر المشرع الأمريكي من خلال القسم (أ) (a)(2) (18, use , 2511) منح مزود الخدمات الحق في أن يقوموا بمراقبة المشتركين في خدماتهم ، وذلك من أجل معرفة مايقوم به هؤلاء المشتركين من نشاط ، حتى يمكنهم من الدفاع عن تلك الحقوق في مواجهة المشتركين في الخدمات التي يقدمونها بمقابل ، أو الذين يستخدمون تلك الخدمات ، وذلك حتى يمكنهم من الأداء اليومي لأجهزتهم ومعداتهم .

فمن حقوق مزودي الخدمات التي يحميها المشرع الأمريكي حقهم في حماية أنظمتهم كالأجهزة من إساءة الاستعمال أو الإضرار بها كزرع الفيروسات أو الاستيلاء عليها كالسرقة أو انتهاك الحق في الخصوصية كالاختراق .

ومن التطبيقات القضائية على اعتراض الاتصالات الإلكترونية ، ما قضى به من أنه يجوز لمزودي الخدمات ، أن يقوموا بالاعتراض لمكافحة السرقة الواقعة على الخدمات التي يقدمونها من ذلك أن يقوم أحد الأشخاص بتقليد خط الهاتف المحمول للحصول على الخدمة دون دفع الاشتراك ، الأمر الذي يقضي أن يتابع مزودو الخدمة هذا الخط المقلد لتحديد مكانه ومعرفة الفاعل لذلك[320] .

غير أن المشرع الأمريكي لم يمنح هذا الحق على مصراعيه بالنسبة لمزودي الخدمات وإنما قيد ذلك بشروط محددة[321] ، وهي :

1- أن يكون مزود الخدمات مجنياً عليه في الجريمة .

2- أن يقوم مزود الخدمات باعتراض الاتصالات من أجل حماية حقوقه .

3- أن تقوم السلطات القضائية المختصة بتأكيد صحة قيام مزود الخدمات العمل من أجل حماية حقوقه من عدمها .

4- عدم طلب المساعدات من مزود الخدمات الاعتراض لأجل أهداف أخرى ، كمساعدة السلطات في التحريات التي يقومون بها .

---

[320] شيماء عبدالغني محمد عطا الله ، مرجع سابق ، ص221 – 222 .

[321] عمر محمد بن يونس ، الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي ، مرجع سابق ، ص386 – 387.

5- عدم إشراف السلطات القضائية المختصة عند قيام مزودي الخدمات بالاعتراض .

ب) اعتراض الاتصالات الإلكترونية بناءً على شكوى المشترك :

اختلفت الآراء بين مؤيد ومعارض فيما يتعلق باعتراض الاتصالات الإلكترونية من قِبل مزود الخدمات وذلك بناءً على شكوى المشترك في حالة الاعتداء على الجهاز الخاص به وسنعرض هذين الاتجاهين فيما يلي :

الاتجاه الأول :

يرى أنصار هذا الاتجاه والذي يعتنقه القانون الأمريكي بأنه يسمح القسم ((i) (2)2511) لضحايا الهجوم على الحاسب الآلي بتفويض السلطات القضائية المختصة لاعتراض الاتصالات السلكية أو الإلكترونية للمعتدى[322] ، التي يتم بثها إلى أو من جهاز حاسب آلي محمي أي الحاسوب المرتبط بالإنترنت ، إذا توافرت أربعة شروط[323] ، وهي :

1- أن يسمح صاحب الجهاز للسلطات القضائية المختصة بوضع الجهاز الخاص به تحت المراقبة ، على أن يكون صاحب الجهاز قد سمح بذلك بطريقة مكتوبة .

2- يجب أن يكون الشخص الذي تكفل إليه مهمة اعتراض الاتصالات عضواً في التحقيق بشكل قانوني .

3- يجب أن تكون هناك معلومات كافية لدى الشخص الذي يعترض الاتصالات ، بأن محتويات الاتصالات القادمة من جهاز الحاسب الآلي الصادر منه الاعتداء ، له صلة بالتحقيق ويفيد في إظهار الحقيقة .

4- يجب أن تقتصر مهمة السلطات المخولة بالمراقبة على اعتراض الاتصالات التي تم بثها من وإلى الأجهزة محل الاعتداء .

---

[322] يستبعد المشرع الأمريكي في تحديده لمفهوم المعتدي على النظام ، كل من تربطه علاقة تعاقدية مع مزود الخدمة والذي يتجاوز الحدود التي تسمح بها تلك العلاقة ، ومثال ذلك مستخدمو شركة معينة لا يعتبرون في عداد المعتدين على النظام إذا استغلوا أجهزة الشركة في أغراض أو في أوقات بالمخالفة لنظام الشركة .
(شيماء عبدالغني محمد عطا الله ، مرجع سابق ، ص225) .

[323] عمر محمد بن يونس ، الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي ، مرجع سابق ، ص390 - 391.

الاتجاه الثاني :

يذهب أنصار هذا الاتجاه والذي يعتنقه ميثاق الحقوق والحريات الكندي في المادة (24 فقرة 2) ، الذي يعتبر فيه أن مزود الخدمة متماثل في عمله مع رجال السلطة العامة ، وبالتالي فإنه ليس من حقه القيام باعتراض الاتصالات دون إذن[324] .

وذلك إستنادا إلي أن القضاء هو الحامي للحقوق والحريات العامة ، فاعتراض المحادثات التليفونية يعد انتهاكاً خطيراً للحرية والحق في السرية ، مما يجب أن يصدر الإذن بها من القضاء منعاً للتعسف من أي جهة أخرى[325] .

ومن خلال الموازنة بين الاتجاهين نرجح ونؤيد الاتجاه الأول ، لأن في ذلك مصلحة تفيد المجتمع في إظهار حقيقة الجريمة ، ومنعاً لإفلات المجرمين من العقاب تعلو مصلحة الفرد في حرمة حياته الخاصة ، إذا تم ذلك في حدود الشروط أو الضمانات القانونية لإتخاذ مثل هذا الإجراء ، علاوة على ذلك فإن الجرائم الإلكترونية لا تستغرق غالباً في إرتكابها إلا بضع ثواني ، ويمكن إزالة آثار إرتكابها وإخفائها بسهولة أو العبث بأدلتها .

ثانياً . أن يكون إذن القاضي باعتراض الاتصالات الإلكترونية مسبباً :

من الضمانات الأساسية التي نص عليها المشرع المصري ، عدم جواز ضبط المراسلات أو مراقبة المحادثات التليفونية وغيرها من وسائل الاتصال ، إلا بأمر قضائي مسبب، والحكمة من وراء ذلك أن مراقبة الاتصالات تعد إجراء خطيراً يمس حريات الأفراد وحقوقهم وتنتهك حقهم الطبيعي في السرية ، وهو إجراء استثنائي تبرره المصلحة العامة المتمثلة في كشف الحقيقة عن جريمة وقعت ومعاقبة مرتكبيها.

ولم يحدد القانون شكلاً معيناً للتسبيب ، لذا ذهب جانب من الفقه إلى القول بأن من الأسباب التي يجوز للقاضي إصدار إذن باعتراض الاتصالات الإلكترونية ، الاعتقاد بأن هناك معلومات تفيد في كشف الجريمة يمكن الحصول عليها عن طريق ذلك التنصت المتعلق بالاتصالات الإلكترونية المطلوب التصريح بها ، وكذلك من تلك الأسباب أيضاً عدم كفاية ما نفذ من الإجراءات العادية للبحث والتحري وعدم قدرتها على إظهار حقيقة الجريمة[326] .

---

(324) شيماء عبدالغني محمد عطا الله ، مرجع سابق ، ص224 – 225.

(325) محمد أبو العلا عقيدة ، مراقبة المحادثات التليفونية ، مرجع سابق ، ص169 .

(326) محمد حلمي حسان ، مرجع سابق ، ص60 .

ثالثاً . عدم جواز اعتراض الاتصالات الإلكترونية إلا بصدد جريمة معينة وقعت فعلاً :

تعتبر هذه الضمانة من الضمانات الضرورية لصحة اعتراض الاتصالات الإلكترونية وهو ما نص عليه المشرع المصري في المادتين (95 ، 206) من قانون الإجراءات الجنائية المصري ، حيث اشترط لمراقبة المحادثات التليفونية أن تكون بصدد جريمة معينة جناية أو جنحة معاقب عليها بالحبس مدة تزيد على ثلاثة أشهر ، ويشترط أن تكون الجريمة قد وقعت فعلاً واكتشف أمرها فلا يصح اللجوء إليه في جريمة أقل من ذلك شأناً ، كما لا يصح اتخاذه وسيلة لضبط جريمة لم تقع بعد ولو كانت وشيكة الوقوع ، لأن هذا الإجراء بطبيعته وفي كل أحواله إجراء تحقيق وليس إجراء استدلال[327] .

وقد حدد المشرع الجزائري الجرائم التي يجوز فيها اعتراض المراسلات وذلك بموجب القانون الصادر في (20 ديسمبر 2006) المعدل لقانون الإجراءات الجزائية وتم النص عليها في المادة (65 مكرر 5) على نوع الجرائم التي يجوز فيها اعتراض المراسلات بواسطة وسائل الاتصال السلكية واللاسلكية ، وهي جرائم المخدرات والجريمة المنظمة وجريمة تبييض الأموال والجرائم الإرهابية وجرائم الفساد والجرائم المعلوماتية[328] .

أما في هولندا فإنه يجوز لقاضي التحقيق أن يأمر بالتنصت على شبكات اتصالات الحاسب الآلي إذا كان لغرض ضبط جرائم خطيرة ، ويمكن أن تتم المراقبة أيضاً على الفاكس ونقل البيانات.[329]

رابعاً ـ أن تكون هناك مدة محددة قانوناً لاعتراض الاتصالات الإلكترونية :

لقد حدد المشرع المصري مدة معينة لمراقبة المحادثات التليفونية ثلاثين يوماً قابلة للتجديد لمدة أو لمدد أخرى .

ويصدر الأذن بتجديد مدة المراقبة من القاضي الجزئي بعد أن تطلب منه النيابة العامة ذلك ، أما إذا كان قاضي التحقيق هو المختص بالتحقيق في الدعوى فإن تجديد مدة المراقبة يقوم به من تلقاء نفسه ، وتكمن العلة من وراء تحديد مدة المراقبة أو الاعتراض هو منع التعسف في إساءة استعمال السلطة[330] .

---

[327] عوض محمد عوض ، المبادئ العامة في قانون الإجراءات الجنائية ، مرجع سابق ، ص405 .

[328] Http//www.startimes.com/f.aspx?t=33675371

[329] علي محمود علي حمودة ، مرجع سابق ، بدون ترقيم صفحات .

[330] محمد أبو العلا عقيدة ، مراقبة المحادثات التليفونية ، مرجع سابق ، ص193 .

خامساً . أن يكون المتهم طرفاً في المحادثات التي يؤمر باعتراضها أو تسجيلها :

ويقصد بذلك أن يكون المتهم هو صاحب التليفون أو الحاسوب أو حائزه ، أو أن يكون موجوداً في المجلس الذي يدور الحديث فيه ، وهذا الشرط غير منصوص عليه صراحة لكنه ضروري ، لأن عدم ذكره يؤدي إلى المساس بالضمانة القانونية التي تحمي الحياة الخاصة للأفراد المتعلقة بحرمة وسائل الاتصال وسريتها.[331] .

وكما هو ملاحظ فيما تقدم أنه إذا اجتمعت الضوابط المقررة قانوناً ، فيما يتعلق بمراقبة الاتصالات السلكية واللاسلكية ، يترتب على ذلك مشروعية الإجراء ومشروعية الدليل الرقمي المسفر عنه في إثبات الجريمة الإلكترونية ونسبتها إلى مرتكبها ، وفي حالة فقدان شرط من الشروط السابقة ، يترتب عليه عدم مشروعية الإجراء وبطلان الدليل ، علاوة على ذلك فإنه يسأل منفذ هذا الإجراء عن جريمة الاعتراض الغير مشروع المنصوص عليه في قانون العقوبات الليبي في المادة (244) عقوبات ليبي التي تنص على أنه "يعاقب بالحبس مدة لا تقل عن ستة أشهر كل موظف عمومي تابع لمصلحة البريد والتليفون والبرق أخفى أو أوقف أو أخر رسالة أو اطلع عليها وأفشى للغير ما حوته ، وفي هذه المادة يراد من الرسالة المكاتيب والمحادثات التليفونية والبرقيات وما إلى ذلك من وسائل الإرسال .

وإذا ارتكب الأفعال المذكورة أشخاص آخرون تكون العقوبة الحبس مدة لا تزيد على ستة أشهر أو غرامة لا تتجاوز عشرين جنيهاً وذلك بناءً على شكوى الطرف المتضرر ." كما أشار قانون رقم (22) لسنة 1378و.ر (2010 م) بشإن الاتصالات الليبي إلى تجريم إفشاء الأسرار حين نصت المادة (26) على أنه " يعاقب بالحبس مدة لاتزيد على ثلاثة أشهر وبغرامة لاتقل عن ألف دينار ولاتزيد على خمسة ألاف دينار كل من أذاع أو نشر أو أشاع دون حق ، مضمون رسالة أو اتصال أو جزءا منه إطلع عليه بحكم عمله أو أساء استعمال معلومات تتعلق بالمستفيدين ".

---

[331] عوض محمد عوض ، المبادئ العامة في قانون الإجراءات الجنائية ، مرجع سابق ، ص406 .

الفصل الثالث

حجية الدليل الرقمي أمام القضاء الجنائي

القاعدة العامة في الدعوى الجنائية ، هي جواز الإثبات بجميع الوسائل القانونية ، والقيد على هذه القاعدة أنه يجب أن يكون الدليل من الأدلة المقبولة قانوناً ، وبالتالي تظهر أهمية اعتراف القانون بالأدلة الرقمية خاصة مع احتمال ظهور أنماط إجرامية جديدة لجميع الجرائم ، وخاصة في الجرائم الإلكترونية ، فالتطور الحالي الذي تأثر به قانون العقوبات قد تأثر به أيضاً قانون الإجراءات الجنائية ، بحيث أن هذا القانون الأخير قد لا يطبق بسبب عجز القانون الأول عن ضم الجرائم ذات الطبيعة الخاصة إليه ، والتي ترتكب بالوسائل الإلكترونية وبما أن الإثبات الجنائي هو أحد الموضوعات الهامة لهذا القانون قد تأثر هو أيضاً بالتطور الهائل الذي لحق بالأدلة الجنائية نظراً لتطور طرق ارتكاب الجريمة مما يؤدي إلى كثير من المشكلات خاصةً أن الدليل الرقمي يمر بمراحل معقدة لكي يتم الحصول عليه ، غير أن الدليل الرقمي يخضع لنفس القواعد المقررة لباقي الأدلة الجنائية سواءً كانت هذه القواعد تتعلق بقبول الدليل الرقمي، أو تقديره أمام القضاء الجنائي ، ذلك أن قبول الدليل الرقمي أمام القضاء الجنائي ، يتطلب معرفة موقف الأنظمة الإجرائية من حيث وجود مشروعيته ، حيث تختلف تلك الأنظمة مابين نظام الإثبات القانوني ونظام الإثبات الحر ونظام الإثبات المختلط ، وكذلك من حيث مشروعية حصوله ، ذلك أن الدليل يتطلب لكي يتم قبوله أمام القضاء الجنائي ، أن يكون قد تم الحصول عليه من إجراء صحيح ومشروع وخضع لحرية مناقشة أطراف الدعوى خلال جلسات المحاكمة ، أما تقدير الدليل الرقمي أمام القضاء الجنائي هذا مرده أن هذا الدليل يتمتع بخصائص تميزه عن غيره من الأدلة الجنائية التقليدية ، مما يجعله دليلا ذو طبيعة علمية يؤدي إلى إثارة صعوبات في مدى تأثيرها على عقيدة القاضي الجنائي والذي لايستطيع أن يؤسس حكمه إلا على دليل مستمد من أدلة مقتنع بها إلى حد الجزم واليقين ، ولعل أهم هذه الصعوبات مشكلة المصلحة الأولى بالرعاية ، وصعوبات تعارض الإثبات بالدليل الرقمي مع حرية القاضي الجنائي في تكوين عقيدته من حيث عدم رؤية الدليل الرقمي ومشكلة التحقق من أصالة ومصدر هذا الدليل .

وبناء على ما تقدم سنقسم هذا الفصل إلى مبحثين : نخصص المبحث الأول لدراسة قبول الدليل الرقمي أمام القضاء الجنائي . ونكرس المبحث الثاني لدراسة تقدير القضاء الجنائي للدليل الرقمي.

المبحث الأول

قبول الدليل الرقمي أمام القضاء الجنائي

يعتبر قبول الدليل الرقمي أمام القضاء الجنائي من المراحل الإجرائية الأولية ، وذلك للتأكد من صحته قبل البدء في تقديره مما يتطلب معرفة موقف الأنظمة الإجرائية من الدليل الرقمي كدليل إثبات أمام القضاء الجنائي ، حيث تختلف تلك الأنظمة ما بين نظام الإثبات القانوني المقيد و نظام الإثبات الحر و نظام الإثبات المختلط ، ويسعى القاضي الجنائي في هذه المرحلة إلى التأكد من صحة وسلامة الدليل الرقمي ، مما يستلزم ذلك بيان مشروعية الدليل الرقمي ، وكيفية مناقشته ومدى تقيده بطرق الإثبات المقررة في القوانين الخاصة .

وبناء على ما تقدم سنقسم هذا المبحث إلى مطلبين : نخصص المطلب الأول لدراسة موقف الأنظمة الإجرائية من قبول الدليل الرقمي أمام القضاء الجنائي . أما المطلب الثاني سنخصصه لدراسة شروط قبول الدليل الرقمي أمام القضاء الجنائي .

المطلب الأول

موقف الأنظمة الإجرائية من قبول الدليل الرقمي أمام القضاء الجنائي

اختلفت التشريعات المقارنة في الأخذ بالدليل الرقمي كدليل إثبات أمام القاضي الجنائي ، فمنها من حدد الأدلة المقبولة في الإثبات ، وهو ما يسمى بالإثبات المقيد أو القانوني ، وثانيهما من أوكل إلى القاضي تقدير قيمة الدليل ، وتكوين عقيدته عليه ، وهو ما يسمى بالإثبات الحر ، وآخر هذه الأنظمة هو مزيج من النظامين السابقين ، وهو ما يسمى بالنظام المختلط .

وبناءً على ما تقدم سنقسم هذا المطلب إلى ثلاثة فروع : نخصص الفرع الأول لدراسة نظام الإثبات المقيد أو القانوني . ونكرس الفرع الثاني لدراسة نظام الإثبات الحر . ونفرد الفرع الثالث لدراسة نظام الإثبات المختلط .

الفرع الأول

نظام الإثبات المقيد أو القانوني

يقصد بنظام الإثبات القانوني ، أو ما يسمى بنظام الأدلة القانونية أن المشرع يحدد مسبقاً للقاضي الأدلة التي يجوز قبولها ، والاستناد إليها في الحكم بالإدانة ، فإذا توافرت أدلة الإدانة بشروطها التي حددها القانون ألتزم القاضي بإدانة المتهم ، ولو كان ذلك مخالفاً لقناعته بالإدانة وإذا لم تتوافر تلك الأدلة فإن القاضي يلتزم بتبرئة المتهم ، ولو كان مقتنعاً بإدانته.[332]

وفي هذا النظام يقوم اقتناع المشرع بصحة الإسناد ، وعدم صحته مقام اقتناع القاضي ، وهو اقتناع مبني على افتراض صحة الدليل ، بغض النظر عن حقيقة الواقعة المعروضة على

---

[332] محمود نجيب حسني ، مرجع سابق ، ص421.

القاضي ، واختلاف ظروف الدعوى[333] ، فيلزم القاضي الأخذ بوسيلة معينة للإثبات مراعياً تطبيق القانون من حيث توافر الأدلة وشروطها فقط ، ولا يجوز له إثبات المسألة محل النزاع إلا بهذه الوسيلة.[334]

وفي مقدمة الدول التي تتبنى هذا النظام بريطانيا حيث أصدرت قانون إساءة استخدام الحاسوب 1990م ، غير أنه لم يتناول الأدلة الناتجة عن الحاسوب ، ويرجع ذلك إلى وجود قانون البوليس والإثبات الجنائي الصادر في سنة 1984م ، الذي يتضمن بشيء من التحديد مسألة قبول مخرجات الحاسوب كأدلة إثبات في المواد الجنائية ، فمخرجات الحاسوب لاتقبل كدليل إثبات ، إلا في حالة عدم وجود سبب معقول بان هذه المخرجات غير دقيقة ، أو أن بياناتها غير سليمة ، كما يجب أن يكون جهاز الحاسوب الذي ينتج عنه هذه المخرجات يعمل بكفاءة وبصورة سليمة وصحيحة.[335]

غير أن الأحكام الأخيرة للمحاكم البريطانية تتضمن إلى أن الشروط سالفة الذكر لا تنطبق إذا كانت مطبوعات الحاسب الآلي دليلاً أصلياً وليس نقلاً عن الغير ، وقد حدا ذلك ببعض المتخصصين في مجال الحاسوب استحالة إثبات دقة جهاز الحاسوب بالشروط المنصوص عليها في القانون ، وهو ما أدى إلى مناقشة عدد من المعلقين إلغاء القسم (69) من هذا القانون أسوةً بما قررته اللجنة القانونية الاسكتلندية في القسم (69) بشأن الدليل المستخلص عن الحاسوب حيث اعتبرته غير ضروري في المحاكم الجنائية باسكتلندا.[336]

أما في الولايات المتحدة الأمريكية فقد نص قانون الحاسوب الصادر سنة 1984م بولاية (إيوا) على أن مخرجات جهاز الحاسوب تكون مقبولة بوصفها أدلة إثبات بالنسبة للبرامج والبيانات المخزنة فيه ، كما نص أيضاً قانون الإثبات الصادر سنة 1983م بولاية كاليفورنيا ، على أن النسخ المستخرجة من البيانات التي يتضمنها جهاز الحاسوب تكون مقبولة بوصفها أفضل الأدلة في مجال الإثبات.[337]

وهذا ما أكدته المحاكم الجنائية الأمريكية عند اعترافها بالأدلة الرقمية ، حيث أخذت بالملفات الرقمية والرسائل الالكترونية كدليل في المحاكم لتصبح من المشهد القضائي ، مما يشكل ذلك سلاحاً جديداً بين أيدي الشرطة والنيابة العامة والقضاء في الدعاوى الجنائية[338]، بشرط أن يكون

---

[333] محمود محمود مصطفى ، الاثبات في المواد الجنائية ، مرجع سابق ، ص7.

[334] عبدالحكم فوده ، مرجع سابق ، ص18.
- أحمد الصادق الجهاني ، مرجع سابق ، ص1.

[335] هلالي عبداللاه أحمد ، حجية المخرجات الكمبيوترية في المواد الجنائية ، مرجع سابق ، ص 52 – 53.

[336] طارق فوزي الفقي ، الجوانب الإجرائية في الجرائم المعلوماتية ، رسالة دكتوراه ، كلية الحقوق ، جامعة المنوفية ،2011 ، ص226.

[337] أيمن عبدالحفيظ عبدالحميد سليمان ، استرتيجية مكافحة الجرائم الناشئة عن استخدام الحاسب الآلي ، رسالة دكتوراه ، اكاديمية الشرطة ، كلية الدراسات العليا ، 2003 ، ص372.

[338] سامح أحمد بلتاجي موسى ، مرجع سابق ، ص438.

الحاسوب المتولد عنه الدليل يؤدي وظائفه بصورة سليمة ، وأن يكون القائم عليه تتوافر فيه الثقة والطمأنينة[339] .

وفي كندا يمكن قبول السجلات الناتجة عن الحاسوب إذا توفرت شروط محددة ، حيث نصت المادة (29) من قانون الإثبات الكندي والخاصة بسجلات المؤسسات المالية على عدد من الشروط التي يجب اتخاذها قبل القيام بعمل صورة من السجل الذي يضاف إلى الأدلة ، ومن هذه الشروط أن تكون الصورة حقيقية من المدخّل الأصلي.

وقد قضت محكمة استئناف اونتاريو في قضية بيل وبيرس ، لمواقع كانت فيها قاعدة البيانات الالكترونية الأصلية قد حذفت وكل ما تبقى منها هي مخرجات الطابعة ، وقد استخدم البنك هذه المخرجات المطبوعة على أنها هي الأصل وليس مجرد صورة ، فأيدت المحكمة ذلك وقالت أن الصورة في هذه الظروف التي كان يستخدمها البنك تنزل منزلة الأصل ، وتصبح هذه الصورة هي السجل الأصلي.[340]

ومما تجدر الإشارة إليه أن نظام الإثبات المقيد أو القانوني الذي أخذت به التشريعات الانجلوساكسونية ، تخضع بوجه عام لقاعدتين : قاعدة عدم جواز الشهادة بالتسامع وهذا ما سنتناوله في هذا المقام ، وقاعدة الدليل الأفضل (يقينية الدليل الرقمي) ، والتي سنتناولها بشيء من التفصيل عند دراستنا في المبحث الثاني لتقدير القضاء الجنائي للدليل الرقمي في المطلب الثاني المتعلق بيقينية الدليل الرقمي.

الشهادة بالتسامع : يقصد بها "ماتتسامعه الناس في شأن الواقعة وهي لاتنصب على الواقعة المراد إثباتها ، بل على الرأي الشائع لدى جمهور الناس عن هذه الواقعة ، فهي لا تعتبر دليلاً ولايجوز أن يستمد القاضي منها اقتناعه"[341] ، وتختلف الشهادة بالتسامع عن الشهادة السماعية (أو النقلية أو شهادة السماع) حيث أن هذه الأخيرة تعرف بأنها هي رواية الشاهد أمام المحكمة وقائع لم يعاينها بنفسه وإنما علم بها من شخص آخر ليس موجوداً أمام المحكمة[342] ، والجدير بالذكر أن الشهادة السماعية لا يعتد بها في كثير من الأحيان ، غير أنه إذا أقتنع بها القاضي ، له أن يستمد منها اقتناعه ويبني عليها حكمه.[343]

إلا أن موقف القضاء الأمريكي يختلف وذلك بشأن الشهادة السماعية حيث أنه يأخذ بها في حالات معينة كدليل تستند إليه المحكمة وتحكم بمقتضاها ، ولا تأخذ بها في حالات أخرى إلا على أنه دليل معزز ، وهذه الحالات [344] هي كالاتي :

---

[339] سليمان أحمد فضل ، مرجع سابق ، ص368.
[340] هلالي عبداللاه أحمد ، حجية المخرجات الكمبيوترية في المواد الجنائية ، مرجع سابق ، ص 55-56.
[341] محمود نجيب حسني ، مرجع سابق ، ص453.
[342] رمزي رياض عوض ، سلطة القاضي الجنائي في تقدير الأدلة (دراسة مقارنة) ، دار النهضة العربية ، القاهرة ، 2010 ، ص100
[343] محمود نجيب حسني ، المرجع السابق ، ص453.
[344] رمزي رياض عوض ، المرجع السابق ، ص 101 ومابعدها .

أ) الأقوال المنقولة عن المجني عليه التي نطق بها قبل وفاته.
ب) إخبار أحد أعضاء الاتفاق الجنائي .
ج) التسجيلات الرسمية .
د) التقرير التلقائي .
هـ) النطق بمفهوم الانطباعية .
و) المعلومات والبيانات التي تم الحصول عليها من الحاسوب.[345]
ي) الدفاتر التجارية.[346]

أما القضاء الانجليزي قد يستبعد الشهادة السماعية إذا وجدت أدلة أخرى ، أو إذا لم يطمئن إليها ، وقد يقبلها كدليل بوصفه شهادة مباشرة وليست سماعيه ، حيث قضت محكمة في انجلترا بقبول الدليل المستخرج من الكمبيوتر في قضية R.V.pettigrew والتي تتلخص وقائعها أنه وجد في حيازة المتهم الذي قام بالسطو على البنك أرقام النقود المسروقة ، والتي كانت مسجلة في كمبيوتر البنك في انجلترا ، وقد قبلت المحكمة في هذه القضية مخرجات الكمبيوتر الورقية باعتبارها دليلاً مباشراً وليس من الأدلة السماعية.[347]

ونلاحظ فيما تقدم أنه لا يمكن القول بان الشهادة السماعية تصلح كدليل في الدعوى الجنائية بحكم مقتضاها كقاعدة عامة ، وإنما يكفي النظر إليها على أنها دليل معزز ، ويرجع ذلك في عدم الثقة في الشخص الذي يدلي بالعبارات والأقوال خارج المحكمة ، وهو لايؤدي يميناً ، ولايخضع لملاحظة القاضي أو المحكمة وقت إدلائه بأقواله.

الفرع الثاني

نظام الإثبات الحر

يقصد بنظام الإثبات الحر[348]، أن القاضي الجنائي حر في تكوين عقيدته ، حيث تطرح أمامه أدلة الإثبات ثم تترك له الحرية في أن يبني اقتناعه على أي دليل من هذه الأدلة دون تقييده بدليل منها[349] ، وذلك ما لم يكن قد ألزمه المشرع الاجرائي بوسائل معينة أو خاصة في الإثبات[350] ، وهكذا يتميز نظام الإثبات الحر بالدور الفعال للقاضي حيال الدليل ، وهذا الدور يبدو من ناحيتين ، فمن ناحية أن القاضي حر في أن يستعين بكافة طرق الإثبات للبحث عن الحقيقة ،

---

[345] عمر محمد يونس ، الإجراءات الجنائية عبر الانترنت في القانون الأمريكي ، مرجع سابق ، ص 437.
[346] سعيد عبداللطيف حسن ، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت ، الطبعة الأولى ، دار النهضة العربية ، القاهرة 1999 ، ص186 ومابعدها .
[347] شيماء عبدالغني ، مرجع سابق ، ص 391.
[348] يطلق عليها البعض أيضاً ، نظام الأدلة الأدبية ، أو نظام الاقتناع الذاتي للقاضي ، أو نظام الإثبات المطلق أو المعنوي . (شعبان محمود محمد الهواري ، مرجع سابق ، ص7.
- عبدالخالق محمد أحمد الصلوي ، مرجع سابق ، ص319.
- أحمد فتحي سرور ، مرجع سابق ، ص345.
- موسى مسعود ارحومة ، حرية القاضي الجنائي في تكوين عقيدته ، مرجع سابق ، ص25.) .
[349] فوزية عبدالستار ، مرجع سابق ، ص511.
[350] رمزي رياض عوض ، مرجع سابق ، ص9.

والكشف عنها ، والمثال على ذلك أنه بإمكان القاضي الجنائي أن يأمر القائم بتشغيل النظام بتقديم البيانات المعلوماتية اللازمة لاختراق النظام والولوج إلى داخله كالإفصاح عن كلمات المرور السرية أوالشفرات[351] الخاصة بتشغيل البرامج ، ومن ناحية أخرى فإن القاضي الجنائي حر في وزن وتقدير كل دليل طرح أمامه.[352]

فمبدأ حرية القاضي الجنائي في الاقتناع تعني أن يقدر القاضي بكامل حريته قيمة الأدلة المعروضة عليه ، ما لم يقيده القانون بدليل معين ، واستخلاص النتيجة المنطقية لهذه الأدلة التي تتمثل في الحكم بالإدانة أو بالبراءة وفقاً لما يستقر في وجدانه الشخصي واقتناعه.[353]

ويستند هذا النظام على مبررات عديدة من أهمها ، أن الإثبات الجنائي يرد على وقائع مادية ونفسية تتعلق بالمجرم والجريمة ، ولايرد كما هو الأمر في المواد المدنية على تصرفات قانونية يتلاءم معها تحديد المشرع سلفاً لأدلة الإثبات.[354]

ويعتبر نظام الإثبات الحر من الأنظمة التي سادت معظم التشريعات الإجرائية المعاصرة كالقانون الفرنسي ، والقوانين الأخرى التي تأثرت به كالقانون الإيطالي ، والمصري ، والليبي حيث نجد صدى هذا النظام في التشريع الإجرائي الليبي في العديد من نصوصه في المادة (275) إ ج ليبي حيث نصت على أنه " يحكم القاضي في الدعوى حسب العقيدة التي تكونت لديه بكامل حريته....." .

كما نصت المادة (264)إ ج ليبي على أنه "للمحكمة أن تأمر ولو من تلقاء نفسها أثناء نظر الدعوى بتقديم أي دليل تراه لازماً لظهور الحقيقة" ، ويقابل ذلك نص المادة (291) من قانون الإجراءات الجنائية المصري.

أما في فرنسا فقد نصت المادة (427) من قانون الإجراءات الجنائية الفرنسي على أنه "فيما عدا الحالات التي ينص فيها القانون على خلاف ذلك يمكن إثبات الجرائم بكل وسائل الإثبات ويقضي القاضي بمقتضى اقتناعه الشخصي"[355] ، وبالتالي فإن مشكلة قبول الدليل الرقمي كدليل إثبات أمام القضاء الجنائي ليست مُلحة أو عاجلة في نظر الفقه الفرنسي ، فالأساس هو حرية القاضي في تقدير الدليل[356] ، حيث يدرس الفقه الفرنسي حجية قبول الدليل الرقمي تحت نطاق قبول الأدلة الناشئة عن الآلة أو الأدلة العلمية مثل الرادارات والأجهزة السينمائية ، وأجهزة

---

(351) التشفير : هو عملية تحويل البيانات إلى شكل غير قابل للقراءة إلى حروف أو أرقام أوعلامات تكون غير واضحة أو غير مفهومة . (www.hardiscussion/hr45894.html.) .

(352) سليمان أحمد فضل ، مرجع سابق ، ص363 -364.

(353) أشرف إبراهيم جمال إبراهيم قنديل ، حرية القاضي الجنائي في تكوين اقتناعه ، رسالة دكتوراه ، جامعة عين شمس ، كلية الحقوق ، 2009 ، ص40.

(354) محمد زكي أبوعامر ، الإثبات في المواد الجنائية ، مرجع سابق ، ص108.

(355) حسن عوض سالم الطراونه ، ضوابط السلطة التقديرية للقاضي الجنائي ، رسالة دكتوراه ، كلية الحقوق ، جامعة عين شمس ، 2005 ، ص9.

(356) هلالي عبداللاه أحمد ، حجية المخرجات الكمبيوترية في المواد الجنائية ، مرجع سابق ، ص42.

التصوير ، وأشرطة التسجيل وأجهزة التنصت[357] ، ولايختلف موقف القضاء الفرنسي من موقف الفقه في قبول الدليل الرقمي المتحصل عليه من الحاسوب ، فقد قضت محكمة النقض الفرنسية ، أن أشرطة التسجيل الممغنطة التي يكون لها قيمة دلائل الإثبات يمكن أن تكون صالحة للتقديم أمام القضاء الجنائي[358].

ومن خلال استقراء نصوص المواد السابق الإشارة إليها ، نلاحظ أن الدليل الرقمي شأنه في ذلك شأن الأدلة الجنائية الأخرى ، التي تم ذكرها على سبيل المثال في التشريعات الإجرائية مقبول مبدئياً في الإثبات الجنائي بصفة عامة ، والإثبات في مجال الجرائم الإلكترونية بصفة خاصة.

الفرع الثالث

نظام الإثبات المختلط

يقصد بنظام الإثبات المختلط ، هو النظام الذي يجمع بين النظامين نظام الإثبات المقيد أو القانوني ، ونظام الإثبات الحر ، وبالتالي يتبع نظاماً وسطاً بين الإثبات المقيد ، والإثبات الحر وطبقاً لهذا النظام يحدد المشرع الأدلة المقبولة في الإثبات الجنائي تاركاً للقاضي الجنائي الحرية في تقدير الأدلة القانونية[359] ، حيث يقوم هذا النظام على التوفيق بين قناعة القانون ، وقناعة القاضي بحيث لا يحكم القاضي بإدانة المتهم إذا لم تتوافر الأدلة القانونية ، كما أنه لا يحكم بالإدانة مع قيام الأدلة القانونية إذا لم تتحقق قناعته[360] ، ومن التشريعات التي أخذت بهذا النظام قانون الإجراءات الجنائية الياباني حيث حصر المشرع الياباني طرق الإثبات المقبولة في أقوال المتهم ، وأقوال الشهود ، والقرائن ، والخبرة ، أما بالنسبة للأدلة الرقمية المتحصل عليها من الحاسوب والانترنت ، فإن الفقه الياباني يرى أن السجلات الإلكترونية المغناطيسية تكون غير مرئية[361] ، ولذلك لايمكن أن تستخدم كدليل في المحكمة ، إلا إذا تم تحويلها إلى صورة مرئية ومقروءة عن طريق مخرجات الطابعة لمثل هذه السجلات وفي مثل هذه الحالة يتم قبول الأدلة الرقمية المتولده عن الحاسوب أو الانترنت ، سواء كانت هي الأصل ، أم كانت نسخة من هذا الأصل. [362]

أما في تشيلي فقد نص قانون الإجراءات الجنائية التشيلي في المادة (113) ، على أن الأفلام السينمائية ، والنظم الأخرى الخاصة بإنتاج الصورة ، والصوت ، وبصفة عامة أي وسائل أخرى

---

[357] صالح شنين ، الحماية الجنائية للتجارة الالكترونية دراسة مقارنة ، رسالة دكتوراه ، كلية الحقوق ، جامعة ابوبكر بلقايد تلمسان ، 2012-2013 ، ص 130.

[358] عفيفي كامل عفيفي ، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون ، منشأة المعارف ، الاسكندرية ، 2000 ، ص372.

[359] سليمان أحمد فضل ، مرجع سابق ، ص369.

[360] محمود محمود مصطفى ، الإثبات في المواد الجنائية ، مرجع سابق ، ص11.

[361] هلالي عبداللاه أحمد ، حجية المخرجات الكمبيوترية في المواد الجنائية ، مرجع سابق ، ص62.

[362] طارق فوزي الفقي ، مرجع سابق ، ص227.

قد تكون ملائمة ، ووثيقة الصلة ، وتفضي إلى استخلاص المصداقية يمكن أن تكون مقبولة كدليل إثبات[363] .

ويرى الفقه التشيلي أن الدليل الرقمي المتحصل عليه من الحاسوب أو الانترنت يمكن أن يكون مقبولاً أمام القضاء كدليل كتابي أو مستندي ، مثله مثل النظم الحديثة الأخرى لجمع وتسجيل المعلومات ، والهدف من ذلك هو توسيع مظلة الوسائل العلمية الحديثة في الإثبات لتغطي العناصر الإثباتية المتحصلة عليها من الجرائم الإلكترونية . [364]

---

[363] علي حسن الطوالبه ، مشروعية الدليل الالكتروني المستمد من التفتيش الجنائي دراسة مقارنة ، مركز الاعلام الامني ، 2009 ، بدون ترقيم صفحات ، منشور على الانترنت A www.policemc.gov.hlreeports/2011

[364] علي حسن محمد الطوالبة ، التفتيش الجنائي على نظم الحاسوب والانترنت ، مرجع سابق ، ص202-203.

المطلب الثاني

شروط قبول الدليل الرقمي أمام القضاء الجنائي

لقد تناولنا فيما سبق موقف الأنظمة الإجرائية من قبول الدليل الرقمي كدليل إثبات أمام القضاء الجنائي ، إلا أن هناك شروطاً أو ضوابط معينة تحكم الأدلة المتحصلة عليها عن طريق الوسائل الإلكترونية يخضع لها القاضي الجنائي خوفاً من عدم تعبيرها عن الحقيقة ، وذلك لأن إجراءات الحصول على هذا النوع من الأدلة غالباً ما تتعرض للأخطاء ، مما يتطلب وجوباً مجموعة من الشروط التي تمنحها المصداقية والثقة لقبولها أمام القضاء الجنائي من أجل الوصول إلى الحقيقة التي ينشدها سواء في الحكم الصادر بالإدانة أو بالبراءة ، ولا تختلف تلك الشروط عن الضوابط التي يلتزم بها القاضي الجنائي حيال أي دليل جنائي ، من حيث أنه لا يستطيع أن يؤسس حكمه إلا على دليل مشروع مستمد من أدلة طرحت بالجلسة مقتنع بها إلى حد الجزم واليقين ، علاوةً على ذلك تقيده بطرق الإثبات المقررة في القوانين الخاصة .

وبناء على ما تقدم سنقسم هذا المطلب إلى أربعة فروع : نخصص الفرع الأول لدراسة مشروعية الدليل الرقمي . ونكرس الفرع الثاني لدراسة مناقشة الدليل الرقمي . ونكرس الفرع الثالث لدراسة تقيد القاضي الجنائي بأدلة معينة في جريمة الزنا. ونفرد الفرع الرابع لدراسة تقيد القاضي الجنائي بطرق الإثبات الخاصة بالمواد غير الجنائية.

الفرع الأول

مشروعية الدليل الرقمي

إن كل الأدلة التي يتم الحصول عليها عن طريق انتهاك حق أساسي للمتهم تكون باطلة ، ولايمكن التمسك بها ، ومراعاتها في أي مرحلة من مراحل الإجراءات ، حيث أن من المستقر عليه هو استبعاد الدليل المتحصل عليه بطريقة غير مشروعة[365] .

وبمعنى آخر ، أن المقصود من مبدأ مشروعية الدليل الرقمي هو ضرورة اتفاق الإجراء مع القواعد القانونية ، والأنظمة الثابتة ، أي أن قاعدة مشروعية الدليل الرقمي لاتقتصر فقط على مجرد المطابقة مع القاعدة القانونية التي ينص عليها المشرع ، بل يجب أيضاً مراعاة قواعد النظام ، والآداب ، ومقتضيات العدالة.[366]

ولقد وضعت الاتفاقيات الدولية[367] ، والتشريعات الإجرائية المختلفة نصوصاً تتضمن ضوابط لشرعية الإجراءات الماسة بالحرية ، ومن ثم فإن مخالفة هذه النصوص في تحصيل

---

[365] راشد بن حمد البلوشي "الدليل في الجريمة المعلوماتية " مجلة الحقوق ، العدد الأول ، 2008 ، ص 34.

[366] أحمد ضياء الدين محمد خليل ، مرجع سابق ، ص272 -273.

[367] نصت المادة (1/8) من الاتفاقية الأوروبية لحقوق الإنسان الصادرة في روما 4 نوفمبر سنة 1950 على أنه "لكل إنسان حق احترام حياته الخاصة والعائلية ومسكنه ومراسلاته" .

(www.umn.edu/humantrts/arab/eunrcom.html.)

الدليل الجنائي يسفر إلى عدم مشروعية هذا الدليل الجنائي ، مما يستلزم أن تكون الأدلة الرقمية قد تم الحصول عليها بطريقة مشروعة حتى يمكن الحكم بالإدانة ، مما يتطلب منا بيان موقف الانظمة الاجرائية عن مشروعية الدليل الرقمي من خلال دراسة التشريعات ذات النظام اللاتيني والانجلوساكسوني ، والمختلط في الفقرات التالية :

أولاً . النظام اللاتيني :

في إطار مشروعية الدليل الرقمي ، نجد أن قانون الإجراءات الجنائية الفرنسي ، لم يتضمن أي نصوص تتعلق بمبدأ الأمانة أو النزاهة في البحث عن الحقيقة ، إلا أن الفقه والقضاء في فرنسا أخذ بالوسائل العلمية الحديثة لاستعمالها في البحث والتنقيب عن الجرائم التقليدية والجرائم الإلكترونية ، والمثال على هذه الأخيرة كأن يستخدم رجال الشرطة وسائل إلكترونية في أعمال التنصت على المحادثات الهاتفية ، بشرط أن يتم الحصول على الأدلة الجنائية ، ومن بينها الأدلة الرقمية بطريقة مشروعة.[368]

وكذلك نجد المشرع الليبي والمصري قد حرصا في قانون الإجراءات الجنائية على مشروعية الدليل الجنائي ، وبالتالي فإن أي دليل يتم الحصول عليه بطريقة غير مشروعة يتم إبطاله بما في ذلك الدليل الرقمي ، حيث نصت المادة (309) إ ج ليبي على أنه "إذا تقرر بطلان إجراء فإنه يتناول جميع الآثار التي تترتب عليه مباشرة ، وتلزم إعادته متى أمكن ذلك" ويقابل ذلك نص المادة (336) إ ج مصري.

ومن أمثلة الطرق الغير مشروعة التي يمكن أن تستخدم في الحصول على الأدلة الرقمية التدليس والغش والخداع[369] ، والإكراه المادي والمعنوي في مواجهة المتهم المعلوماتي لفك شفرة نظام من النظم المعلوماتية أو الوصول إلى ملفات البيانات المخزنة[370] ، واستخدام اجهزة التنصت الهاتفي والتنويم المغناطيسي[371] .

والسؤال الذي يطرح نفسه في هذا المقام هل يلزم مبدأ مشروعية الدليل الجنائي بصفة عامة ، والدليل الرقمي بصفة خاصة على دليل البراءة أيضاً ؟

للإجابة عن هذا التساؤل يوجد هناك اتجاهان :

الاتجاه الأول : يرى أنصار هذا الاتجاه أنه لا يشترط أن يكون دليل البراءة وليد إجراء مشروع ، وأساس هذا الرأي أن الأصل في الإنسان البراءة ، ولاحاجة للمحكمة في أن تثبت براءته ، وكل ما تحتاج إليه هو أن تشكك في إدانته.[372]

---

[368] هلالي عبداللاه أحمد ، حجية المخرجات الكمبيوترية في المواد الجنائية ، مرجع سابق ، ص 121-122.
[369] علي حسن محمد الطوالبة ، التفتيش الجنائي على نظم الحاسوب والانترنت ، مرجع سابق ، ص193.
[370] طارق فوزي الفقي ، مرجع سابق ، ص212.
[371] محمد حلمي محمد حسان ، مرجع سابق ، ص182.
[372] أحمد فتحي سرور ، مرجع سابق ، ص348.

الاتجاه الثاني : يرى مؤيدو هذا الاتجاه أن المشروعية ضرورية في كل دليل ، سواء كان بالإدانة أو بالبراءة ، وذلك تأسيساً على نص المادة (309) إ ج ليبي ، التي لا تفرق بين دليل الإدانة ودليل البراءة.[373]

ومن خلال الموازنة بين الاتجاهين نؤيد الاتجاه الأول ، وذلك استناداً لقاعدة افتراض براءة المتهم ، وبالتالي فإن أي دليل يساعد على تطبيق هذه القاعدة يجب قبوله دون النظر لأي اعتبار آخر.

ثانياً . النظام الانجلوساكسوني :

إن القاعدة الأساسية في القانون الانجليزي لا تلزم لقبول الدليل سوى تعلقه بالواقعة المراد إثباتها ، أياً كانت الطريقة التي تم الحصول عليه من خلالها ، أي حتى ولو تم ذلك بطريقة غير مشروعة.[374]

إلا أنه بعد ذلك ظهر اتجاه آخر في القضاء الانجليزي يخفف من صرامة وحدّة مبدأ قبول الدليل أياً كانت الوسيلة التي تم الحصول عليه ، غير أنه سرعان ما تم العودة إلى تكريس قاعدة الإطلاق في عدم استبعاد الدليل غير المشروع ، والمضي باتجاه نظرية الضبط الجرمي.[375]

وتأكيداً على ما جاء في ظل الاتجاه الذي خفف من صرامة وحدة مبدأ قبول الدليل نصت المادة (86) من قانون البوليس والإثبات الجنائي الصادر سنة 1984م على أنه "إن اعتراف المتهم يتم رفضه باعتباره دليلاً إذا لم تستطيع سلطة الإدعاء أن تثبت أنه لم يتم الحصول عليه بواسطة الضغط أو أنه كان نتيجة لسلوك معين يجعل هذا الاعتراف مشكوكاً فيه".

وكما هو مفهوم من نص هذه المادة أن المحكمة تستطيع استبعاد قبول اعتراف المتهم كدليل من قبل سلطة الإدعاء ، إذا أتضح لها أن ذلك الاعتراف قد تم باستخدام وسيلة ضغط ضد المتهم ، أو على إثر شيء قيل يكون من المحتمل في ظل الملابسات المعاصرة للاعتراف قد أثر على مصداقية الاعتراف[376] .

كما نصت المادة (78) من القانون السالف الذكر على أنه "إذا بدا للمحكمة أنه إذا أخذ في الاعتبار كل الظروف ، وتم فهم هذه الظروف التي أعطى فيها الدليل ، وأن تلقيه كان بسبب وقوع أضرار تتعلق بعدالة إجراءات الدعوى فإن المحكمة لا يمكن أن تقبله" ، إذ تمنح هذه المادة للمحكمة سلطة استبعاد الدليل الذي تريد النيابة العامة أن تقدمه.[377]

---

[373] رؤوف عبيد ، مرجع سابق ، ص740.

[374] أحمد عوض بلال ، قاعدة استبعاد الأدلة المتحصلة بطرق غير مشروعة في الإجراءات الجنائية (دراسة مقارنة)، الطبعة الثانية ، دار النهضة العربية ، القاهرة ، 2008 ، ص41.

[375] عماد عوض عدس ، التحريات كإجراء من إجراءات البحث عن الحقيقة ، دار النهضة العربية ، القاهرة ، 2007 ، ص395.

[376] راشد بن حمد البلوشي ، مرجع سابق ، ص37.
- أحمد عوض بلال ، المرجع السابق ، ص57.

[377] هلالي عبداللاه أحمد ، حجية المخرجات الكمبيوترية في المواد الجنائية ، مرجع سابق ، ص129.

ونلاحظ على نص هذه المادة أنها لم تضع أي ضوابط بشأن إعمال أحكام هذه المادة ، وكل ما بينته هو ألا يؤثر الدليل على نزاهة الإجراءات ، ولايوجد معيار محدد يوضح متى تكون الإجراءات غير عادلة أو غير نزيهة.

ولذلك أوجد بعض الفقهاء[378]، معايير محددة يمكن استلهامها من خلال تطبيق نص المادة (78) من قانون البوليس والإثبات الجنائي الانجليزي ، تتمثل في ثلاثة مبادئ : مبدأ حُسن النية ، ومبدأ الحماية ويدور حول فكرة حماية المتهمين ، ومبدأ المخالفة الجوهرية.[379]

أما القانون الأمريكي فقد خصص مبحثاً خاصاً وهو المبحث الخامس في المرشد الفيدرالي الأمريكي لتفتيش وضبط الحواسيب وصولاً إلى الدليل الرقمي يتعلق بعلاج انتهاكات الباب الثالث (قانون المراقبة وقانون التسجيل والتقصي) ، ويقصد به علاج بطلان الإجراءات الغير مشروعة في الحصول على الدليل الرقمي حيث نص في ذلك على انه يجب على رجال الضبط القضائي ، والمدعين العموميين سلوك مسلك أوامر الباب الثالث ، وقانون التسجيل والتقصي ، عند التخطيط للمراقبة الالكترونية ، إذ يمكن ان تسفر الانتهاكات عن غرامات وجزاءات مدنيه وجنائية ، وبطلان الدليل الذي تم الحصول عليه.[380]

ومع ذلك فإن القضاء الأمريكي تخبط كثيراً بخصوص استبعاد الأدلة المتحصلة بطريقة غير مشروعة ، إلا أنه حسم الامر في قضية شهيرة سنة 1914م (weeks.v.united states) والتي تتلخص وقائعها بأن المتهم في هذه القضية قد اتهم باستعمال البريد من أجل نقل تذاكر اليانصيب ، وطلب إلى محكمة الموضوع استرجاع أوراقه التي دفع بها بأنها ضبطت بالمخالفة للدستور ، ولكن محكمة الموضوع رفضت طلبه وأصدرت المحكمة الاتحادية العليا بإجماع أعضائها مبدأ عدم قبول الدليل المتحصل عليه بالمخالفة للتعديل الدستوري الرابع[381].

ثالثاً . النظام المختلط :

يستبعد الفقه الياباني الأدلة الجنائية التي يتم الحصول عليها بطريقة غير مشروعة سواء كانت أدلة تقليدية أو أدلة رقمية ، [382] غير أنه بالرغم من تبني المحكمة العليا في اليابان قاعدة استبعاد الدليل الذي تم الحصول عليه بطريقة غير مشروعة شريطة اتصاف عدم المشروعية بالخطير ، إلا أنه من الناحية العملية فإن التطبيقات القضائية لحالات استبعاد الأدلة الجنائية بما في ذلك الأدلة الرقمية قليلة الوقوع [383].

---

[378] عماد عوض عدس ، مرجع سابق ، ص 401-402.

[379] **مبدأ المخالفة الجوهرية** : يقصد به هو مايتم إعماله دون النظر إلى قصور الشرطة أو نتائج المخالفة فيكفي تحققه وقوع مخالفة جسيمه وجوهرية لاحكام القانون ويظهر إعمال هذا المبدأ بوضوح في مخالفة قواعد الاستجواب . (عماد عوض عدس ، نفس المرجع السابق ، ص403) .

[380] عمر محمد بن يونس ، الاجراءات الجنائية عبر الانترنت في القانون الامريكي ، مرجع سابق ، ص400.

[381] أحمد عوض بلال ، مرجع سابق ، ص 85-87.

[382] سليمان أحمد فضل ، مرجع سابق ، ص380.

[383] طارق فوزي فقي ، مرجع سابق ، ص213.

والجدير بالذكر أنه لا يجوز للقاضي الجنائي أن يعتمد على دليل باطل ومجرد من قيمته القانونية ويستمد منه قناعته الذاتية[384]، ويدخل في مدلول الدليل الباطل ذلك الدليل الذي لم يستوفِ الضوابط التي نص عليها القانون كي تكون له حجة أقناعيه للقاضي الجنائي ، فتكوين عقيد القاضي الجنائي يجب أن تكون مبنية على أدلة مستمدة من إجراء صحيح ومشروع ، أما إذا تكونت عقيدة القاضي على أدلة مستمدة من إجراءات غير مشروعة ، فإن ذلك يؤدي إلى بطلان الحكم تطبيقاً لقاعدة مابني على باطل فهو باطل.[385]

الفرع الثاني

مناقشة الدليل الرقمي

يقصد بشرط مناقشة الدليل الرقمي ، أن القاضي الجنائي لا يستطيع أن يبني اقتناعه إلا على العناصر ألإثباتيه التي طرحت في جلسات المحاكمة ، وخضعت لحرية مناقشة أطراف الدعوى.[386]

وقد نصت على قاعدة وجوب مناقشة الدليل الجنائي المادة (275) إ ج ليبي في قولها ".....ومع ذلك لا يجوز للقاضي الجنائي أن يبني حكمه على أي دليل لم يطرح أمامه في الجلسة"، وعلة هذه القاعدة هي مبدأ الشفوية والمواجهة في المحاكمة الجنائية ، وهو مبدأ أساسي في الإجراءات الجنائية ، فلا يجوز للقاضي أن يأخذ بدليل قد قدمه أحد الخصوم في الدعوى الجنائية ، إلا إذا قام بعرضه شفوياً في جلسة المحاكمة بحيث يعلم به جميع أطراف الدعوى فتمنح لهم مناقشة الدليل ، ومن خلال ذلك يستطيع القاضي أن يكون عقيدته بشأن قيمة هذا الدليل.[387]

وبالتالي إذا استند القاضي الجنائي في حكمه إلى دليل لم يطرح للمناقشة في الجلسة كان ذلك منه إخلالاً بحق الدفاع ، حتى ولو كان لهذا الدليل أصل في أوراق الدعوى.[388]
ولا يختلف الأمر بالنسبة للأدلة الرقمية بوصفها أدلة إثبات قائمة في أوراق الدعوى التي ينظرها القاضي ، فإنه يجب عليه مناقشتها أمام الخصوم.[389]

---

(384) محمود نجيب حسني ، مرجع سابق ، ص441.
- عبدالحكيم فوده ، البطلان في قانون الإجراءات الجنائية دراسة تحليلية على ضوء الفقه والقضاء والنقض ، دار المطبوعات الجامعية ، الإسكندرية ، 1996 ، ص 446 ومابعدها .
(385) سامح أحمد بلتاجي ، مرجع سابق ، ص442.
(386) المحكمة العليا ، نقض جنائي 1971/1/12 ، مجلة المحكمة العليا ، س3 ، عدد 7 ، ص153.
(387) محمود نجيب حسني ، المرجع السابق ، ص 439.
(388) فوزية عبدالستار ، مرجع سابق ، ص517.
(389) راشد بن حمد البلوشي ، مرجع سابق ، ص31.

وهذا يعني أن الأدلة الرقمية سواء كانت مطبوعة ، أم بيانات معروضة على شاشة الحاسب الآلي ، أو اتخذت شكل أشرطة ، أو أقراص ممغنطه ، أو مصغرات فيلميه ، كل هذه ستكون محلاً للمناقشة عند الأخذ بها كأدلة إثبات أمام القضاء.[390]

وعلى ذلك فإن كل دليل يتم الحصول عليه من خلال البيئة الالكترونية يجب أن يتم عرضه في جلسات المرافعة ليس من خلال ملف الدعوى ، أو التحقيق الابتدائي ، لكن بصفة مباشرة أمام القاضي ، وهذه الأحكام تنطبق على كافة الأدلة الرقمية ، المتحصلة من الحاسوب ، والانترنت ، إلى غير ذلك من وسائل تقنية المعلومات.

وتأكيداً على ما سبق أن القوانين ذات النظام اللاتيني قد نصت على وجوب مناقشة الدليل الجنائي حيث نصت المادة (275) إ ج ليبي على انه " يحكم القاضي في الدعوى حسب العقيدة التي تكونت لديه بكامل حريته ، ومع ذلك لا يجوز له أن يبني حكمه على أي دليل لم يطرح أمامه في الجلسة" ويقابل ذلك نص المادة (302) إ ج مصري.

أما في فرنسا فقد نصت المادة (427 فقرة 2) من قانون الإجراءات الجنائية الفرنسي على أنه" لا يجوز للقاضي أن يؤسس حكمه إلا على أدلة طُرحت عليه أثناء المحاكمة ، ونوقشت أمامه في مواجهة الأطراف"[391] .

ولا يختلف الأمر في القوانين ذات النظام الانجلوساكسوني ، حيث أن كل عناصر الإثبات لابد أن تكون معروضة للمناقشة بحضور أطراف الدعوى ، بينما يكون القاضي إلى حدٍ ما مُصغياً لكل ما يمكن أن يقال في الجلسة.[392]

فالأدلة التي يجوز الاستناد إليها وحدها،هي التي تكون قد طُرحت للمناقشة في الجلسة أمام الخصوم ، حتى يتمكن كل ذي مصلحة من مناقشتها والرد عليها ، ويترتب على مناقشة الأدلة الرقمية عدم جواز أن يحكم القاضي في الجرائم الالكترونية بناءً على معلوماته الشخصية أو أن يصدر حكماً بناءً على رأي الغير ، بالإضافة إلى ضرورة تأهيل القاضي من ناحية معرفته لتكنولوجيا المعلومات وتقنياتها وهذا ما سنبينه في الفقرات التالية :

أولاً . عدم جواز أن يحكم القاضي في الجرائم الإلكترونية بناءً على معلوماته الشخصية:

ويقصد بذلك عدم جواز استناد القاضي الجنائي إلى معلوماته الشخصية التي حصل عليها من خارج الجلسة ، ذلك بأن هذه المعلومات لم تعرض في الجلسة ، ولم يتم مناقشتها وتقييمها[393] ، وبالتالي فإن الاستناد عليها يخالف مبدأ الشفوية والمواجهة الذي يسود مرحلة

---

[390] علي حسن محمد الطوالبه ، التفتيش الجنائي على نظم الحاسوب والانترنت ، مرجع سابق ، ص197.
[391] عبدالخالق محمد أحمد الصلوي ، مرجع سابق ، ص363.
[392] هلالي عبداللاه أحمد ، حجية المخرجات الكمبيوترية في المواد الجنائية ، مرجع سابق ، ص106.
[393] محمود محمود مصطفى ، شرح قانون الاجراءات الجنائية ، مرجع سابق ، ص366.

المحاكمة ، علاوةً على ذلك فإن صفة القاضي بالنسبة لمعلوماته الشخصية تكون بمثابة الشاهد حيث أن هناك تناقض بين صفة القاضي والشاهد.[394]

وبما أن القاضي الجنائي يعتمد في حكمه على المعلومات التي حصل عليها ، وهو في مجلس القضاء أثناء نظر الدعوى ، غير أنه لا يعد من قبيل المعلومات الشخصية استناد القاضي في حكمه إلى المعلومات العامة ، التي يفترض كل شخص أن يكون ملماً بها[395] ، والمثال على المعلومات العامة سطوع القمر في الخامس عشر من الشهر العربي.[396]

ويرى بعض الفقهاء[397] ، أن شرط عدم جواز أن يستند القاضي في حكمه بناء على معلوماته الشخصية ، لم ينص عليه المشرع الليبي صراحةً ، إلا أنها مستقاة ضمناً من نص المادة (275) إ ج ليبي ، التي تحظر على القاضي الجنائي أن يؤسس حكمه على أي دليل لم يطرح أمامه بالجلسة.

ثانياً . عدم استناد القاضي في حكمه بناءً على رأي الغير:

ويقصد بذلك إحاطة القاضي الجنائي بالدليل بصورة كاملة قبل أن يخضع لعملية التقدير ، فإعطاء الرأي سلفاً بقيمة الدليل يتنافى مع أسس تكوين القناعة القضائية ، ذلك أن القاضي يتقيد في تكوين عقيدته ، ويستمد قناعته من التحقيق الذي يقوم به بنفسه في الدعوى ، ولايعول على رأي الغير.[398]

وتأكيداً على ذلك فقد نصت المادة (273) إ ج ليبي على أنه " لا تتقيد المحكمة بما هو مدون في التحقيق الابتدائي أو في محاضر جمع الاستدلالات إلا إذا وجد في القانون نص على خلاف ذلك" ، غير أن هذا لا يعني أن يطرح القاضي سائر الأدلة التي توصلت إليها سلطة التحقيق ، أو الاستدلال ، وإنما معناه أن لا يجعل منها أساساً لاقتناعه لأنها في الواقع قناعة غيره.[399]

---

[394] محمود نجيب حسني ، مرجع سابق ، ص439-440.

[395] محمد عيد الغريب ، حرية القاضي الجنائي في الاقتناع اليقيني وأثره في تسبيب الأحكام الجنائية ، دار النهضة العربية ، القاهرة ، 2008 ، ص 59-60.

[396] أحمد فتحي سرور ، مرجع سابق ، ص347.

[397] موسى مسعود ارحومة ، حرية القاضي الجنائي في تكوين عقيدته ، مرجع سابق ، ص114.

[398] عبدالخالق محمد أحمد الصلوي ، مرجع سابق ، ص 366-367.

[399] حسن عوض سالم الطراونه ، مرجع سابق ، ص89.

ثالثاً . ضرورة تأهيل القضاة لمعرفة تكنولوجيا المعلومات:

يتعين على القاضي الجنائي الإلمام بمعرفة الأساليب التقنية المستخدمة في ارتكاب الجرائم الإلكترونيه ، ووسائل الكشف عنها ، والأدلة المستخدمة في إثباتها ، وذلك لمواكبة المناقشة العلمية للأدلة الرقمية التي يتم عرضها عليه في جلسات المحاكمة.[400]

ونلاحظ فيما تقدم أن التشريعات المقارنة كالتشريع الإجرائي الفرنسي يشترط بناء قناعة القاضي على الأدلة التي طرحت ، ونوقشت في الجلسة على خلاف المشرع الليبي الذي لم يبين صراحةً وجوب مناقشة الدليل من قبل أطراف الدعوى ، واكتفى بالنص على طرح الدليل بالجلسة ، ولذا نهيب بالمشرع الليبي تعديل النص الوارد في نهاية المادة (275) إ ج ليبي ليصبح كالأتي "..... ،ومع ذلك لا يجوز له أن يبني حكمه إلا على الأدلة التي طرحت في الجلسة ، ونوقشت في مواجهة الخصوم أثناء المحاكمة."

الفرع الثالث

تقيد القاضي الجنائي بأدلة معينة في جريمة الزنا

حدد المشرع الليبي عدداً من الأدلة الجنائية في إثبات جريمة الزنا ، حيث تنص المادة (6) مكرر من القانون رقم (70) لسنة 1973م في شأن إقامة حد الزنا وتعديل بعض أحكام قانون العقوبات على انه "تثبت جريمة الزنا المنصوص عليها في هذا القانون ، باعتراف الجاني أو بشهادة أربعة شهود ، أو بأية وسيلة إثبات علمية"

وكما هو ملاحظ على هذا النص ، أن المشرع الليبي بيّن الأدلة التي على ضوئها تثبت جريمة الزنا على المتهم ، هي اعتراف الجاني ، أو شهادة أربعة شهود ، أو بأية وسيلة إثبات علمية أخرى ، وعندما نقف عند عبارة أي وسيلة إثبات علمية أخرى ، نجد أن المشرع الليبي قد استخدم مصطلحاً فضفاضاً يتسم بالطابع العمومي ، حيث يندرج تحت مسمى أي وسيلة إثبات علمية على سبيل المثال الحمض النووي (DNA) والأدلة الرقمية ، لأنها تعتبر من الوسائل العلمية الحديثة.

والجدير بالذكر أن المشرع المصري له موقف مختلف عن المشرع الليبي ، حيث حدد المشرع المصري الأدلة الجنائية في إثبات جريمة الزنا ، وذلك على سبيل الحصر لا المثال ، حيث نصت المادة (276) من قانون العقوبات المصري على أن الأدلة التي تكون لها حجية على المتهم بالزنا هي القبض عليه حين تلبسه بالفعل أو اعترافه أو وجود مكاتيب أو أوراق أخرى صادرة منه أو وجوده في منزل مسلم في محل مخصص للحريم[401].

---

[400] علي حسن محمد الطوالبه ، التفتيش الجنائي على نظم الحاسوب والانترنت ، مرجع سابق ، ص200.

[401] قانون العقوبات المصري طبقاً لأحدث التعديلات ، بالقانون رقم (95) لسنة 2003 ، القانون رقم (58) لسنة 1937 بإصدار قانون العقوبات.

(www.seoudi-Law.com/forums/showthread php? t=3233)

ولهذا لا يجوز للقاضي الجنائي ، أن يقبل لإثبات جريمة الزنا أدلة أخرى غير مقررة في نص المادة (276) من قانون العقوبات المصري ، حتى ولو كان دليلاً رقمياً ، إلا أن المفهوم من نص المادة (6) مكرر من قانون رقم (70) لسنة 1973 ، بشأن إقامة حد الزنا السابق الإشارة إليه ، أنه يقبل لإثبات جريمة الزنا أي دليل علمي سواء كان عبارة عن صورة فيديو أو رسالة مرسلة عن طريق الهاتف النقال ، أو عن طريق الانترنت ، ويعد مضمون هذه الرسالة ، أو صورة الفيديو دليل على وقوع جريمة الزنا.

الفرع الرابع

تقيد القاضي الجنائي بطرق الإثبات الخاصة بالمواد غير الجنائية

يعتبر هذا القيد مبدأ موجوداً في القضاء ، ويرجع أساسه إلى خضوع المسائل غير الجنائية لقانون واحد في إثباتها مهما تنوع القضاء المطروحة أمامه مثل تلك المسائل ، حتى لا يتخذ البعض القضاء الجنائي كوسيلة للتهرب من قوانين الإثبات[402] ، ويجد هذا القيد سنده في المادة (198) من قانون الإجراءات الجنائية الليبي حيث نصت على أنه "تتبع المحاكم الجنائية في المسائل غير الجنائية التي تفصل فيها تبعاً للدعوى الجنائية ، طرق الإثبات المقررة في القانون الخاص بتلك المسائل" ، ويقابلها المادة (225) إ ج مصري.

وعلى الرغم من عموم صياغة النص ، وإشارته إلى كل المسائل غير الجنائية ، إلا أنه يقتصر بصفة أساسية على المسائل المدنية التي يتوقف عليها الفصل في الدعوى الجنائية ، إذ هي تخضع لقواعد إثبات مختلفة عن قواعد الإثبات الجنائي[403] تطبيقاً لقاعدة أن قواعد الإثبات ترتبط بموضوع الدعوى لا بنوع المحكمة التي تفصل فيه[404].

غير أن تقييد القاضي الجنائي بوسائل الإثبات المقررة في القوانين غير الجنائية بالنسبة للمسائل الأولية مرتبط بشرطين[405] :

أ) أن تكون الواقعة المتعلقة بالقوانين غير الجنائية لازمة للفصل في الدعوى الجنائية.

ب) أن لا تكون الواقعة موضوع الإثبات هي نفسها الواقعة موضوع التجريم.

أو بمعنى آخر ، ألا تكون هذه المسألة هي ذاتها الفعل الإجرامي ، وإلا جاز إثباتها بكافة طرق الإثبات بما فيها الدليل الرقمي باعتباره مسألة جنائية.

---

[402] محمد زكي أبوعامر ، شرح الاجراءات الجنائية ، مرجع سابق ، ص892.

[403] محمود نجيب حسني ، مرجع سابق ، ص443.

[404] فوزية عبدالستار ، مرجع سابق ، ص518.

- جندي عبدالملك ، الموسوعة الجنائية ، الجزء الأول ، مرجع سابق ، ص112.

[405] مأمون محمد سلامه ، الإجراءات الجنائية في التشريع الليبي ، الطبعة الثانية ، الجزء الثاني ، منشورات مكتبة الجامعة ، الزاوية ، 2000 ، ص161.

ومتى وجد هذان الشرطان وجب على المحكمة أن تلجأ إلى وسائل الإثبات المقررة في القوانين الخاصة بالمواد غير الجنائية ، وهذه الوسائل لا تتعلق بالنظام العام ، وإنما تتعلق بمصلحة الخصوم ، وعلى صاحب المصلحة التمسك بضرورة اتخاذ وسائل الإثبات غير الجنائية.[406]

وتجدر الإشارة إلى أن إلزام القاضي الجنائي بقواعد الإثبات غير الجنائية يقتصر فقط على أحكام الإدانة دون البراءة ، إذ يجوز في حالة الحكم بالبراءة أن يستمد القاضي في تكوين عقيدته ، بعدم وجود العلاقة المدنية التي تفترضها الجريمة من أي دليل.[407]

ومع ظهور الحاسوب ، وشبكات المعلومات الدولية الانترنت ، والمحررات الإلكترونية ، وسائر المكونات المعنوية للحاسب الآلي التي تقع عليها جرائم السرقة ، والنصب ، وخيانة الأمانة ، وهي إما مسائل مستحدثة ، أو متغيرة المضمون بسبب ثورة الاتصالات والمعلومات عن بعد ، لذلك فإن إثبات هذه المسائل سيكون بالأدلة تتطابق مع طبيعتها ، والتي تجد مصدرها في قوانين غير جنائية كالقانون التجاري ، والقانون المدني ، وفي هذه الحالة على القاضي الجنائي أن يستثني الدليل الرقمي من استبعاد الدليل الجنائي عند إثبات المسائل الأولية.[408]

---

[406] إبراهيم الغماز ، الشهادة كدليل إثبات في المواد الجنائية ، عالم الكتب ، القاهرة ، 1980 ، ص659.

[407] ومثال ذلك : جريمة خيانة الأمانة التي تفترض وجود عقد أمانة بين طرفين ، وهي مسألة مدنية سابقة على وجود الجريمة المتمثلة في الاختلاس ، الذي تقوم به الجريمة ، ويخضع إثبات هذا العقد بقواعد الإثبات المدنية.(د. محمود نجيب حسني ، مرجع سابق ، ص443) .

[408] علي محمود علي حموده ، مرجع سابق ، بدون ترقيم صفحات.

المبحث الثاني

تقدير القضاء الجنائي للدليل الرقمي

نظراً للطبيعة العلمية للدليل الرقمي ، ومدى تأثيرها على عقيدة القاضي الجنائي وما تتسم به الجرائم الإلكترونية من خصائص تميزها عن غيرها من الجرائم التقليدية ، مما يتطلب أن يكون للقضاء دوراً هاماً في الوقاية من هذه الجرائم ، أو الفصل فيها ، حيث أن هذه الفئة من الجرائم تستلزم ضرورة اتخاذ تدابير وقتية وسريعة بما يضمن عدم طمس معالم الجريمة ، أو العبث بالأدلة ، أو تدميرها ، كما لايستطيع القاضي أن يؤسس حكمه إلا على دليل مستمد من أدلة مقتنع بها إلى حد الجزم واليقين.

وبناءً على ما تقدم سنقسم هذا المبحث إلى ثلاثة مطالب : نخصص المطلب الأول لدراسة الصعوبات التي تؤثر على الدليل الرقمي. ونكرس المطلب الثاني لبيان يقينية الدليل الرقمي . ونفرد المطلب الثالث لدراسة دور القضاء المستعجل في الجرائم الإلكترونية .

المطلب الاول

الصعوبات التي تؤثر على الدليل الرقمي

يعد الإثبات بالدليل الرقمي من الأدلة المتقدمة في مجال الإثبات الجنائي ، غير انه توجد العديد من الصعوبات التي يثيرها الإثبات بالدليل الرقمي ، ولعل أبرز هذه الصعوبات هي مشكلة المصلحة الأولى بالرعاية ، وصعوبة تعارض الإثبات بالدليل الرقمي مع حرية القاضي الجنائي في تكوين عقيدته. وأخيراً الطبيعة العلمية للدليل الرقمي ، وبناءً على ما تقدم سنقسم هذا المطلب إلى ثلاثة فروع : نخصص الفرع الاول لدراسة مشكلة المصلحة الأولى بالرعاية. ونكرس الفرع الثاني لدراسة صعوبات تعارض الإثبات بالدليل الرقمي مع حرية القاضي الجنائي في تكوين عقيدته. ونفرد الفرع الثالث لدراسة الطبيعة العلمية للدليل الرقمي.

الفرع الأول

المصلحة الأولى بالرعاية

يثير استخدام الوسائل العلمية الحديثة كالدليل الرقمي في الإثبات مشكلة في التعارض بين مصلحتين هما :

أولاً . مصلحة المجتمع في أن يتحقق الأمن والاستقرار ، وأن لا يفلت المجرم من العقاب وهي المصلحة التي تدعو إلى حماية المجتمع من الجريمة ، وتقتضي مصلحة التحقيق اتخاذ بعض الإجراءات الجنائية الضارة بالحرية في مواجهة المجتمع من الجريمة.

ثانياً . مصلحة المتهم في أن تُصان حريته وكرامته ، والتي يستمدها من مبدأ افتراض البراءة والتي لا يجوز المساس بها ، إلا في أضيق نطاق ، وضمن شروط معينة تتحقق معها

الضمانات[409] ، لحماية الإنسان من مظاهر التعسف التي يمكن أن يتعرض لها من قِبل الجهات المخولة لتطبيق القواعد الإجرائية.[410]

فإذا كان الدليل الرقمي يشكك في مشروعيته باعتباره طريقة للتدخل في الحياة الخاصة للإفراد فما هي المصلحة الأولى بالرعاية ؟ هل هي مصلحة المجتمع دون النظر إلى مصلحة الفرد ؟ أم أن مصلحة الفرد هي الأولى بالرعاية بغض النظر عن مصلحة المجتمع ؟

تضاربت الآراء حول هذا الأمر حيث أنقسم رأي الفقه في ذلك إلى ثلاثة اتجاهات نستعرضها على النحو الآتي :

الاتجاه الأول :

يرى أنصار هذا الاتجاه أن مصلحة المجتمع أولى بالرعاية من المصلحة الخاصة، وذلك أن استعمال الطرق العلمية الحديثة مثل الانترنت ، واستخدامه كدليل على وقوع جريمة نشر المطبوعات الفاضحة يستهدف المصلحة العامة ، حتى تتمكن الدولة من حماية النظام الاجتماعي ، لكي لاينهار هذا النظام بسبب احترام الحقوق ، والحريات ، فكل ما ينتج عنه العلم الحديث يجب أن يتخذ في تحقيق أمن واستقرار المجتمع ، وإذا تم التسليم بالقول بأن هناك تعدي على حريات الأفراد ، فإنه يعتبر ضئيلاً للغاية.[411]

الاتجاه الثاني :

يرى مؤيدو هذا الاتجاه أنه يجب تغلب مصلحة المتهم ، التي تحميها الشرعية الإجرائية وذلك حمايةً لحرمة الحياة الخاصة للأفراد من كل ما يُعدّ انتهاكاً له ، أو تهديداً لسلامته[412].

ويستند هذا الرأي إلى المواثيق والمعاهدات الدولية التي تقرر صون الحريات الفردية ، والتي بموجبها تلتزم الدول الموقعة على هذه المعاهدات بتضمين هذه المبادئ في قوانينها ، ومن ذلك على سبيل المثال المادة (5) من الميثاق العربي لحقوق الإنسان[413] الصادر سنة 1997 ، والتي تنص على أنه "لكل فرد الحق في الحياة ، وفي الحرية ، وفي سلامة شخصه ، ويحمي القانون هذه الحقوق" .

---

(409) حسن المرصفاوي ،"ضمانات المتهم في التحقيق الإبتدائي"، مجلة الأمن العام ، العدد التاسع عشر ، 1962، ص63.

(410) برهامي ابوبكر عزمي ، مرجع سابق ، ص501.

(411) محمد محمد الألفي ، مدى مشروعية الدليل المستمد من الانترنت ، بدون ترقيم صفحات ، بحث منشور على الانترنت .
Http//www.Artitration mailgroup/posts1953794972.

(412) برهامي أبوبكر عزمي ، المرجع السابق ، ص500.

(413) الميثاق العربي لحقوق الإنسان ، أعتمد ونشر بموجب قرار مجلس جامعة الدول العربية رقم (5427) المؤرخ في 15/سبتمبر/1997 . راجع الموقع على شبكة الانترنت .
Http//heiunige.ch/humanrts/arab/a003-2.

الاتجاه الثالث :

يجمع أنصار هذا الاتجاه بين حق المجتمع ، وحق المتهم عند مباشرة الإجراءات الجنائية فلا تغلب أي من المصلحتين على الأخرى ، بل يجب التوفيق بينهما دون الأخذ بإحداهما دون الأخرى[414] ، بحيث يتم الاعتماد على قرينة البراءة في تحديد الإطار القانوني الذي يتم بداخله تنظيم ممارسة المتهم لحريته الشخصية في ضوء ما تدل عليه القرينة الموضوعية الدالة على اقتراف الجريمة ، فالقانون يعمل على تحقيق التوازن بين مصلحة المجتمع ، ومصلحة المتهم في الدفاع عن نفسه ، ولا تعني افتراض براءة المتهم التضحية بالمصلحة العامة في إظهار الحقيقة.[415]

ومن خلال الموازنة بين الاتجاهات الثلاثة ، نؤيد الاتجاه الثالث الذي يوازن بين مصلحة الفرد ومصلحة المجتمع مع اشتراط مشروعية الوسيلة المستخدمة التي تمس الحرية الفردية ، ففي مثل هذه الحالة لن يتحقق الضرر بل تتحقق مصلحة الفرد ومصلحة المجتمع ، وحتى في حال ثبوت التهمة بالدليل المتحصل من الوسائل العلمية ، كالدليل الرقمي مثلاً ، فإننا نكون قد وصلنا إلى الحقيقة التي هي هدف العدالة.

الفرع الثاني

صعوبات تعارض الإثبات بالدليل الرقمي مع حرية القاضي الجنائي في تكوين عقيدته

يوجد العديد من الصعوبات التي تلحق الإثبات بالدليل الرقمي ومن هذه الصعوبات ما يلي:

أولاً . عدم رؤية الدليل الرقمي :

يقصد بذلك أن الدليل الرقمي عبارة عن نبضات إلكترونية غير مرئية ، تنساب عبر أجزاء الحاسب الآلي ، والشبكة ، كما تنساب الكهرباء عبر الأسلاك فهي غير مرئية[416] ، لا تفصح عن شخصية معينة عادةً مسجلة إلكترونياً بكثافة بالغة ، وبطريقة مرمزة غالباً على دعائم ، أو وسائط للتخزين ضوئية ، أو ممغنطة لا يستطيع الإنسان قراءتها ، وإن كانت قابلة للقراءة من قبل الآلة نفسها.[417]

وهذا ما يبرز وجود صعوبة في جمع الاستدلالات ، والأدلة في الجرائم الإلكترونية حتى يمكن تحقيق عناصرها والتصرف فيها ، لكونها تعتمد على نبضات إلكترونية غير مرئية ، لايمكن قراءتها إلا بواسطة جهاز الحاسوب ، والبيانات التي يمكن استعمالها كوسيلة ضد الفاعل يمكن العبث بها أو محوها بالكامل في لحظة زمنية قصيرة ، ولهذا يمكن القول أن المصادفة لها

---

(414) فيصل مساعد العنزي ، أثر الإثبات بوسائل التقنية الحديثة على حقوق الإنسان ، رسالة ماجستير ، كلية الدراسات العليا ، قسم العدالة الجنائية ، جامعة نايف العربية للعلوم الأمنية ، 2007 ، ص 2.

(415) محمد زكي أبوعامر ، الإجراءات الجنائية ، مرجع سابق ، ص32 ومابعدها .

(416) خيرت علي محرز ، مرجع سابق ، ص36.

(417) هشام محمد فريد رستم ، "الجرائم المعلوماتية أصول التحقيق الجنائي الفني وآلية التدريب التخصصي للمحققين "، مجلة الأمن والقانون ، العدد الثاني ، 1999 ، ص83.

دور كبير في اكتشافها أكثر مما هو متوقع من أساليب المراقبة ، أو التفتيش على الحواسيب الآلية.[418]

ثانياً . صعوبة الأصالة في الدليل الرقمي :

إن التحقق من أصالة ، ومصدر الدليل الرقمي تعتبر ذات أهمية كدليل يمكن تقديمه لأجهزة العدالة الجنائية ، وهذا لا يتم إلا بعد تحديد خصائصه ، وإعادة تجميعه من المكونات المادية للحاسوب ، وعمل نسخة أصلية منه للتأكد من عدم وجود معلومات مفقودة أثناء عملية استخلاص الدليل ، كما يمكن جمع الآثار المعلوماتية الرقمية التي قد تكون تغيرت خلال الشبكة المعلوماتية الانترنت ، والتأكد من أن الدليل لم يتم العبث به ، أو تعديله من خلال استخدام خوارزميات[419] محدده ، ومن خلال هذه الإجراءات يمكن تحريز الدليل الرقمي لإثبات أنه أصيل وموثوق به.[420]

ثالثاً . ضخامة نفقات الحصول على الدليل :

يشكل الكم الهائل للبيانات التي يجرى في الأنظمة المعلوماتية تداولها ، أحد مصادر الصعوبات التي تعيق أجهزة العدالة الجنائية ، مما يتطلب من هذه الأجهزة الاستعانة بالخبراء للتعامل مع الجرائم التي تقع في مجال تكنولوجيا المعلومات[421] ، ولذلك فإن هؤلاء الخبراء يؤدون مهاماً لايستهان بها جراء نقص معرفة رجال القانون للجوانب التقنية الفنية في الجرائم الإلكترونية ، غير أن هؤلاء الخبراء عندما يقومون بأداء مهام فإنهم يحتاجون إلى نفقات في سبيل الحصول على الدليل الرقمي ، مما يؤدي إلى عبء ثقيل على أجهزة العدالة الجنائية.

لذلك يرى جانب من الفقه الجنائي[422] ، أن متطلبات العدالة الجنائية تلزم الأجهزة الحكومية أن تتحمل كامل مسئولياتها تجاه اكتشاف الجرائم ، وضبط الجناة ، ومقاضاتهم ، وهذا يقتضي توفير الإمكانيات التقنية اللازمة ، للاستعانة بها في تحقيق الجرائم الإلكترونية ، ويتعين عدم التذرع بالميزانيات المالية ، كسبب يحول دون قيام الدولة بواجباتها نحو تحقيق العدالة الجنائية.

---

[418] سرحان حسن المعيني ، "التحقيق في جرائم تقنية المعلومات "، مجلة الفكر الشرطي ، المجلد العشرون ، العدد الرابع ، 2011 ، ص35.

[419] الخوارزميات : هي عبارة عن مجموعة من الخطوات الرياضية ، والمنطقية ، والمتسلسلة لحل مشكلة ما . (www.dbaasco.com)

[420] ناصر بن محمد البقمى ، "أهمية الادلة الرقمية في الإثبات الجنائي دراسة وفق الانظمة السعودية "، مجلة الفكر الشرطي ، المجلد الحادي والعشرون ، العدد الأول ، 2012 ، ص 33.

[421] هشام محمد فريد رستم ، مرجع سابق ، ص87.

[422] عبدالفتاح بيومي حجازي ، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت ، مرجع سابق ، ص 37.

رابعاً . عدم إلمام رجال العدالة الجنائية بالمعرفة التقنية :

يتعين على أجهزة العدالة الجنائية ، أن تعتمد في مواجهتها للجرائم الإلكترونية على أدلة تقنية جديدة تفيد في مجال الإثبات الجنائي[423] ، وهو ما يفرض على الدولة أن تسعى إلى تدريب ، وتأهيل القائمين على جمع الاستدلالات ، والتحقيق الابتدائي ، والحكم على الجرائم الإلكترونية سواء فيما يتعلق بالطرق الفنية المستعملة في اقتراف الجريمة ، وكذلك فيما يتعلق بوسائل الكشف عنها ، والأدلة المستخدمة في مجال إثباتها وكيفية معاينتها ، والتحفظ عليها.[424]

وقد أنشأت المنظمة الدولية للشرطة الجنائية "الأنتربول"[425] ، وتهدف هذه المنظمة إلى تعزيز وتشجيع التعاون الدولي الأمني ، أي مساعدة الأجهزة الأمنية في الدول الأعضاء على التعاون فيما بينها في مجال مواجهة الجريمة بأنواعها المختلفة ، وبصفة خاصة الجرائم ذات الطابع عبر الوطني ، كالجرائم الإلكترونية ، كما تهدف أيضاً إلى تجميع كل المعلومات المتعلقة بالجريمة والمجرمين[426] .

وتم إنشاء جهاز آخر يسمى (الاورجست) ، وهو جهاز يوجد على المستوى الأوروبي ، ويساعد على التعاون القضائي ، والبوليسي في مكافحة كافة أنواع الجرائم الخطيرة ، ومن أهم أنشطته تحسين التنسيق ، والتعاون بين السلطات القضائية المختصة لدول الأطراف ، وإجراء التحقيقات ، والملاحقات المتبعة من قبل السلطات القضائية الوطنية ، والتبليغ عن الجرائم إلى السلطات المختصة للدول الأطراف.[427]

كما أنشأ المجلس الأوروبي في لوكسمبورج سنة 1991م شرطة أوروبية لتكون همزة وصل بين أجهزة الشرطة الوطنية في الدول الأطراف ، ولملاحقة الجناة في الجرائم العابرة للحدود ومنها بطبيعة الحال الجرائم الإلكترونية .[428]

ومن الأمثلة على دور الانتربول في ما يتعلق بالجرائم الإلكترونية ، ما حدث في الجمهورية اللبنانية ، عندما تم توقيف أحد الطلبة الجامعيين من قبل القضاء اللبناني بتهمة إرسال صور

---

[423] "نظره حول المشكلات القانونية والعملية لمواجهة الجريمة المعلوماتية" ، مجلة كلية الدراسات العليا ، العدد الحادي والعشرون ، 2009 ، ص17.

[424] موسى مسعود ارحومة ، الاشكاليات الإجرائية التي تثيرها الجرائم المعلوماتية عبر الوطنية ، مرجع سابق ، ص5.

[425] تبلورت فكرة إنشاء المنظمة الدولية للشرطة الجنائية "الانتربول" منذ مطلع القرن العشرين ، وبالتحديد سنة 1914م ، بمناسبة اجتماع الجمعية الدولية للقانون الجنائي في مدينة (موناكو) الفرنسية ، حيث ناقش هذا الاجتماع العديد من الموضوعات ذات الصلة بالتعاون الأمني بين الدول ، كتبادل المعلومات ، وتوثيقها ، وملاحقة المجرمين ، وتعقبهم ، وإلقاء القبض عليهم ، وتسليم المجرمين ، وقد تم بالفعل إنشاء هذه المنظمة تحت مسمى "اللجنة الدولية للشرطة الجنائية" سنة 1923 وفي سنة 1956م أتخذت هذه اللجنة مسماها الحالي " المنظمة الدولية للشرطة الجنائية" ، حيث أصدرت الجمعية العامة للأمم المتحدة في دورتها الخامسة والعشرين ، والتي عقدت في العاصمة النمساوية "فيينا" قراراً خاصاً بإعتماد النظام الأساسي لهذه المنظمة ، التي يقع مقرها في مدينة "ليون" بفرنسا ، وقد وصل عدد أعضائها إلى (186) دولة. (ضياء عبدالله عبود الجابر وآخرون ، المنظمة الدولية للشرطة الجنائية ، بدون ترقيم صفحات ، بحث منشور على الانترنت .

army.tech Net/forum/index.php?threads/97.

- محمد محمد عنب ، استخدام التكنولوجيا الحديثة في الاثبات الجنائي ، مطبعة السلام ، الاسماعيلية ، 2007 ، ص316-317) .

[426] عادل يحيى ، مرجع سابق ، ص 102-103.

[427] عفيفي كامل عفيفي ، مرجع سابق ، ص485.

[428] جميل عبدالباقي الصغير ، الجوانب الإجرائية للجرائم المتعلقة بالانترنت ، دار الفكر العربي ، القاهرة ، 2001 ، ص79.

إباحية لقاصرة دون العشر أعوام من موقعه على شبكة الانترنت ، وذلك إثر تلقي النيابة العامة اللبنانية برقية من الأنتربول في ألمانيا بهذا الخصوص.[429]

وإلى جانب جهاز الانتربول ، والاورجست ، لقد تم إنشاء فضاء جماعي من غير حدود سُمّي "بشنجن" وذلك من خلال التوقيع على معاهدة شنجن في 1985/6/14م ، وعلى اتفاقية تلك المعاهدة في 1990/6/19م.

وقد استحدثت هذه الاتفاقية وسيلتين جديدتين لتعزيز التعاون البوليسي الأوروبي ، لمواجهة التحديات الأمنية التي تفرضها الظروف الجديدة ، ومنها الجرائم الإلكترونيه ، وتتمثل هاتان الوسيلتان في مراقبة المشتبه فيهم عبر الحدود ، وملاحقة المجرمين.[430]

أما على الصعيد الداخلي لكل دولة فقد أنشأت الولايات المتحدة الأمريكية نقطة مراقبة على الشبكات الانترنت تحت مُسمّى "شرطة الانترنت" لتلقي شكاوي مستخدمي الانترنت ، وملاحقة الجناة ، والقراصنة "الهاكرز" ، والبحث عن الأدلة ضدهم ، وتقديمهم للقضاء.[431]

وكذلك فإن بريطانيا قد خصصت وحدة تجمع نخبة من رجال الشرطة المتخصصين في البحث والتنقيب عن الجرائم الإلكترونيه ، كالجرائم الجنسية ، وخاصةً تلك الواقعة على الأحداث وتضم هذه الوحدة ثمانون مفتشاً ، وتتلخص مهام هذه الوحدة في مواجهة هذا النوع الجديد من الإجرام ، والتي بدأت أعمالها سنة 2001م في متابعة مرتكبي الجرائم الجنسية عبر الانترنت وخصوصاً تلك الواقعة على الأحداث ، والمجرمين الذين يقومون بنشر الفيروسات.[432]

والجدير بالذكر أن هناك دولاً عربية أنشأت أقساماً ، أو إدارات تتعلق بمكافحة الجرائم الإلكترونيه كما هو الحال في السعودية ، والإمارات العربية المتحدة ، وتونس والأردن ، والمغرب ، ومصر وليبيا ، ففي ليبيا قد أنشأ جهاز لمكافحة جرائم تقنية المعلومات تابع للإدارة العامة للأدلة والبحث الجنائي ، وذلك بموجب قرار أمين (وزير) اللجنة الشعبية العامة رقم (63) لسنة 2005 بشأن تطبيق حكم في القرار رقم (131) لسنة 2004 بشأن التنظيم الداخلي للجهاز الإداري للجنة الشعبية العامة للأمن العام.[433]

---

(1) Http//www.star times.com/f.aspx?t=31163480

(430) نبيلة هبه مولاي علي هروال ، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات دراسة مقارنة ، رسالة ماجستير ، كلية الحقوق ، جامعة الاسكندرية ، 2005 – 2006 ، ص52.

(431) جميل عبدالباقي صغير ، مرجع سابق ، ص77.

(432) نبيلة هبه مولاي علي هروال ، المرجع السابق ، ص 36.

(433) موسى مسعود ارحومة ، السياسة الجنائية في مواجهة جرائم الانترنت ، مرجع سابق ، ص108.

الفرع الثالث

الطبيعة العلمية للدليل الرقمي

نظراً للطبيعة الخاصة للدليل الرقمي ، وما يسفر عن مسرح الجريمة وفقاً لظروف كل قضية ووسيلة ارتكابها من آثار تعتمد في استخراجها على التقنيات العلمية الحديثة ، والتي لا يمكن تحديدها على سبيل الحصر ، بل تتكاثر مع التقدم العلمي ، ومع التطور الحديث للحياة في مجال تقنية المعلومات التي تخدم البشرية ، وتستعمل أيضاً كأدلة علمية تستخدم في مجال الكشف عن الجريمة وعن المتهم.

ومن هذه الاكتشافات ما يكون قد استقر علمياً بحيث أصبح لا يقبل الجدل في حقيقته ، ومنها ما يكون التعارض فيه واضحاً بحيث لم يستقر على قاعدة علمية يقينيه ، ومن هنا كان الأخذ بالدليل العلمي يواجه صعوبة في يقينيتة على عقيدة القاضي الجنائي.

وبناءً على ما تقدم سنبين دور الخبير في الدعوى الجنائية ، وتوضيح تقدير القضاء للدليل العلمي وذلك على النحو التالي:

أولاً . دور الخبير في الدعوى الجنائية :

يقوم الخبير بدور هام في الدعوى الجنائية فيما يتعلق بالمسائل ذات الطبيعة الفنية البحتة دون سائر المسائل الأخرى التي لا تتطلب توافر قدر من العلم والخبرة في كشف غموضها ، فالخبرة وسيلة إثبات تهدف إلى كشف بعض الأدلة ، أو تحديد مدلولها بالاستعانة بالمعلومات العلمية ، وهي تفيد في إثبات وقوع الجريمة ، وفي نسبتها إلى المتهم ، أو في تحديد ملامح شخصيته الإجرامية[434] ، فالمسائل ذات الطبيعة الفنية البحتة يتطلب كشفها مهارات ، ومعارف لا تتوافر لدى القاضي ، الأمر الذي يتطلب الاستعانة بالخبراء الذين يكون لهم الدور الهام في كشف غموض الجريمة ، وتقديم الدليل الفني الذي يقدم ضمن أدلة الإثبات ، أو النفي ، ومن ثم يخضع لتقدير القاضي الذي له أن يقتنع بأي من الأدلة المقدمة في الدعوى[435] .

وذلك لأن الوسائل العلمية قد تعرض حياة الإنسان للخطر من حيث التدخل في حياته الخاصة [436]كما أن نظام استخدام الدليل العلمي يجعل من الخبير هو الذي قد أنشأ الحكم ، والقاضي هو الكاشف عنه ، وبالتالي لا يملك القاضي إلا أن يأخذ بما جاء في تقرير الخبير وصبه في قالب قضائي.[437]

---

[434] أحمد فتحي سرور ، مرجع سابق ، ص588.

[435] طه احمد طه متولي ، الدليل العلمي وأثره في الإثبات الجنائي ، رسالة دكتوراه ، كلية الحقوق ، جامعة طنطا ، 2007 ، ص102 ومابعدها .

[436] محمود نجيب حسني ، مرجع سابق ، ص422.

[437] أحمد الصادق الجهاني ، مرجع سابق ، ص3.

ثانياً . تقدير القضاء للدليل العلمي :

يخضع الدليل العلمي كما سبق لنا القول إلى تقدير القاضي ، ذلك لأن الإثبات ليس غاية للقاضي ، ولكنه وسيلة للحكم في الدعوى حيث يتولى القاضي بحث هذه الأدلة لكي يخرج منها الصالح للحكم في الدعوى ، ويطرح مادون ذلك[438] ، وفي هذا الخصوص ينبغي أن نفرق بين فرضين:

أ) القيمة العلمية القاطعة للدليل .

ب) الظروف والملابسات التي وجد فيها الدليل.

فتقدير القاضي لا يتناول الفرض الأول ، وذلك لأن قيمة الدليل تقوم على أسس علمية دقيقة وبالتالي ليس للقاضي حرية في مناقشة الحقائق العلمية القاطعة ذلك أنه لايعني أن يصدر القاضي حكم بالإدانة أو البراءة بمجرد توافر الدليل العلمي دون النظر إلى الظروف ، والملابسات التي تحيط بالدليل ، فالدليل العلمي آلية غير مُعدّه لتقرير تكوين عقيدة القاضي فيما يتعلق بمسألة غير واضحة.[439]

---

[438] طه أحمد طه متولي ، مرجع سابق ، ص 262-263.

[439] هلالي عبداللاه أحمد ، حجية المخرجات الكمبيوترية في المواد الجنائية ، مرجع سابق ، ص 46-47.

المطلب الثاني

يقينية الدليل الرقمي

إذا كان الهدف من الدعوى الجنائية هو الوصول إلى كشف الحقيقة فإنه لا يمكن إظهار هذه الحقيقة إلا عن طريق الاقتناع اليقيني بصحة ما ينتهي إليه الحكم القاضي بالإدانة[440] ، فاليقين هو تلك الحالة الذهنية أو العقلانية التي تؤكد وجود الحقيقة ، ولا يتوصل إلى هذه الصورة إلا عن طريق الاستنتاج حتى يصل الإدراك إلى القاضي من خلال وقائع الدعوى المعروضة أمامه[441] ، فالأحكام الجنائية لا تبنى على الظن والاحتمال ، وإنما تبنى على الجزم واليقين.[442]

وبمعنى آخر فإن اليقين هو أساس الحقيقة القضائية ، وعلاوة على ذلك فإن هذا اليقين هو الذي يمنح الثقة والطمأنينة في عدالة حكم القضاء.[443]

وبناءً على ما تقدم سنتناول في هذا المطلب المراحل التي يصل بها القاضي إلى اليقين وذلك من خلال الفرع الأول . أما الفرع الثاني سنخصصه لبيان موقف الأنظمة الإجرائية المختلفة من يقينية الدليل الرقمي.

الفرع الأول

المراحل التي يصل بها القاضي إلى اليقين

أولاً . مرحلة خلو ذهن القاضي من الواقعة :

ويقصد بذلك كما سبق لنا ، هو أن لا يكون لدى القاضي معلومات مسبقه عن الدعوى المطلوب منه الفصل فيها ، فالقاضي لا يحكم بناءً على معلوماته الشخصية ، أو بناءً على رأي الغير ، أو ما قد يكون شاهده بنفسه في غير مجلس القضاء.

ثانياً . مرحلة الشك :

القاعدة العامة في الدعوى الجنائية ، هي أن الأصل في الإنسان بريء حتى تثبت إدانته ، مما يلزم أن يؤسس القاضي حكمه على اليقين الذي ينفي الأصل وهو البراءة ، فالأحكام تبنى على اليقين لا على الشك والتخمين ، وترتيباً على ذلك فإن الشك دائماً يفسر لصالح المتهم ذلك أن الشك لا يصلح لنفي أصل البراءة الذي يجب أن يبنى على دليل يقيني[444] . فاليقين وفقاً لهذا المفهوم يقوم على عنصرين هما :-

---

[440] محمد عيد الغريب ، مرجع سابق ، ص129.

[441] إيمان محمد علي الجابري ، يقين القاضي الجنائي ، رسالة دكتوراه ، كلية الحقوق ، جامعة الاسكندرية ، 2002 ، ص101.

[442] مأمون محمد سلامه ، الإجراءات الجنائية في التشريع المصري ، ج2 ، مرجع سابق ، ص154.

[443] أحمد فتحي سرور ، مرجع سابق ، ص344.

[444] مأمون محمد سلامه ، الإجراءات الجنائية في التشريع الليبي ، الجزء الثاني ، مرجع سابق ، ص157.

أ) العنصر النفسي الوجداني أو الضميري : ويقصد به ارتياح القاضي واطمئنان نفسه إلى إدانة المتهم على أساس الجزم واليقين[445] .

ب) العنصر الذهني أو العقلي أو المنطقي : ويقصد به أن يؤسس القاضي اطمئنان نفسه ، وارتياح ضميره في إدانة المتهم على أدلة تم استنباطها وفقاً لمقتضيات العقل والمنطق[446] ، وذلك من خلال مناقشتها في جلسات المحاكمة من قبل أطراف الدعوى[447] ، بحيث لا يكون عمل القاضي ابتداعاً للوقائع وانتزاعاً من الخيال.[448]

ثالثاً . مرحلة المعرفة العلمية :

إن وقوع الجريمة الإلكترونية ، ونسبتها إلى المتهم المعلوماتي يتطلب نوعاً جديداً من المعرفة لدى القاضي الجنائي ، وهي المعرفة العلمية المعروفة بتكنولوجيا المعلومات لاسيما وأن القاضي الجنائي يلعب دوراً ايجابياً في الإثبات ، وهو البحث عن الحقيقة ، وقد يؤدي الجهل في بعض الأحيان إلى التشكيك في قيمة الدليل الرقمي ، ومن ثم يقضي بالبراءة ذلك أن الشك يستفيد منه المتهم المعلوماتي في مرحلة المحاكمة ، مما يؤدي إلى إفلات المجرمين من العقوبة .

وهذا الأمر يقتضي أن يقترب الدليل نحو الحقيقة الواقعية قدر المستطاع ، وأن يبتعد عن الشك والتخمين ، مما يترتب على ذلك أن كافة الأدلة الرقمية سواء كانت مخرجات ورقية ، أو إلكترونية ، كالاقراص المغناطيسية ، أو مصغرات فيلمية ، تخضع لتقدير القاضي الجنائي ، ويجب أن يستنتج منها الحقيقة بما يتفق مع يقينه دونما شك أو احتمال .

الفرع الثاني

موقف الأنظمة الإجرائية من يقينية الدليل الرقمي

تختلف الأنظمة الإجرائية من حيث موقفها من يقينية الدليل الرقمي بحسب كل تشريع ، وذلك ما سنبينه على النحو التالي :

أولاً . النظام الانجلوساكسوني :

نصت القواعد الفيدرالية للإثبات في الولايات المتحدة الأمريكية على أن الشرط الأساسي للتوثيق أو التحقق من صحة وصدق الدليل كشرط مسبق لقبوله ، هو أن يفي بأمارة أو بيّنه كافية لأن تدعم اكتشاف أو الوصول إلى الأمور التي تتصل بالموضوع بما يؤيد الإدعاءات أو المطالب المدعى بها.[449]

---

[445] محمد عيد الغريب ، مرجع سابق ، ص130.

[446] أحمد فتحي سرور ، مرجع سابق ، ص348.

[447] السيد محمد حسين الشريف ، النظرية العامة للإثبات الجنائي دراسة مقارنة ، رسالة دكتوراه ، كلية الحقوق ، جامعة القاهرة ، 2002 ص362.

- صنابر نصر غلاب ، ضوابط السلطة التقديرية للقاضي الجنائي دراسة مقارنة ، رسالة دكتوراه ، كلية الحقوق ،جامعة عين شمس ، 2011 ، ص 147-148.

[448] المحكمة العليا ، نقض جنائي ، 1974/3/5م ، مجلة المحكمة العليا ، س3 ، عدد 10 ، ص 274.

[449] سعيد عبداللطيف حسن ، مرجع سابق ، ص159.

أما في إنجلترا يشترط قانون البوليس والإثبات الجنائي الصادر سنة 1984م على أنه لكي تتحقق يقينية الدليل الرقمي يجب أن تكون البيانات ، أو المخرجات المتحصلة من الحاسوب قد تمت بصورة سليمة ودقيقة.[450]

ومما تجدر الإشارة إليه أن الولايات المتحدة الأمريكية وإنجلترا قد أخذتا بقاعدة الدليل الأفضل ، وفحوى هذه القاعدة بأنها لا يجوز قبول صورة للمستند أو المحرر إذا كان من الممكن الحصول على الأصل.[451]

ويرجع وجود هذه القاعدة إلى تفسير الشروط الأساسية التي تقضي بأنه لا يعتبر دليلاً في الإثبات ، إذا كانت ثمة ما يشير بحسب الأصل إلى وجود دليل أفضل مما قُدّم.[452]

ومع ظهور المستندات الإلكترونية استدعى الأمر إلى تغيير هذه القاعدة ، لكي تتلاءم مع عصر المعلومات ، وبذلك قد أقر المشرع الأمريكي من خلال نص صريح توافر الحجية للأدلة الرقمية ، والاعتداد بهذا الدليل ، فقد نصت المادة (1/1001) من قانون الإثبات الفيدرالي الأمريكي على تعريف الكتابة ، والتسجيلات ، بأنها حروف ، أو أرقام ، أو كلمات ، أو ما يماثلها مكتوبة باليد ، أو منسوخة بالآلة الكاتبة ، أو مطبوعة ، أو مصورة ، أو متخذة شكل نبضات مغناطيسية بتسجيل ميكانيكي أو إلكتروني ، أو بأي طريقة أخرى لتجميع المعلومات.

كما عرف القانون ألإتحادي للتوقيعات الإلكترونية والتجارة الدولية الأمريكي الصادر في 30/يونيو/2000 ، المحرر الإلكتروني ، أو المستند الإلكتروني بموجب المادة (4/106) بأن المستند الإلكتروني هو "عقد أو أي مستند (سجل) أخر يتم إنشاؤه ، أو إحداثه ، أو إرساله ، أو نقله ، أو استلامه ، أو تخزينه بوسائل إلكترونية" .

وقد نصت المادة (1002) من قانون الإثبات الفيدرالي الأمريكي على أنه باستثناء ما هو مقرر في هذا القانون أو بقانون خاص يصدر عن الكونجرس ، فإنه عند إثبات مضمون الكتابة والتسجيل والصورة ، يلزم توافر أصل الكتابة ، أو التسجيل ، أو الصورة.

ونلاحظ من خلال هذا النص ، أن الأصل العام لحجية الكتابة ، أو التسجيل ، أو الصورة مرهون بتقديم أصل المستند ، إلا إذا نص القانون على خلاف ذلك.

والجدير بالذكر أن المادة (3/1001) أوردت استثناء على ضرورة توافر أصل الكتابة ، أو التسجيل ، أو الصورة ، يتمثل هذا الاستثناء في قبول الدليل الرقمي باعتباره مستنداً أصلياً مادام البيانات الصادرة عن الحاسوب ، أو أي آلة مشابهة سواء كانت تلك البيانات مطبوعة أو

---

(450) راشد بن حمد البلوشي ، مرجع سابق ، ص28.
- علي حسن محمد الطوالبة ، التفتيش الجنائي على نظم الحاسوب والأنترنت ، مرجع سابق ، ص195.
(451) سليمان أحمد فضل ، مرجع سابق ، ص374.
(452) طارق فوزي الفقي ، مرجع سابق ، ص220.

مقروءة تبرز انعكاساً دقيقاً للبيانات الأصلية [453] ، غير أن هذا لا يمنع القضاء الأمريكي من استبعاد هذه الأدلة ، إذا كانت ناتجة عن جهاز الحاسوب لا يؤدي وظائفه بصورة سليمة ، أو كان القائم عليه لا يتوافر فيه الثقة والطمأنينة[454] .

أما قاعدة الدليل الأفضل في التشريع الإنجليزي كانت ، أنه لا يجوز تقديم الصورة لإثبات محتوى الأصل ، إلا إذا كان الطرف الذي يحتج بالصورة لم يستطيع تقديم الأصل[455] ، أما الآن فصور المستندات تقبل بصفة عامة بموجب المادة (27) من قانون العدالة الجنائية الصادر سنة 1988 [456] .

كما خولت المادة (31) من قانون العدالة الجنائية سالف الذكر سلطة للمحكمة في وضع القواعد في القضايا الجنائية ، التي تسمح للمحلفين فهم الأمور المتعلقة بتكنولوجيا المعلومات بطريقة أفضل كتدبير احترازي لتوافر الدليل في شكل مختلف على الرغم من وجود الدليل الأفضل[457].

ونلاحظ فيما تقدم أنه يمكن اعتبار الكتابة الموجودة داخل الآلة في صورة كهرومغناطيسية من قبل النسخ الأصلية ، وبالتالي لا تصطدم بقاعدة الدليل الأفضل.

ثانياً . النظام اللاتيني :

إن ظهور المحررات الإلكترونية وانتشار التعامل بها عن طريق شبكة المعلومات الدولية الانترنت ، أدى إلى إثارة العديد من المشكلات القانونية ، التي لم تكن في حساب أي مُشرع عند سن القوانين ، التي تنظم المحررات ، والمعاملات القانونية ، فيما يتعلق بالجوانب الإجرائية كإثبات التصرف الذي يتم إجراؤه عن طريق الانترنت فالمحرر الإلكتروني يختلف عن المحرر الكتابي[458] ، حيث يتم تدوين المحرر الإلكتروني على دعامة إلكترونية يسهل تعديل بياناته أو التحريف فيها دون إتلاف الدعامة ، أو ترك أي أثر مادي يدل على التعديل أو التحريف[459] ، مما يترتب على ذلك أن بدأت المحررات الورقية التقليدية تتراجع ، ويحل محلها الدعامات الجديدة للمعلومات ، كنتيجة طبيعية لانتشار الحاسوب خصوصاً في المصارف والشركات والمؤسسات الحكومية ، ومن أمثلتها الشرائط الممغنطة ، وأسطوانات الفيديو ، والميكروفيلم[460] .

---

[453] سامح أحمد بلتاجي موسى ، مرجع سابق ، ص437.

[454] هلالي عبداللاه أحمد ، حجية المخرجات الكمبيوترية في المواد الجنائية ، مرجع سابق ، ص95.

[455] سعيد عبداللطيف حسن ، مرجع سابق ، ص 162.

[456] سليمان أحمد فضل ، مرجع سابق ، ص 374.

[457] طارق فوزي الفقي ، مرجع سابق ، ص220.

[458] **المحرر الكتابي** : هو كل ورقة أو محرر يحمل بيانات في شأن واقعة معينة يمكن نسبتها إلى المتهم . (محمد علي سكيكر ، أدلة الإثبات الجنائي في ضوء التشريع والقضاء والفقه ، دار الجامعة الجديدة ، الاسكندرية ، 2011 ، ص97) .

[459] محمد نصر محمد ، حجية الدليل الإلكتروني أمام القاضي الجنائي والمدني ، الطبعة الأولى ، مكتبة القانون الإقتصادي ، الرياض ، 2013 ، ص 11.

[460] عبدالفتاح بيومي حجازي ، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي دراسة متعمقة في مكافحة جرائم التقنية الحديثة ، الطبعة الاولى ، دار النهضة العربية ، القاهرة ، ص2009 ، ص 65.

وقد عرف القانون المدني الفرنسي رقم (230) الصادر في 13 مارس 2000 الدليل الكتابي بموجب نص المادة (1316) بأنه "مجموعة منتظمة من الحروف أو الأشكال أو الأرقام أو من أشارات أو رموز ذات دلالة مفهومة أياً كانت الدعامة المثبتة عليها أو الكيفية التي تنتقل بها" .

ونلاحظ أن هذا التعريف يتصف بالطابع العمومي فيستوي أن يتم نقل الكتابة بين الأطراف عن طريق شبكة الانترنت ، أو بواسطة إرسال اسطوانات مسجلة إلكترونياً ، أو غير ذلك من الوسائل المستخدمة .

كما عرف المشرع المصري في القانون رقم (15 لسنة 2004) بتنظيم التوقيع الإلكتروني المصري وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات المحرر الإلكتروني بموجب المادة (1 فقرة ب) بأنه "رسالة تتضمن معلومات تنشأ أو تدمج أو تخزن أو ترسل او تستقبل كلياً أو جزئياً بوسيلة إلكترونية أو رقمية أو ضوئية ، أو بأية وسيلة أخرى مشابهة" .

وقد يتعارض الدليل الكتابي مع الدليل الرقمي ، في هذه الحالة حيث أورد القانون المدني الفرنسي رقم (230) لسنة 2000 حكماً خاصاً بهذه الحالة تتمثل في السلطة التقديرية للقاضي المدني في تحديد أي من هذين الدليلين أكثر اتساقاً مع الحقيقة فتنص المادة (13162) على أنه "إذا لم ينص القانون على قاعدة أخرى ، وما لم يوجد اتفاق صحيح بين الأطراف ، يحكم القاضي في تعارض الأدلة الكتابية محدداً بكل الوسائل ، المستند الأكثر احتمالاً للصحة ، أياً كانت دعامته"[461] .

ولا يختلف المشرع المصري عن المشرع الفرنسي في حالة تعارض الأدلة الكتابية مع الأدلة الرقمية حيث نصت المادة (15) من القانون رقم (15) لسنة 2004 السالف الذكر على أنه "للكتابة الإلكترونية[462] والمحررات الإلكترونية في نطاق المعاملات المدنية والتجارية ذات الحجية المقررة للكتابة والمحررات الرسمية والعرفية في أحكام قانون الإثبات في المواد المدنية والتجارية ، متى استوفت الشروط المنصوص عليها في هذا القانون وفقاً للضوابط الفنية والتقنية التي تحددها اللائحة التنفيذية لهذا القانون" .

وقد نصت المادة (18) من ذات القانون على انه "يتمتع التوقيع الإلكتروني[463] والكتابة الإلكترونية ، والمحررات الإلكترونية بالحجية في الإثبات إذا توافرت فيها الشروط الآتية :-

---

(461) محمد نصر محمد ، مرجع سابق ، ص31-61-62.

(462) **الكتابة الإلكترونية** : "هي كل حروف أو أرقام أو رموز أو أي علامات أخرى تثبت على دعامة إلكترونية ، أو رقمية ، أو ضوئية ، أو أية وسيلة أخرى مشابهة ، وتعطي دلالة قابلة للإدراك" (المادة 1/ أ من القانون رقم (15) لسنة 2004 ، بتنظيم التوقيع الإلكتروني المصري ، وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات) .

(463) **التوقيع الإلكتروني** : " هو ما يوضع على محرر إلكتروني ، ويأخذ شكل حروف أو أرقام ، أو رموز ، أو إشارات أو غيرها ، ويكون له طابع منفرد يسمح بتحديد شخص الموقع يميزه عن غيره" (المادة 1/ج ، من القانون رقم 15 لسنة 2004 بتنظيم التوقيع الالكتروني المصري وبإنشاء هيئة التنمية صناعة تكنولوجيا المعلومات) .

1) ارتباط التوقيع الإلكتروني بالموقع وحده دون غيره.
2) سيطرة الموقع وحده دون غيره على الوسيط الإلكتروني.
3) إمكانية كشف أي تعديل أو تبديل في بيانات المحرر الإلكتروني ، أو التوقيع الإلكتروني.

ومن الجدير بالملاحظة أن المادة (15) من القانون رقم (15 لسنة 2004) السالف الذكر تضع على قدم المساواة المحرر الإلكتروني ، والمحرر التقليدي ، وبالتالي فإن حالة التعارض بين محررين أحدهما إلكتروني ، والآخر ورقي لا يبقى سوى الاعتداد بالسلطة التقديرية للقاضي في هذه الحالة ، وذلك للترجيح بينهما.

أما بالنسبة للمشرع الليبي ، فقد أشار في نصوص قانون الإجراءات الجنائية إلى ما يستخلص منه قبول المشرع المحررات كدليل إثبات ، من ذلك مثلاً ما نصت عليه المادة (274) إ ج ليبي "تعتبر المحاضر المحررة في مواد المخالفات حجة بالنسبة للوقائع التي يثبتها المأمورون المختصون ، إلى أن يثبت ما ينفيها" ويقابلها المادة (301) إ ج مصري.

ومما تجدر الإشارة إليه أن المستندات الرقمية لا تختلف عن المحررات التقليدية إلا من حيث الدعامة المدونة عليها ، غير أن هذا الاختلاف ليس له أثر على طبيعة المستند الرقمي من حيث انضمامه لمجموعة المحررات ، ولذا فإن الدليل الرقمي إذا ما اخذ شكل النص المكتوب فإنه يستمد مشروعيته من أنه يأخذ حكم المحررات التي يعتمدها المشرع كوسيلة من وسائل الإثبات الجنائي.[464]

كما نصت المادة (2/97) من قانون المصارف الليبي[465] ، على أنه "يعتد بالمستندات والتوقيعات الرقمية التي تتم في إطار المعاملات المصرفية ، وما يتصل بها من معاملات أخرى ، وتكون لها الحجية في إثبات ما تتضمنه من بيانات " .

وكما هو ملاحظ في هذا النص أنه أعطى للمستندات الرقمية الحجية في الإثبات إلا أن هذا النص لا يقتصر على مجال الإثبات المدني والتجاري كما جاء في نص المادة (1/97) على أنه "تسري على المصارف أحكام القانونين المدني والتجاري ، وذلك بالقدر الذي لا يتعارض مع أحكام هذا القانون " إنما يشمل الإثبات في الأمور الجنائية ، كإثبات جريمة غسيل الأموال التي يتم ارتكابها عن طريق المصارف ، حيث تصلح المستندات الإلكترونية المرتبطة بعمليات غسل الأموال كدليل لإثبات هذه الجريمة[466] ، وبالرغم من تعلق المادة (97) سالفة الذكر بالمعاملات المصرفية والتجارية ، إلا أنه يعتبر خطوة للمشرع الليبي في الأخذ بالمستندات

---

[464] طارق محمد الجملي ، مرجع سابق ، بدون ترقيم صفحات .
[465] القانون رقم (1) لسنة 2005م بشأن المصارف ، المعدل بالقانون رقم (46) لسنة 2012م ، نشر بالجريدة الرسمية في 2012/7/5م .
[466] طارق محمد الجملي ، مرجع سابق ، بدون ترقيم صفحات.

الرقمية ، ولعلنا نأمل من المشرع الليبي أن يساير هذا التطور الحاصل في تقنيات تكنولوجيا المعلومات ، فيما يصدر من تشريع في المستقبل يتعلق بالمسائل الجنائية.

ثالثاً . النظام المختلط :

يقرر الفقه الياباني قبول الأدلة المتحصلة من جهاز الحاسوب ، والتي تم تحويلها إلى الصور المرئية سواء كانت هي الأصل ، أم نسخاً مستخرجة عن هذا الأصل ، وذلك تأسيساً على الاستثناءات التشريعية المنصوص عليها في المادة (323) من قانون الإجراءات الجنائية الياباني ، ففي هذه الحالة يتحقق اليقين الذي يؤسس عليه القاضي الحكم الجنائي ، كما يمكن أن يتحقق اليقين بالنسبة للدليل الرقمي أيضاً بواسطة التقارير التي يقدمها الخبراء.[467]

ونخلص إلى تأييد الرأي الفقهي[468] ، الذي يرى أن المحاكم الجنائية ربما لا تواجه مشاكل في تعاملها مع الأدلة الجنائية الرقمية ، وذلك للأسباب التالية:[469]

أ – ارتباط الأدلة الرقمية ، وأثارها بالجرائم الإلكترونيه .

ب– وضوح الأدلة الرقمية ، ودقتها في إثبات العلاقة بين الجاني والمجني عليه ، او بين الجاني والسلوك الإجرامي.

ج – إمكانية تعقب آثار الأدلة الرقمية ، والوصول إلى مصادرها بدقه .

د– قيام الأدلة الرقمية على نظريات حسابية دقيقة لاشك فيها مما يقوي يقينية الأدلة الرقمية.

هـ الأدلة الرقمية يدعمها عادةً رأي الخبير ، وللخبير في الدعوى الجنائية دوره في إظهار الأدلة ، وفحصها وتقييمها ، وطرحها أمام القضاء وفقاً للشروط والقواعد التي نظمها القانون.

و– انتشار الجرائم الإلكترونيه لم يترك مجالاً للبحث عن وسائل لتحقيق العدالة باعتبارها جرائم مستحدثة ، لا تتم إلا من خلال نفس التكنولوجيا المعلوماتية.

---

[467] هلالي عبداللاه أحمد ، حجية المخرجات الكمبيوترية في المواد الجنائية ، مرجع سابق ، ص95-96.

[468] ناصر بن محمد البقمي ، مرجع سابق ، ص 42-43.

[469] محمد الأمين البشري ، مرجع سابق ، ص 127-128.

- ناصر محمد البقمي ، المرجع السابق ، ص 42-43.

المطلب الثالث

دور القضاء المستعجل في الجرائم الإلكترونية

قد يكون هناك من الظروف ما يستلزم التدخل القضائي الفوري للحفاظ على واقعة ما ، وعدم ضياع معالمها ، وذلك عن طريق اتخاذ إجراءات وقتية حالة وجود خطر محدق يهدد الحقوق والمصالح التي يحميها القانون ، وعندما يتم اللجوء إلى القضاء المستعجل فإنه لا يتم المساس بأصل الحق وجوهره ، وإنما يتلمس المنازعة في ظاهرها بما يحفظ الحق ، والمصلحة دون التعرض للموضوع الذي هو من اختصاص محكمة الموضوع.[470]

هذا وإن كان القضاء المستعجل قد حصر اختصاصه بالمسائل المدنية فقط إلا أنه وتحقيقاً للغاية منه باعتباره يدخل ضمن منظومة القوانين الإجرائية التي من ضمن أهدافها ضمان نفاذ القوانين الموضوعية ، فإنه يمكن أن يكون له دور عندما يشكل الاعتداء على الحق جريمة جنائية.

ويؤكد ذلك أن هناك أحوال استثنائية يطبق فيها قانون المرافعات أمام المحاكم الجنائية منها الإحالة بنص صريح ، وكذلك في وجود نقص في قانون الإجراءات الجنائية فيلتزم القاضي أن يولي شطر قانون المرافعات لسد هذا النقص غير أن ذلك مقيد بألا يوجد تعارض مع المبادئ العامة في قانون الإجراءات الجنائية.[471]

وتبعاً لما تقدم ونظراً للطبيعة الخاصة للجرائم الإلكترونيه سنجد لهذا القضاء دوراً هاماً في الوقاية من هذه الجرائم أو الفصل فيما يتعلق باستخدام الوسائل الإلكترونية في ارتكاب الجرائم الإلكترونية مما يتطلب في هذه الفئة من الجرائم ضرورة اتخاذ تدابير وقتية وسريعة بما يضمن عدم طمس معالم الجريمة أو تدمير أدلتها.

وبناءً على ذلك سنقسم هذا المطلب إلى ثلاثة فروع نخصص الفرع الأول لدراسة الأساس القانوني لتدخل القضاء المستعجل . ونكرس الفرع الثاني لدراسة شروط اختصاص القضاء المستعجل . ونفرد الفرع الثالث لدراسة الدور الوقائي للقضاء المستعجل.

الفرع الأول

الأساس القانوني لتدخل القضاء المستعجل

القضاء المستعجل وإن كان واسع التطبيق في المواد المدنية والتجارية إلا أنه لا يوجد ثمة ما يمنع قانوناً من تطبيقه في المواد الجنائية ، فلا يمكن أن ينكر حق اللجوء إليه على القانون الجنائي في حين أنه يجوز اللجوء إليه في فروع القضاء الأخرى هذا من جانب ، ومن جانب

---

[470] خميس السيد اسماعيل ، موسوعة القضاء المستعجل وقضاء التنفيذ وإشكالاته مع الأحكام الحديثة والصيغ القانونية أمام القضاء العادي ومجلس الدولة ، المجلد الأول ، الطبعة الأولى ، دار الطباعة الحديثة ، القاهرة ، 1990 ، ص 10 ومابعدها .

[471] محمود نجيب حسني ، مرجع سابق ، ص17.

- فوزية عبدالستار ، مرجع سابق ، ص12.

آخر لا يحق الاحتجاج بخصوصية القضاء المستعجل وحصره في قانون الإجراءات المدنية والتجارية خاصةً ، وذلك هذا الأخير يدخل ضمن منظومة القوانين الإجرائية والتي تشمل قانون الإجراءات الجنائية باعتبارها موضوعاً لقانون واحد هو القانون الإجرائي.[472]

كما أن القضاء المستعجل والقضاء الجنائي ينتميان إلى جهة قضائية واحدة ويرتدان إلى محكمة عليا واحدة بالإضافة إلى أن هذا القضاء لا يشكل عثره أمام النيابة العامة في أن تجري التحقيق في نفس الواقعة من الناحية الجنائية ، فالقرار الذي يتخذه قاضي الأمور المستعجلة ما هو إلا قراراً وقتياً يزول بمجرد صدور الحكم الموضوعي من القضاء المختص ، وإذا كان القانون قد أعطى للمضرور من الجريمة حق اللجوء إلى المحاكم الجنائية للمطالبة بالتعويض عن الضرر الذي لحقه المادة (224) إ ج ليبي ، رغم أن الاختصاص الأصيل للمطالبة بهذا التعويض منعقد للمحاكم المدنية ، فليس ثمة ما يمنع من مشاركة القضاء المستعجل للقضاء الجنائي من خلال تدخله لوقف الاعتداءات غير المشروعة حيث لا وجود لتعارض بين قضائين.[473]

وهذا ما ذهب إليه القضاء الفرنسي حيث قرر صلاحية القضاء الجنائي في إصدار أحكام مستعجلة في بعض المسائل الجنائية مثلما هو الحال في المادة (332-1) من قانون الملكية الفكرية الفرنسي رقم (354) الصادر في 10 مايو 1994 التي تجيز التقدم للقاضي الوقتي في المواد الجنائية بطلب ضبط المواد المقلدة سواء في العالم المادي أو العالم الافتراضي وذلك بعريضة مستعجلة وفقاً للمادة (332-4) من القانون ذاته.[474]

الفرع الثاني

شروط اختصاص القضاء المستعجل

يوجد العديد من الشروط التي على ضوئها يختص القضاء المستعجل بالنظر في الدعاوى المستعجلة وهي كالأتي :

أولاً . شرط الاستعجال :

يعتبر هذا الشرط من أهم الشروط التي أدت إلى نشوء هذا القضاء فالبطء الطبيعي المتعلق بمباشرة الحماية القضائية للحقوق الناجمة عن إجراءاتها الطويلة ، والمعقدة في بعض الأوقات قد يجعلها من غير الممكن تلافي وقوع هذه الأضرار ، مما يؤدي إلى عجز القضاء العادي عن إزالة هذه الأضرار بعد وقوعها بالفعل ، لأن عدم الاستعجال في مثل هذا الإجراء يترتب عليه وقوع أضرار لا يمكن إزالتها.[475]

---

[472] حسين بن سعيد الغافري ، السياسة الجنائية في مواجهة جرائم الانترنت ، مرجع سابق ، ص626.
[473] جميل عبدالباقي صغير ، الجوانب الإجرائية للجرائم المتعلقة بالانترنت ، مرجع سابق ، ص 24.
[474] سامح أحمد بلتاجي موسى ، مرجع سابق ، ص467-468.
[475] حسن سليمان محمد صالح ، الحكم المستعجل دراسة مقارنة ، دار المطبوعات الجامعية ، الاسكندرية ، 2013 ، ص16-17.

وإذا لم يتوافر هذا الشرط تعين على القاضي الحكم بعدم اختصاصه من تلقاء نفسه ، حتى ولو لم يدفع به الخصوم ، كما يجوز إبداء هذا الدفع في أي مرحلة كانت عليها الدعوى لتعلق الاختصاص بالنظام العام.[476]

ثانياً . أن يكون المطلوب إجراء وقتياً لا يمس أصل الحق :

فالقضاء المستعجل يتدخل لاتخاذ تدابير وقتيه أو تحفظيه لا تمس أصل الحق المتنازع عليه ، ولذلك فإن عمل القاضي المستعجل مقصور على بحث الأمر الظاهر ، فيقوم ببحث المستندات والأدلة المقدمة من الخصوم ، غير أن بحثه في هذا المجال لا يكون بحثاً وافياً للتوصل إلى وجود الحق الموضوعي أو عدم وجوده ، وإنما يكون بحثاً سطحياً يدل على احتمال وجود هذا الحق أو عدم وجوده.[477]

ثالثاً . أن يكون هناك خطراً عاجلاً أو محدقاً ماثلاً بالفعل :

للجوء إلى القضاء المستعجل يجب أن يكون هناك خطراً حالاً ومحدقاً ماثلاً بالفعل فلا يكفي أن يكون الخطر محتملاً أو مضموناً وقوعه ، ولا يكفي قيام الخطر العاجل في ذاته ، وإنما لابد وأن يكون من شأنه إحداث أضرار غير عادية على درجة معينة من الجسامة ويصل الضرر إلى هذه الدرجة إذا كان من شأنه أن يستنفذ أثاره دون أن يتمكن القضاء بإجراءاته العادية من تداركه[478] ، كضياع معالم واقعة معينة مما يترتب عليه فقدان الدليل وبالتالي ضياع الحق.

الفرع الثالث

الدور الوقائي للقضاء المستعجل في الجرائم الإلكترونيه

يقوم القضاء المستعجل كما سبق لنا القول بدور وقائي لحماية المصالح والحقوق المهددة بالخطر عن طريق مجموعة من التدابير والإجراءات ذات طبيعة وقتية وتحفظية دون المساس بأصل الحق ، وذلك حتى يتمكن القضاء بإجراءاته العادية من إنزال حمايته الموضوعية عليها.

وإذا كانت فكرة القضاء المستعجل قد أثبتت صلاحيتها في إطار الاختصاص القضائي فإنها كفكرة تصلح أيضاً في مجال الموضوعات الحديثة التي تطرح لأول مرة أمام القضاء[479]فقد أثبت الواقع العملي أن الدعاوى الجنائية تستغرق وقتاً طويلاً حتى يتم فيها الأمر الذي قد تضيع خلاله معالم الجريمة وخاصةً فيما يتعلق بالبيئة الالكترونية ، فبالنظر إلى الطابع المعنوي لمحل الجرائم الإلكترونية مثل جريمة التشهير عبر الانترنت ، أو جريمة التنصت المعلوماتي ، ومما تتسم به الجرائم الإلكترونية بإمكانية التلاعب فيها من على بُعد ، أو تعديل محتواها ، التي قد تستخدم كدليل إدانة ، ولكي يتدخل القضاء المستعجل بشأن هذه الجرائم يقتضي إثبات الواقعة

---

[476] www.startimes.com

[477] خميس السيد إسماعيل ، مرجع سابق ، ص19.

[478] حسن سليمان محمد صالح ، المرجع السابق ، ص 18-19.

[479] حسين بن سعيد الغافري ، السياسة الجنائية في مواجهة جرائم الانترنت ، مرجع سابق ، ص 612.

حتى يمكن الحكم فيها ، وخاصةً إذا رفعت دعوى قضائية بإجراءات عادية فإنها يمكن أن تستغرق فترة طويلة ، وهي مدة يمكن من خلالها إخفاء مواقع من على شبكة الانترنت ، أو تعديل محتواها الأمر الذي يمنح الفرصة للمتهم للاحتجاج بأن المعلومات قد تم التلاعب فيها أو تعديلها من قبل الغير.[480]

ومن هذا المنطلق لجأ البعض إلى الاعتراف لهذا القضاء بدوره في إطار الجرائم الإلكترونية لكونه يمنح القضاء دوراً أكثر ايجابية لجرائم تتسم بطبيعة خاصة من حيث حداثة الأسلوب ، وسرعة التنفيذ وسهولة الإخفاء ، والقدرة على محو آثارها ومعالمها.[481]

ومن التطبيقات القضائية لتدخل القضاء المستعجل في هذا المجال ما حدث في قضية (أيف روشيه) والتي تتلخص وقائعها في قيام المدعى عليه بنشر خصومته ضد المصرف الوطني لباريس على شبكة المعلومات الدولية (الانترنت) مستعملاً عبارات تحمل في طياتها ما يمكن اعتباره قذفاً في المصرف المذكور ، مما دفع الأخير إلى رفع دعوى أمام القضاء المستعجل بباريس طالباً الحكم بإلزام المدعى عليه بمحو كل ما قام بنشره على شبكة الانترنت إلا أن المدعى عليه دفع بأنه من المستحيل فنياً وتقنياً إيقاف ما تم نشره ، وبثه على شبكة الانترنت نظراً لأنه مجرد نشر المعلومات على الشبكة يتم تسجيلها أتوماتيكياً على كل الحواسب الآلية وبناء على ذلك قضت المحكمة بأنه يجب على من قام بنشر المعلومات غير المشروعة والتي تحمل في طياتها عبارات شائنة أن يثبت أنه بذل قصارى جهده لوقف هذا الاعتداء.[482]

---

[480] جميل عبدالباقي صغير ، الجوانب الإجرائية للجرائم المتعلقة بالانترنت ، مرجع سابق ، ص25.
[481] حسين بن سعيد الغافري ، السياسة الجنائية في مواجهة جرائم الانترنت ، المرجع السابق ، ص 617.
[482] جميل عبدالباقي صغير ، المرجع السابق ، ص 40.

الخاتمة

تم اختيار موضوع مدى قبول الدليل الرقمي في الإثبات الجنائي لما لهذا الموضوع من أهمية في وقتنا الحالي نظراً للطبيعة الخاصة التي تتسم بها الجرائم الإلكترونية مما يترتب عليه أن إثبات هذا النوع من الجرائم يحيط به كثير من الصعوبات وقد توصلنا في هذا البحث إلى النتائج والمقترحات الآتية :-

أولاً . النتائج :

أ) على الرغم مما قدمته وسائل التقنية الحديثة من تسهيلات للبشرية إلا أنه لم ينجُ من المجرمين الذين أساءوا استخدام وسائل التقنية الحديثة لارتكاب الجرائم ، مما ترتب عليه ظهور جرائم مستحدثة تختلف عن الجرائم التقليدية من حيث أساليب ارتكابها.

ب) قصور كثير من التشريعات العقابية العربية في مواجهة ظاهرة الجرائم الإلكترونية ، مما يترتب عليها إفلات الجُناة من العقاب ، إلا أنه في مقابل ذلك سعت عدة دول إلى إدخال تعديلات تشريعية في قوانينها العقابية لمواجهة ظاهرة الجرائم الإلكترونية ، كما أصدرت دول أخرى تشريعات خاصة لمواجهة هذه الظاهرة الإجرامية المستحدثة.

ج) إن الدليل الرقمي لا يقتصر على المعلومات أو البيانات المخزنة في الحاسب الآلي بل يشمل أيضاً ملحقاته كالطابعات والفاكس وغير ذلك من شبكات الاتصال ووسائلها كالانترنت والهاتف النقال وتشمل كذلك أي جهاز يعتمد على التقنية الرقمية كجهاز التصوير الرقمي بشرط أن يتم تجميعها وتحليلها باستخدام برامج وتطبيقات خاصة بهدف إثبات وقوع الجريمة ونسبتها إلى مرتكبها .

د) صعوبة تطبيق النصوص الجنائية الإجرائية التقليدية في مجال التقنيات الحديثة ، ذلك لأن هذه النصوص وضعت لحماية الأشياء المادية ، علاوة على ذلك أن تطبيق النصوص الإجرائية التقليدية قد يتعارض أحياناً مع طبيعة الوسائل المستخدمة لتنفيذ الجرائم التي يكون محلها البيانات أو المعلومات المخزنة بجهاز الحاسب الآلي مثلاً .

هـ) يجب أن يخضع التفتيش الذي يحدث في بيئة الجرائم الإلكترونية لمجموعة من الضوابط الموضوعية والشكلية لكي يسفر عن صحة النتائج المترتبة عليه.

و) يجوز تفتيش وضبط الكيانات المعنوية للحاسب الآلي وغير ذلك من وسائل تقنية المعلومات بشرط أن يتم تحويل البيانات أو المعلومات إلى صور أو تسجيلات أو نصوص عن طريق وحدات الإخراج الخاصة بالحاسب الآلي أو عن طريق وسائط التخزين أو الحفظ الإلكترونية كالأسطوانات أو الأقراص.

ز) تعقب مرتكب الجريمة الإلكترونية وتفتيش حاسبه الآلي ، وضبط الأدلة الرقمية الدالة على ارتكابه الجريمة لا يتقيد بإقليم الدولة التي تضررت من جريمته ، وإنما قد يمتد إلى خارج إقليم الدولة.

ح) إن المعاينة في مجال إظهار حقيقة أو كشف الجرائم الإلكترونية لا تصل إلى نفس الدرجة من الأهمية التي تلعبها في مجال الجرائم التقليدية لأن الجرائم الإلكترونيه قلما يترتب على اقترافها آثار مادية محسوسة فضلاً عن ذلك أن الأعداد الكبيرة من الأشخاص الذين قد يترددون على مسرح الجرائم الإلكترونية خلال المدة الزمنية الطويلة بين اقتراف الجريمة والكشف عنها يؤدي إلى حدوث تغيير أو عبث بالآثار المادية أو إتلافها.

ط) حرص كافة التشريعات الإجرائية المختلفة على تطبيق مبدأ مشروعية الدليل الجنائي ، وينطبق ذلك على الدليل الرقمي.

ي) إن التشريعات المقارنة أقرت حجية الدليل الرقمي ، إلا انها قيدت قبول ذلك بتوافر شروط معينة.

ق) إن الدليل الرقمي ما هو إلا تطبيق من تطبيقات الدليل العلمي بما يتميز به من موضوعية وحياد وكفاءة.

ثانياً . المقترحات :

أ) ضرورة تطوير قوانين العقوبات في الدول المختلفة ، وذلك بإصدار تشريعات خاصة لمواجهة الجرائم الإلكترونية .

ب) ضرورة تعديل قانون الإجراءات الجنائية الليبي ، ليواكب التطور التكنولوجي خاصة فيما يتعلق بنصوص إجراءات جمع الأدلة ، كالتفتيش والضبط والمعاينة.

ج) يجب رفع كفاءة رجال الشرطة من خلال معرفته بتكنولوجيا المعلومات بكيفية استخدامها والتعامل معها عن طريق دورات علمية وعملية .

د) عقد دورات للقائمين على التحقيق ، والحكم في الجرائم الإلكترونية من أعضاء النيابة العامة وكذلك القضاة ، لكي يكونوا على دراية بالتقنيات الحديثة ، حتى يكتسبوا ثقافة معلوماتية عن الحاسب الآلي وغير ذلك من الوسائل التقنية التي يتم استخدامها في ارتكاب الجرائم الإلكترونية.

هـ) ضرورة إضافة مقرر دراسي لطلاب كليات الحقوق وكليات الشرطة والمعاهد القضائية ، تتضمن معلومات عن وسائل التقنية الحديثة كجهاز الحاسب الآلي ، وكيفية التحقيق في القضايا المتعلقة بالجرائم الإلكترونية .

و) يجب توفير الإمكانيات الإلكترونية للخبير في المختبرات القضائية.

ز) ضرورة التعاون الدولي بين الدول لمواجهة الجرائم الإلكترونية والإشكاليات الإجرائية من خلال عقد اتفاقيات إقليمية و دولية في هذا المجال.

ح) يجب توافر الضمانات القانونية عند استخدام وسيلة اعتراض الاتصالات الإلكترونية.
ط) يمكن أن يتحقق التوازن بين مصلحة المجتمع في كشف الجريمة وملاحقة مرتكبيها ومصلحة المتهم في احترام حقوقه وحرياته ، بشرط مشروعية الوسيلة التي تمس الحرية الفردية عن طريق احترام القواعد القانونية واحترام النظام العام والآداب السائدة في المجتمع.

المراجع

أولاً . الكتب :

أ) الكتب العامة :

1- أحمد العطار ، شرح قانون الإجراءات الجنائية المصري المحاكمة وطرق الطعن في الأحكام ، 2013.

2- أحمد ضياء الدين محمد خليل ، قواعد الإجراءات الجنائية ومبادئها في القانون المصري ، الجزء الثاني ، كلية الشرطة ، 2004-2005.

3- أحمد فتحي سرور ، الوسيط في قانون الإجراءات الجنائية ، الطبعة الثانية ، دار النهضة العربية ، القاهرة ، 1970.

4- إيهاب عبدالمطلب ، الموسوعة الجنائية الحديثة في شرح قانون الإجراءات الجنائية ، المركز القومي للإصدارات القانونية ، الجزء الثالث ، الطبعة الأولى .

5- جلال ثروت ، نظم الإجراءات الجنائية وفقاً لآخر التعديلات ، مطابع السعدني ، 2004.

6- جندي عبدالملك ، الموسوعة الجنائية ، الأجزاء 1-2 ، دار أحياء التراث العربي ، بيروت ، لبنان ، 1976.

7- رؤوف عبيد ، مبادئ الإجراءات الجنائية ، دار الجبل للطباعة ، القاهرة .

8- عوض محمد عوض :

- قانون الإجراءات الجنائية ، الجزء الثاني ، 1995.

- المبادئ العامة في قانون الإجراءات الجنائية ، دار المطبوعات الجامعية ، الاسكندرية ، 1999.

9- فوزية عبدالستار ، شرح قانون الإجراءات الجنائية ، دار النهضة العربية ، القاهرة ، 1986.

10- مأمون محمد سلامه :

- الإجراءات الجنائية في التشريع الليبي ، الجزء الثاني ، الطبعة الثانية ، منشورات مكتبة الجامعة ، الزاوية ، 2000.

- الاجراءات الجنائية في التشريع المصري ، الجزء الثاني ، دار الفكر العربي ، القاهرة .

11- محمد زكي أبوعامر :

- الاجراءات الجنائية ، دار المطبوعات الجامعية ، الاسكندرية ، 1984.

12- محمود نجيب حسني ، شرح قانون الاجراءات الجنائية ، دار النهضة العربية ، القاهرة ، 1982.

13- محمود مصطفى ، شرح قانون الاجراءات الجنائية ، الطبعة الثامنة ، دار المطابع الشعبي ، 1962-1963.

14- محمد رمضان باره :

- القانون الجنائي الليبي ، القسم الخاص جرائم الاعتداء على الاموال ، الجزء الثاني ، مطابع عصر الجماهير ، الخمس ، 2002 .

- القانون الجنائي الليبي ، القسم الخاص جرائم الاعتداء على الاشخاص ، الجزء الأول الطبعة الأولى ، الدار العربية للنشر والتوزيع ، القاهرة ، 2005.

ب) الكتب المتخصصة :

1- إبراهيم الغماز ، الشهادة كدليل إثبات في المواد الجنائية ، عالم الكتب ، القاهرة ، 1980.

2- أحمد عوض بلال ، قاعدة استبعاد الأدلة المتحصلة بطرق غير مشروعة في الاجراءات ، دراسة مقارنة ، الطبعة الثانية ، دار النهضة العربية ، القاهرة ، 2008.

3- أبو العلا علي أبو العلا نمر ، الجديد في الاثبات الجنائي ، الطبعة الأولى ، دار النهضة العربية ، القاهرة .

4- أمير فرج يوسف ، الجرائم المعلوماتية على شبكة الانترنت ، دار المطبوعات الجامعية الاسكندرية ، 2010.

5- أحمد محمود موافي ، الجرائم الالكترونية وشبكة الانترنت ، دار نور الاسلام للطباعة والنشر والتوزيع ، القاهرة .

6- أحمد يوسف سوليه ، الحماية الجنائية والأمنية للشاهد ، دراسة مقارنة ، دار الفكر الجامعي ، الاسكندرية ، 2007.

7- التحكم في جرائم الحاسوب وردعها "المراقبة الدولية للسياسة الجنائية" ، ترجمة :د. عمر محمد بن يونس ، الطبعة الاولى ، دار النهضة العربية ، القاهرة ، 2005.

8- إيهاب أبوالعزم ، الخطوة الأولى في عالم الكمبيوتر ، الطبعة الأولى ، دار الكتب العلمية للنشر والتوزيع ، القاهرة ، 2009.

9- بشير علي القائد ، مقدمة في علم الحاسب الآلي ، الطبعة الرابعة ، دار الحكمة ، طرابلس 2009.

10- بلال أمين زين الدين ، الجرائم المعلوماتية في التشريع المقارن والشريعة الإسلامية دار الفكر الجامعي ، الإسكندرية ، 2014.

11- برهامي أبوبكر عزمي ، الشريعة الإجرائية للأدلة العلمية ، دراسة تحليلية لأعمال الخبرة ، دار النهضة العربية ، القاهرة ، 2006.

12- بكري يوسف بكري ، التفتيش عن المعلومات في وسائل التقنية الحديثة ، الطبعة الأولى ، دار الفكر الجامعي ، الاسكندرية ، 2011.
13- جميل عبدالباقي صغير :
- الجوانب الإجرائية للجرائم المتعلقة بالأنترنت ، دار الفكر العربي ، القاهرة ، 2001.
- الانترنت والقانون الجنائي ، دار النهضة العربية ، القاهرة ، 2012 .
14- حسين المحمدي بوادي ، الوسائل العلمية الحديثة في الإثبات الجنائي ، منشأة المعارف ، الاسكندرية ، 2008.
15- حسن سليمان محمد صالح ، الحكم المستعجل "دراسة مقارنة" ، دار المطبوعات الجامعية ، الإسكندرية ، 2013.
16- خميس السيد إسماعيل ، موسوعة القضاء المستعجل وقضاء التنفيذ وإشكالاته مع الاحكام الحديثة والصيغ القانونية أمام القضاء العادي ومجلس الدولة ، المجلد الأول ، الطبعة الأولى ، دار الطباعة الحديثة ، القاهرة ، 1990.
17- خيرت علي محرز ، التحقيق في جرائم الحاسب الآلي ، دار الكتاب الحديث ، القاهرة ، 2012.
18- خالد عبدالعظيم وآخرون ، مدى حجية الشهادة والقرائن وضوابط مشروعيتها في الإثبات ، دراسة مقارنة بين النظم الإسلامية والنظم الوضعية ، الطبعة الأولى ، دار الفكر الجامعي ، الاسكندرية ، 2013.
19- رمزي رياض عوض ، سلطة القاضي الجنائي في تقدير الأدلة "دراسة مقارنة" ، دار النهضة العربية ، القاهرة ، 2010.
20- رامي متولي القاضي ، مكافحة الجرائم المعلوماتية في التشريعات المقارنة وفي ضوء الاتفاقيات والمواثيق الدولية ، دار النهضة العربية ، القاهرة ، 2011.
21- سليمان أحمد فضل ، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية "الانترنت" ، دار النهضة العربية ، القاهرة ، 2013.
22- سعد حماد صالح القبائلي ، الشهادة أمام القضاء الجنائي "دراسة نظرية وتطبيقية مقارنة بالشريعة الاسلامية" ، الطبعة الأولى ، الدار العالمية للنشر والتوزيع ، الاسكندرية ، 2014.
23- سعيد عبداللطيف ، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت ، الطبعة الاولى ، دار النهضة العربية ، القاهرة ، 1999.
24- شيماء عبدالغني محمد عطا الله ، الحماية الجنائية للتعاملات الإلكترونية ، دار الجامعة الجديدة ، الاسكندرية ، 2007 .

25- شعبان محمود محمد الهواري ، أدلة الاثبات الجنائي ، الطبعة الأولى ، دار الفكر والقانون للنشر والتوزيع ، المنصورة ، 2013.
26- عبدالفتاح بيومي حجازي :
- الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت ، منشأة المعارف ، الاسكندرية ، 2009.
- الجوانب الإجرائية لأعمال التحقيق الإبتدائي في الجرائم المعلوماتية ، الطبعة الأولى 2009.
- مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي ، دراسة متعمقة في مكافحة جرائم التقنية الحديثة ، الطبعة الأولى ، دار النهضة العربية ، القاهرة ، 2009.
- الجريمة في عصر العولمة ، الطبعة الأولى ، دار النهضة العربية ، القاهرة ، 2009 ، 2010.
27- عفيفي كامل عفيفي ، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة ، منشأة المعارف ، الاسكندرية ، 2000.
28- عطا عبدالعاطي محمد السنباطي ، موقف الشريعة الإسلامية من جرائم الحاسب الآلي والانترنت "دراسة مقارنة" ، الطبعة الأولى ، دار النهضة العربية ، القاهرة ، 2002.
29- علي عبدالقادر القهوجي ، الحماية الجنائية لبرامج الحاسب الآلي ، دار الجامعة الجديدة ، الاسكندرية ، 2010.
30- عماد عوض عدس ، التحريات كإجراء من إجراءات البحث عن الحقيقة ، دار النهضة العربية ، القاهرة ، 2007.
31- عبدالحكم فوده :
- البطلان في قانون الإجراءات الجنائية ، دراسة تحليلية على ضوء الفقه والقضاء والنقض ، دار المطبوعات الجامعية ، الاسكندرية ، 1996.
- حجية الدليل الفني في المواد الجنائية والمدنية ، دار الفكر الجامعي ، الاسكندرية ، 2014.
32- عادل يحيى ، السياسة الجنائية في مواجهة الجريمة المعلوماتية ، دار النهضة العربية القاهرة ، 2014.
33- عاطف شعبان ، الاثبات في مرحلة التحقيق النهائي في ضوء الفقه والقضاء ، الطبعة الثانية ، 1994.
34- علي حسن محمد الطوالبة ، التفتيش الجنائي على نظم الحاسوب والانترنت ، "دراسة مقارنة" ، 2010.

35- عبدالله حسين علي محمود ، سرقة المعلومات المخزنة في الحاسب الآلي ، الطبعة الرابعة ، دار النهضة العربية ، القاهرة ، 2011.

36- عبدالخالق محمد أحمد الصلوي ، حجية الخبرة في الإثبات الجنائي "دراسة مقارنة" دار النهضة العربية ، القاهرة ، 2009.

37- عمر محمد بن يونس :

- الإجراءات الجنائية عبر الانترنت في القانون الأمريكي ، المرشد الفيدرالي الأمريكي لتفتيش وضبط الحواسيب وصولاً إلى الدليل الإلكتروني في التحقيقات الجنائية ، الطبعة الأولى ،2005.

- الدليل الرقمي ، الطبعة الأولى ، الجمعية العربية لقانون الانترنت ، 2007 .

38- فائزة يونس الباشا ، السياسة الجنائية لجرائم الكمبيوتر التشريع الليبي "نموذجاً وقانوناً" ، الطبعة الأولى ، دار النهضة العربية ، القاهرة ، 2012-2013.

39- قدري عبدالفتاح الشهاوي ، ضوابط التفتيش في التشريع المصري ، منشأة المعارف الاسكندرية ، 2005.

40- محمود أحمد طه ، المواجهة التشريعية لجرائم الكمبيوتر والانترنت ، "دراسة مقارنة" دار الفكر والقانون ، المنصورة ، 2012.

41- محمد عبدالله أبوبكر سلامه ، جرائم الكمبيوتر والانترنت ، منشأة المعارف ، الاسكندرية ، 2006.

42- مصطفى الشاذلي ، الجرائم الماسة بالشرق والاعتبار والآداب ، المكتب العربي الحديث الاسكندرية.

43- منير محمد الجنبيهي ، وممدوح محمد الجنبيهي ، جرائم الانترنت والحاسب الآلي ، دار الفكر الجامعي ، الاسكندرية ، 2004.

44- موسى مسعود ارحومة ، حرية القاضي الجنائي في تكوين عقيدته "دراسة مقارنة" ، الطبعة الأولى ، الدار الجماهيرية للنشر والتوزيع والإعلان ، ليبيا ، 1988.

45- محمد محي الدين عوض ، الإثبات بين الازدواج والوحدة في الجنائي المدني في السودان ، "دراسة مقارنة" ، مطبوعات جامعة القاهرة ، الخرطوم ، 1974.

46- محمد علي سكيكر ، أدلة الاثبات الجنائي في ضوء التشريع والقضاء والفقه ، دار الجامعة الجديدة ، الاسكندرية ، 2011.

47- محمد حسين منصور ، قانون الإثبات مبادئ الاثبات وطرقه ، منشأة المعارف ، الاسكندرية ، 1998.

48- محمد أبو العلا عقيدة ، مراقبة المحادثات التليفونية ، "دراسة مقارنة" ، دار الفكر العربي ،1994.

49- محمد عيد الغريب ، حرية القاضي الجنائي في الاقتناع اليقيني وأثره في تسبيب الأحكام الجنائية ، دار النهضة العربية ، القاهرة ، 2008.
50- محمد زكي أبوعامر ، الإثبات في المواد الجنائية ، دار الجامعة الجديدة ، الاسكندرية 2011.
51- محمود محمود مصطفى ، الاثبات في المواد الجنائية ، الجزء الأول ، الطبعة الأولى مطبعة جامعة القاهرة ، 1977.
52- مصطفى محمد موسى :
- المراقبة الالكترونية عبر شبكة الانترنت ، "دراسة مقارنة" ، الطبعة الاولى ، 2003
- التحقيق الجنائي في الجرائم الالكترونية ، الطبعة الأولى ، مطابع الشرطة ، القاهرة ، 2009.
53- محمد محمود الشركسي ، أحكام التفتيش في قانون الإجراءات الجنائية الليبي ، الطبعة الأولى ، دار النهضة العربية ، القاهرة ، 2012.
54- مصطفى مرعي هرجه ، شهادة الشهود في المجالين الجنائي والمدني وشهادة الزور واليمين الكاذبة ، دار محمود ، القاهرة .
55- محمد محمد محمد عنب ، استخدام التكنولوجيا الحديثة في الاثبات الجنائي ، مطبعة السلام ، الأسماعليه ، 2007.
56- محمد نصر محمد ، حجية الدليل الإلكتروني أمام القضاء الجنائي والمدني ، الطبعة الأولى ، مكتبة القانون والاقتصاد ، الرياض ، 2013.
57- مصطفى يوسف ، مشروعية الدليل في المسائل الجنائية في ضوء الفقه والقضاء ، الطبعة الأولى ، 2010.
58- نائلة عادل محمد فريد قوره ، جرائم الحاسب الآلي الاقتصادية ، دراسة نظرية تطبيقية ، دار النهضة العربية ، القاهرة ، 2004.
59- ناير نبيل عمر ، الحماية الجنائية للمحل الالكتروني في جرائم المعلوماتية ، دار الجامعة الجديدة ، الاسكندرية ، 2012.

60- هلالي عبداللاه أحمد :

- حجية المخرجات الكمبيوترية في المواد الجنائية ، "دراسة مقارنة" ، 1999

- الجوانب الموضوعية والإجرائية للجرائم المعلوماتية ، دار النهضة العربية ، القاهرة ، 2006.

- تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي ، الطبعة الثانية ، دار النهضة العربية ، القاهرة ، 2008.

- إلتزام الشاهد بالإعلام في الجرائم المعلوماتية ، "دراسة مقارنة" ، الطبعة الثانية ، دار النهضة العربية ، القاهرة ، 2008.

- جرائم المعلوماتية التقليدية والمستحدثة وتطبيقاتها في النظام البحريني ، دار النهضة العربية ، القاهرة ، 2013.

61- هدى حامد قشقوش ، جرائم الحاسب الإلكتروني في التشريع المقارن ، دار النهضة العربية ، القاهرة .

62- هشام عبدالحميد الجميلي ، المرجع الحديث في الاثبات الجنائي والدفوع الجنائية في ضوء مختلف الاراء وأحكام النقض ، دار علام للإصدارات القانونية ، 2014.

ثانياً . الرسائل العلمية :

1- السيد محمد حسن الشريف ، النظرية العامة للإثبات الجنائي ، "دراسة مقارنة" ، رسالة دكتوراه ، كلية الحقوق ، جامعة القاهرة ، 2002.

2- أيمن عبدالحفيظ عبدالحميد سليمان ، إستراتيجية مكافحة الجرائم الناشئة عن استخدام الحاسب الآلي ، "دراسة مقارنة" ، رسالة دكتوراه ، كلية الدراسات العليا ، أكاديمية الشرطة ، 2003.

3- أشرف إبراهيم جمال إبراهيم قنديل ، حرية القاضي الجنائي في تكوين إقتناعه ، رسالة دكتوراه ، كلية الحقوق ، جامعة عين شمس ، 2009.

4- إيمان محمد علي الجابري ، يقين القاضي الجنائي ، رسالة دكتوراه ، كلية الحقوق ، جامعة الاسكندرية ، 2002.

5- حسن عوض سالم الطراونه ، ضوابط السلطة التقديرية للقاضي الجنائي ، رسالة دكتوراه كلية الحقوق ، جامعة القاهرة ، 2005.

6- رشدي محمد علي محمد عيد علي ، الحماية الجنائية للمعلومات على شبكة الانترنت ، رسالة دكتوراه ، كلية الحقوق ، جامعة القاهرة ، 2009.

7- سامح أحمد بلتاجي موسى ، الجوانب الإجرائية للحماية الجنائية شبكة الانترنت ، رسالة دكتوراه ، كلية الحقوق ، جامعة الاسكندرية ، 2010.

8- صغير يوسف ، الجريمة المرتكبة عبر الانترنت ، رسالة ماجستير ، كلية الحقوق والعلوم السياسية ، جامعة مولود معمري ، 2013.
9- صنابر نصر غلاب ، ضوابط السلطة التقديرية للقاضي الجنائي ، "دراسة مقارنة" ، رسالة دكتوراه ، كلية الحقوق ، جامعة عين شمس ، 2011.
10- صالح شنين ، الحماية الجنائية للتجارة الإلكترونية ، "دراسة مقارنة" ، رسالة دكتوراه ، كلية الحقوق ، جامعة أبوبكر بلقايد تلمسان ، 2012-2013.
11- طارق فوزي الفقي ، الجوانب الإجرائية في الجرائم المعلوماتية ، "دراسة مقارنة" ، رسالة دكتوراه ، كلية الحقوق ، جامعة المنوفية ، 2011.
12- طه أحمد متولي ، الدليل العلمي وأثره في الاثبات الجنائي ، رسالة دكتوراه ، كلية الحقوق ، جامعة طنطا ، 2007.
13- فيصل امساعد العنزي ، أثر الاثبات بوسائل التقنية الحديثة على حقوق الإنسان ، رسالة ماجستير ، قسم العدالة الجنائية ، كلية الدراسات العليا ، جامعة نايف العربية للعلوم الإنسانية ،2007.
14- محمد مسعود محمد خليفة ، الحماية الجنائية لمعطيات الحاسب الآلي ، رسالة ماجستير ، كلية الحقوق ، جامعة الإسكندرية ، 2005-2006.
15- محمد حلمي حسان ، الحماية الجنائية للمحادثات الهاتفية ، رسالة ماجستير ، كلية الحقوق ، جامعة الاسكندرية ، 2008.
16- محمد رشاد إبراهيم ، الحماية الجنائية للحق في حرمة الاتصالات الشخصية ، رسالة دكتوراه ، كلية الحقوق ، جامعة الاسكندرية ، 2009.
17- نبيله هبه مولاي علي هروال ، الجوانب الاجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات ، "دراسة مقارنة" ، رسالة ماجستير ، كلية الحقوق ، جامعة الاسكندرية ، 2005.

ثالثاً – المقالات والبحوث :

1- أحمد الصادق الجهاني ، مقدمة في الاثبات الجنائي محاضرات قدمت لطلبة الدراسات العليا قسم القانون الجنائي ، جامعة قاريونس ، كلية القانون ، 2010.
2- أسامة بن غانم العبيدي ،"التفتيش عن الدليل في الجرائم " ، المجلة العربية للدراسات الأمنية والتدريب ، المجلد التاسع والعشرون ، العدد الثامن والخمسون ، 2013.
3- إيهاب صلاح الدين ، "الجرائم الإلكترونية" ، مجلة القضاء العسكري ، العدد الخامس عشر ، 2006.
4- إيناس هاشم رشيد ، "تحليل البصمة الوراثية ومدى حجيتها في مسائل الاثبات القانوني" مجلة رسالة الحقوق ، العدد الثاني ، 2012.

5- إياد علي الدرة ، "الأدلة الجنائية الإلكترونية" ، مجلة المعلوماتية ، العدد 72 ، منشور على الانترنت
Infomag.News sy//indexphp?ine=issues/showartictles?aid=1363
6- بوعناد فاطمة زهرة ،"مكافحة الجريمة الإلكترونية في التشريع الجزائري" ، مجلة الندوة للدراسات القانونية ، العدد الأول ، 2013.
7- جمانه كاظم علي الخليفة ، تقنيات الأدلة الجنائية الإلكترونية ، مقال منشور على الانترنت
Http//coeia.ksu.edu.say.
8- حسين بن سعيد الغافري ، الانترنت والاتجار بالبشر ، مقال منشور على الانترنت
www oman legal.Net vb/show thread.php?t=3629
9- حسن المرصفاوي ،"ضمانات المتهم في التحقيق الابتدائي" ، مجلة الأمن العام ، العدد التاسع عشر ، 1962.
10- راشد بن حمد البلوشي ، "الدليل في الجريمة المعلوماتية" ، مجلة الحقوق ، العدد الأول ، 2008.
11- سليمان عبدالمجيد ،"مراقبة المحادثات التليفونية" ، مجلة الأمن العام ، العدد 41 ، 1968.2- د. سرحان حسين المعيني ،"التحقيق في جرائم تقنية المعلومات" ، مجلة الفكر الشرطي ، المجلد العشرون ، العدد الرابع ، 2011.
13- ضياء عبدالله عبود الجابر وآخرون "المنظمة الدولية للشرطة الجنائية" مقال منشور على الانترنت .
Army.tech Net/forum/index php?threads
14- طارق محمد الجملي ، الدليل الرقمي في مجال الإثبات الجنائي ، مقال منشور على الانترنت.
Http//www.start imes.com.if aspx ? =30245909
15- علي محمود علي حموده ،"الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي" ، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية المنعقد بمركز البحوث والدراسات بدولة الأمارات العربية المتحدة فترة (26-27-2003/4/28).
Http//www.Flaw.Net/threads/11338
16- عمر محمد بن يونس "الإثبات الجنائي عبر الانترنت" ، مقال منشور على الانترنت
Http//www.ituarabis.org.coe/coe/2006 E.crime/Doeiu ARAdo ppt
17- عبدالناصر محمد محمود فرغلي ، و د. عبيد سيف سعيد المسماري ، "الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية ، دراسة تطبيقية ، بحث مقدم للمؤتمر المغاربي الأول لعلوم الأدلة الجنائية والطب الشرعي المنعقد بالرياض فترة (12-2007/11/14)

18- عبدالله علي محمود ، "إجراءات جمع الأدلة في مجال جريمة سرقة المعلومات" ، بحث مقدم إلى المؤتمر المغاربي حول الجوانب القانونية والأمنية للعمليات الإلكترونية المنعقدة بدولة الأمارات العربية المتحدة فترة (26-27-2003/4/28) منشور على الانترنت
Http//www.Flaw.Net/threads/11338
19- علي حسن الطوالبة "مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي ، دراسة مقارنة" ، مقال منشور على الانترنت
www.police.gov.bhireports/2011
20- فواز دليم الحربي "الأدلة الجنائية الحاسوبية مبادئ ومفاهيم وتقنيات" مقال منشور على الانترنت.
Http//Lexpertarabs.com.lar chives.1127.
21- كمال أحمد الكركي "التحقيق في جرائم الانترنت" بحث مقدم إلى المؤتمر المغاربي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية المنعقد بدولة الامارات العربية المتحدة فترة (26-27-2003/4/28) منشور على الانترنت
Http//almohok moon alarab.Ahlamontada.com/tlootopic.
22- محمد أبو العلا عقيدة ، "التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية " مقال منشور على الانترنت
www.osamabahar.com
23- محمد عبدالله المنشاوي ، جرائم الانترنت من منظور شرعي وقانوني ، موقع المنشاوي للدراسات والبحوث على شبكة الانترنت .
Http//www.minshawi.com/old/inter Netcrime.
24- مفتاح أبوبكر المطردي ، "الجريمة الإلكترونية والتغلب على تحدياتها" ، بحث مقدم إلى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية المنعقد بالسودان فترة (23-2012/9/25).
25- ممدوح عبدالحميد ، "الأدلة الرقمية والتحقيق الجنائي في جرائم الكمبيوتر" ، مقال منشور على الانترنت
Http//www.drmamdooh.com/images/lectures/is2fd.ppt.

26- موسى مسعود ارحومة:

- "ظاهرة غسل الاموال والجهود الدولية لمواجهتها " ، مجلة قاريونس العلمية ، السنة الخامسة عشر ، الأعداد الاول ، والثاني ، والثالث ، والرابع ، 2002 .

- " السياسة الجنائية في مواجهة جرائم الانترنت " ، مجلة دراسات قانونية ، العدد السابع عشر ، 2008.

- "الاشكاليات الاجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية" ، بحث مقدم إلى المؤتمر المغاربي الأول حول المعلوماتية والقانون ، المنعقد بأكاديمية الدراسات العليا طرابلس خلال الفترة (28-2009/10/29)

27- محمد محمد الألفي ، "مدى مشروعية الدليل المستمد من الانترنت: مقال منشور على الانترنت .

Http//www.Arbitraation.mailgroup/past 19537949972.

28- محمد علي سالم ، وحسن عبيد هجيج ،" الجريمة المعلوماتية " ، مجلة بابل للعلوم الانسانية ، المجلد 14 ، العدد 3 ، 2007.

29- محمد الامين البشري "الادلة الجنائية الرقمية مفهومها ، ودروها في الاثبات " المجلة العربية للدراسات العلمية والتدريب ، المجلد 17 ، العدد 33 .

30- ناصر محمد البقمي ، "اهمية الادلة الرقمية في الاثبات الجنائي دراسة وفق الانظمة السعودية" ، مجلة الفكر الشرطي ، المجلد الحادي والعشرون ، العدد الاول ، رقم 80 ، 2012.

31- "نظرة حول المشكلات القانونية والعملية لمواجهة الجريمة المعلوماتية" ، مجلة كلية الدراسات العليا ، العدد الحادي والعشرون ، 2009.

32- هشام محمد فريد رستم "الجرائم المعلوماتية أصول التحقيق الجنائي الفني وآلية التدريب التخصصي للمحققين " ، مجلة الأمن والقانون ، العدد الثاني ، السنة السابعة ، 1999.

33- وليد الكشباطي ، "جرائم اختراق الأنظمة المعلوماتية" مقال منشور على الانترنت .

Http//www.chawkitabib.info/spipphp?artict leu77.

رابعاً . المدونات التشريعية :

1- مجموعة التشريعات الجنائية ، الجزء الثاني ، الاجراءات الجنائية ، إعداد الإدارة العامة للقانون ، ليبيا ، الهيئة العامة لشئون القضاء ، 1987.

2- ، موسوعة التشريعات الجنائية ، قانون العقوبات الليبي ، منشور بالجريدة الرسمية ، عدد خاص ، 1954.

3- قانون الإجراءات الجنائية المصري والقوانين المكملة لها وفقاً لأحدث التعديلات ، إعداد ومراجعة أسامة أنور ، دار العربي ، 2014.

4- قانون تنظيم الخبرة القضائية (رقم (1) لسنة 1371)aladel.gov.ly/hom/?P=1297
5- قانون العقوبات المصري طبقاً لأحدث التعديلات بالقانون رقم (95) لسنة 2003) القانون (رقم (58) السنة 1937) بإصدار قانون العقوبات.
www.seoudi-Law.com/forums/showthread.
6- قانون (رقم (2) لسنة 2005) بشأن مكافحة غسل الأموال.
7- القانون (رقم (15) لسنة 2004) بشأن تنظيم التوقيع الإلكتروني المصري ، وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات.
8- قانون (رقم (1) لسنة 2005) بشأن المصارف المعدل بالقانون (رقم (46) لسنة 2012) نشر بالجريدة الرسمية (2012/7/5)
9- قانون جرائم المعلوماتية السوداني الصادر في (2007/6/20) .
10- قانون نظام مكافحة جرائم المعلوماتية السعودي ، الصادر بالمرسوم الملكي (رقم (17) بتاريخ 1428/3/8)
11- قانون جرائم أنظمة المعلومات الأردني (رقم (30) لسنة 2010) .
12- قانون الإتحادي الاماراتي (رقم (2) لسنة 2006) بشأن مكافحة جرائم تقنية المعلومات الاماراتي.
13- قانون العقوبات القطري (رقم (11) لسنة 2004) المتضمن فصل خاص بعنوان جرائم الحاسب الآلي.
14- قانون (رقم (70) لسنة 1973) بشأن إقامة حد الزنا وتعديل بعض أحكام قانون العقوبات الليبي.

خامساً . الأحكام القضائية :

أ) أحكام القضاء الليبي " المحكمة العليا "
ب) أحكام القضاء المصري " مجموعة أحكام النقض "

سادساً. مراجع أخرى :

1- مختار الصحاح ، محمد بن أبي بكر بن عبدالقادر الرازي ، الهيئة المصرية العامة للكتاب
2- الاتفاقية الأوروبية لحقوق الإنسان الصادرة في روما 4 نوفمبر /سنة/1950 .
www1.umn.edu/humantrts/arab/eunrcom.html.
3- الميثاق العربي لحقوق الإنسان أعتمد ونشر بموجب قرار مجلس جامعة الدول العربية رقم 5427 الصادر في 1997/9/15 منشور على الانترنت
Http//heiunige.ch/humanrts/arab/a003-2html
4- المنظومة الحصرية للتكنولوجيا التعليمية ، مفهوم الواقع الافتراضي ، منشور على الانترنت .
Http//techm31omat2012-b to gspot.com

5- موقع منظمة التعاون الاقتصادي والتنمية على شبكة الانترنت
www.occd.org
6- www.alalam-ir/News/177
7- Http//www.panapress.com
8- Http//www.press.maroc.com/t3438 topic.
9- www.aladel.gov/main/madu les/sections/itm.php?itemid=13101.
10- Http//www.star times.com/f.aspx?t=33675371.
11- www.hardiscssion/hr 45894.html.
12- www.dbaasco.com.
13- www.star times.com.