# الجـريمـــة المعلـومـاتيــة

## أنواعها وسبل مواجهتها

**La cybercriminalité, ses types et les moyens de la combattre**

**"دراسة تحليلية"**

**«Une étude analytique»**


**دكتور**

**احمد أبو زيد شحاته**

الحقيقة التي لا يساورها أدنى شكٍّ في مجال الإلكترونيات أنَّ الجريمة المعلوماتية cybercriminalité تُمثِّل تهديدًا خطيرًا على أمن الأشخاص وحرمة حياتهم الخاصة وأموالهم، بل تُمثِّل تهديدًا كبيرًا على أمن الدول، وقد تصل آثاره إلى حدِّ محوها من الوجود.

ومن زاوية أخرى، فإنَّ تعريف الجريمة الإلكترونية يكتنفه بعض الصعوبات؛ ويرجع ذلك لاختلاف الدول في تحديد ما يُمثِّل اعتداءً على حرمة الحياة الخاصة، وما هو مباح ويمكن تناوله عبر الوسائط الإلكترونية supports électroniques، فالقيم الأخلاقية تختلف من دولة لأخرى.

فالاعتداء على حرمة الحياة الخاصة l'atteinte à l'inviolabilité de la vie privée، والتحرش الجنسي، والسبُّ والقذف الإلكتروني، والاحتيال المعلوماتي، والسرقة المعلوماتية، والإرهاب، والتجسس الإلكتروني Cyber espionage (cyberespionage)؛ كلها تمثل أنواعًا للجرائم المعلوماتية. والواقع أنَّ الجريمة الإلكترونية تزداد يومًا بعد يوم، ويتفنَّن في ارتكابها المجرم المعلوماتي، الذي يتسم بالذكاء الشديد والتحوُّط في إخفاء آثارها المادية، فهي تُسمَّى –وبحقٍّ– الجريمة النظيفة، التي تخلو من العنف بعكس الجريمة التقليدية.

بيد أنَّ هناك تحدياتٍ كبيرةً تكتنف مواجهة هذا النوع من الجرائم؛ في مقدمتها: التعاون بين الدول في منع ارتكابها، والقبض على مرتكبيها، وتسليم المجرمين Extradition؛ لذلك يقف الاختصاص المكاني والقضائي عائقًا في تسهيل القضاء على هذه الجريمة.

لذلك لا بدَّ من وجود تعاون دولي وإقليمي حقيقي –وليس مجرد توصيات– وإجراءات وطنية للحدِّ من آثار هذه الجريمة، أُولى هذه الإجراءات: التوعية بكافة وسائل وقنوات الإعلام بخطورة هذه الجريمة وآثارها على المجتمعات، وإنشاء بنية تحتية تكنولوجية متطورة قاعدة على مجابهة مرتكبي هذا النوع من الإجرام.

**الكلمات المفتاحية:** حرمة الحياة الخاصة – الجريمة النظيفة – تعاون دولي – المجرم المعلوماتي – الوسائط الإلكترونية – أمن الأشخاص.

## Abstract:

The fact that there is not the slightest doubt in the field of Electronics is that information crime represents a serious threat to the security of people and the inviolability of their private life and money, and even represents a significant threat to the security of states, and its effects may reach the point of being erased from existence.

From another point of view, the definition of cybercrime is fraught with some difficulties; this is due to the differences between countries in determining what constitutes an attack on the inviolability of private life, and what is permissible and can be addressed through electronic Media supports electronics, moral values differ from one country to another.

The invasion of privacy L'atteinte à l'involilité de la vie privée, sexual harassment, cyber slander and slander, information fraud, information theft, terrorism, cyber espionage (cyberespionage) are all types of Information Crimes.

Indeed, cybercrime is increasing day by day, and the information criminal, who is very smart and careful in concealing its physical traces, is proficient in committing it.it is rightly called Clean crime, which is devoid of violence unlike traditional crime.

However, there are great challenges surrounding the face of this type of crime, foremost among them: cooperation between states in preventing its commission, arresting the perpetrators, and extraditing criminals Extradition; therefore, spatial and judicial jurisdiction stands as an obstacle in facilitating the elimination of this crime.

Therefore, there must be genuine international and regional cooperation-not just recommendations-and national measures to reduce the effects of this crime, the first of these measures: raising awareness of all media outlets and channels of the seriousness of this crime and its effects on societies, and the creation of advanced technological infrastructure based on confronting the perpetrators of this type of crime.


**Keywords:** inviolability of private life-clean crime-International Cooperation-Information criminal-electronic media - security of persons.

## مقدمة

### أولًا: موضوع البحث وأهميته:

أحدث التطور التكنولوجيُّ طفرةً غير مسبوقة في عالم الاتصالات وتقنية المعلومات، ويسَّر للأشخاص إمكانية الدخول السريع للشبكة العنكبوتية Internet، ولكن هذه التكنولوجيا أظهرت لنا الوجه القبيح لها، فيما ظهر من اعتداءات جرَّاءَ استخدام الحاسب الآلي، ويتمثل ذلك في: حالات الدخول غير المصرَّح به لجهاز الحاسب الآلي Cas d'accès non autorisé à un ordinateur الخاص بالمجني عليه La victime أو لحساباته الرقمية Ses comptes numériques بغرض سرقة بياناته ومعلوماته الخاصة، وقد تترتب على هذه السرقة نتائج خطيرة؛ من ذلك: معرفة بيانات حسابات الشخص الرقمية أو البنكية Les comptes numériques ou bancaires d'une personne، وكذلك معرفة الأرقام السرية لحساباته ولبطاقات الائتمان الخاصة؛ ما يؤدي إلى سهولة سرقة حسابات الشخص وتحويلها للجاني.

لذلك مسَّت الحاجة للمشتغل بالقانون فيما يتعلق بالإجرام المعلوماتي أو الإلكتروني Criminalité informatique ou électronique أنْ يكون ملمًّا به وبكل جوانبه وأبعاده؛ حيث بدأت بوادر هذا الإجرام تظهر مع زيادة وتيرة النمو المتسارع الذي تشهده دولة مصر على وجه الخصوص في استخدام النظم المعلوماتية، فضلًا عن ظروف السياسة الدولية والتبعية التكنولوجية Dépendance technologique في قطاع المعلوماتية؛ ما أدَّى إلى وجود مناخ ملائم لانتهاك حرمة البيانات الشخصية Inviolabilité des données personnelles وحق الإنسان في الخصوصية Le droit de l'homme à la vie privée، بل قد يصل الأمر إلى المساس بالأمن القومي والسيادة الوطنية Souveraineté nationale. فالعالم أصبح بلا شك غرفةً صغيرة يتنافس سكانها فيما بينهم للظفر بالحصول على أدوات التحكُّم ليتسيَّد الغرفة من لديه التقدم المعرفي؛ وبالتالي يستنزف الثروات ويتلاعب بمقدَّرات باقي سكان هذه الغرفة ومستقبلهم. والحقيقة أنَّ هذا التقدم المرعب كانت بذرةُ نشأته ومولده هو ظهور جهاز الحاسب الآلي، الذي أتاح بدوره

أمكانية تخزين المعلومة وتداولها بسهولة وسرعة عبر قرص مدمج صلب، ليتطوَّر بعد ذلك الأمر بظهور الإنترنت، الذي كان له عظيم الأثر في بيئة الاقتصاد والأعمال على وجه الخصوص.

**ونتساءل:** متى نستطيع الصمود في وجه الجرائم التكنولوجية الحديثة، التي تكاد تعصف بنا وتجعل منا لُعبة ملعونة في يد دول محتكرة لصناعة التكنولوجيا؟

ممَّا سبق نجد أن سبب ارتكاب هذه الجرائم هو الاستخدام السيئ لتكنولوجيا الاتصالات وبرامج الحاسب الآلي Programmes informatiques بوجه خاص، وهذا يضعنا في موضع صعب عند محاولة إثبات هذه الجريمة حال ارتكابها عن طريق الشبكة العنكبوتية – الإنترنت– ووسائل الاتصال الحديثة. وجدير بالذكر أنه نتج عن التقدم الذي شهده الحاسب الآلي والإنترنت والتطور التكنولوجي والذكاء الاصطناعي والتقدم التقني سهولة المعلومة وإتاحتها disponibilité de l'information؛ ممَّا فتح الباب على مصراعيه لظهور نوع جديد من الحروب، ولكنها –أي الحروب– لا يُسمَع فيها صوت الرصاص، وهي الحروب السيبرانية Cyber guerres والهجمات السيبرانية cyberattaques لحماية الأمن القومي والأمن الشخصي وأمن أنظمة الشبكات. فوسائل الاتصال التكنولوجية الحديثة أصبحت تخدم أغلب أفراد العالم، وفي تزايد مستمر؛ مما نتج عنه ظهور جرائم معلوماتية وإلكترونية خطيرة تنتهك غالبًا الأمن الشخصي والاقتصادي للأفراد.

بيد أنَّ الأمر يزداد صعوبة عند مواجهة هذه الجرائم وضبط مرتكبيها؛ نظرًا لتحوُّط وتمرُّس ودراية مرتكبي هذه الجرائم بكافة وسائل الانتهاكات واستغلال ثغرات النظام التكنولوجي، مما يفقد ثقة المتعاملين على هذه الوسائل ويهدد أمن المجتمع. الأمر الذي دفع المشرع المصري إلى التنبؤ بخطورة هذه الجريمة على أمن المجتمع وسلامته وحماية الأمن القومي للدولة؛ لذلك فقد أُصدر القانون رقم ١٧٥ لسنة ٢٠١٨م بشأن مكافحة جرائم تقنية المعلومات لمعالجة مشكلة في غاية الخطورة وتتسم بالتعقيد؛ وهي المعلوماتية أو الأمن المعلوماتي. بيد أنه نظرًا للتطور المُتلاحق في ارتكاب هذا الجريمة، الذي يساير دائمًا التقدم

الملحوظ في وسائل الاتصالات وشبكات الإنترنت؛ جعل من اكتشافها الصعوبة الأكبر التي تُعيق مواجهتها والقضاء عليها.

**ثانيًا: إشكالية البحث:**

لعلَّ أُولى الصعوبات التي تواجه الباحث هو حداثة موضوع الدراسة نسبيًّا، فضلًا عن أن التقنيات الإلكترونية تُعدُّ مجالًا خصبًا للتكوينات الإجرامية وعابرة للحدود الوطنية، بالإضافة إلى أنَّ تنامي وسائط الحاسب الآلي وتطورها بصورة مذهلة سهَّل من ارتكاب الجريمة الإلكترونية، وجعل من حصرها وتتبُّع مرتكبيها عملًا شاقًّا تكتنفه صعوبات بالغة.

يُضاف إلى ذلك أن التشريعات في الدول النامية تعجز عن مواكبة التطور الحاصل – الذي يتمثل في الجريمة المعلوماتية– عليه، وصعوبة تصور النظرة القانونية لهذه الجريمة، وأحيانًا يكون هناك بهذه الدول فراغٌ تشريعيٌّ بخصوص تكييف الأفعال والاعتداءات الواقعة والتداخل بين أنواع كثيرة من الجرائم الإلكترونية. وتبرز صعوبة تصنيف الجرائم المعلوماتية في تشعُّبها وتشابهها في بعض النقاط؛ فهناك جرائم تُرتكَب على نظم الحاسوب، وأخرى بواسطته، ومنها أيضًا تلك التي تسند إلى مرتكبها، أو إلى الأسلوب المتَّبع فيها، إلَّا أن التقسيم المتعارف عليه في أوساط الباحثين يضم ثلاثة أنواع رئيسية تتفرع عنها مجموعة من الجرائم.

جدير بالذكر أنَّ الدراسة تُثير إشكالية كبيرة بخصوص الجرائم الواقعة على الدولة، التي تتمثل في الصعوبات العملية في تطبيق الأفكار التقليدية والمستقرة بالقانون الجنائي والإجراءات الجنائية؛ كمبدأ الشرعية وسريان القانون من حيث الزمان والمكان وتنازع الاختصاص، وأهم هذه الجرائم: الإرهاب الإلكتروني، والتجسس الإلكتروني (Cyber espionage).

ناهيك عن أنَّ هذه الجرائم تُثير كثيرًا من الإشكاليات؛ ومنها المتمثل في: حداثة القوانين المنظمة لها، والتزايد الكمي في أعداد الجرائم الإلكترونية، والتطور النوعي في أساليب ارتكابها، وعدم مواكبة التشريعات للمجتمع الرقمي الذي هو في تطور مستمر، وصعوبة الوصول إلى شهود للجريمة، وصعوبة إثباتها خاصة فيما يخص الركن المادي الذي يتطلَّب

نصوصًا قانونية خاصة بها، وبخاصة في ظل شرعية العقوبات؛ حيث "لا جريمة ولا عقوبة أو تدابير أمن بغير قانون"، ووجود مبدأ تنازع القوانين خاصةً في ظل وجود مبدأ إقليمية القوانين؛ لأنها في غالبيتها جرائم عابرة للحدود، ومنه أيضًا صعوبة الملاحقة الأمنية في حال اشتراك عناصر إجرامية داخل الوطن وخارجه، وصعوبة الكشف عن الشروع في الجرائم الإلكترونية.

**ثالثًا: أهداف البحث:**

يهدف البحث إلى التوصل إلى تعريف جامع مانع للجريمة المعلوماتية، وبيان أنواع الجرائم المعلوماتية، وأركان كلِّ جريمة على حدة، والوقوف على المعالجة التشريعية لكل جريمة، ومعرفة مدى نجاح المشرع في إقرار نصوص التجريم والعقاب لكل جريمة.

بل والتحديات التي تواجه مكافحة الجريمة المعلوماتية Lutte contre la criminalité de l'information، وأساليب التعاون الدولي في مجال ضبط مرتكبي هذه الجرائم.

**رابعًا: منهج البحث:**

للإجابة عن إشكالية البحث، ولتحقيق الأهداف المبتغاة من الدراسة؛ ارتأى الباحث الاعتماد على المنهج التحليلي للنصوص القانونية بشيء من التفصيل؛ بغية استجلاء الأبعاد والجوانب المختلفة للموضوع، بالإضافة إلى دراسة التحديات وسبل تضافر الجهود الوطنية والإقليمية والدولية لمكافحة الجريمة المعلوماتية، أو الحد من آثارها الخطرة التي تصل إلى حدِّ محو الدولة المستهدفة من على خريطة العالم، بتقويض القيم والمبادئ الأخلاقية في المجتمع، بل وانهيار التجارة والصناعة في بعض الجرائم المالية. ولذلك سوف نتناول بالتحليل نصوص قانون العقوبات التي تعالج أنواع الجريمة المعلوماتية وقانون الإجراءات الجنائية؛ لتُطبَّق على هذه النوعية المستحدثة من الجرائم، فضلًا عن تناول قانون مكافحة جرائم تقنية المعلومات والاتصالات وبعض القوانين المقارنة كلما دعت الحاجة لذلك.

**خامسًا: خطة البحث:**

تمَّ تقسيم الدراسة إلى مبحثين رئيسَيْن؛ نتناول في الأول منهما: أنواع الجرائم المعلوماتية، التي تتمثل في: الجرائم الواقعة على الشرف بالنسبة للأشخاص، والجرائم الواقعة على الأموال،

والجرائم الواقعة على الدولة، ثم نتناول في المبحث الثاني: تحدِّيات مواجهة الجريمة المعلوماتية؛ حيث نوضح فيه سبل مكافحة الجرائم المعلوماتية وجهود الدولة والأجهزة الرقابية في ذلك، على أن يسبق هذين المبحثين مطلب تمهيدي للتعريف بالجريمة المعلوماتية؛ وذلك على النحو التالي: **مطلب تمهيدي: مفهوم الجريمة المعلوماتية.**

**المبحث الأول: أنواع الجرائم المعلوماتية.**

**المبحث الثاني: تحدِّيات مواجهة الجريمة المعلوماتية.**

## مطلب تمهيدي
## مفهوم الجريمة المعلوماتية

نشير بدايةً إلى حقيقة مؤدَّاها أنَّ طبيعة الجرائم المعلوماتية لا تختلف كثيرًا عن الجرائم التقليدية من الناحية الموضوعية، فموجود مجرم له دافع رئيسي ومحدَّد، وضحية لديها ثغرات معقَّدة أحيانًا، ومكان لارتكاب الجريمة، وأداة مستخدمة لارتكاب الفعل. وجدير بالذِّكر أنَّ هذه الأدوات التقليدية التي تُستخدم فيها أدوات مادية ملموسة هي بعكس الجرائم المعلوماتية التي يُستخدم فيها الحاسب الآلي نفسه، أو عن طريقه؛ حيث يتم الربط بين هذا الجهاز والإنترنت، الذي تطوَّر لدرجة تدعو لإعادة النظر في التشريعات الوطنية والدولية القائمة التي تناولت هذه الجريمة لمنعها وضبط مرتكبيها.

فالركن المادي في الجريمة المعلوماتية يُمثِّل كيان الجريمة؛ وهو عبارة عن "فعل الفاعل بصورة يمكن إثباتها كجريمة، وبه يتحقق الاعتداء على المصلحة المراد حمايتها، وعن طريق هذا الفعل تقع الأعمال التنفيذية للجريمة، فهو يُمثِّل النشاط الذي يصدر عن الجاني؛ ليتدخَّل من أجل هذا الفعل النظامُ ويقوم بعقابه". أمَّا الركن المعنوي فيُعبِّر عن إرادة المجرم المعلوماتي cyberdélinquant (القصد الجنائي)؛ فلا بدَّ أن يُرتكب الفعل المَجرَّم من شخص مريد إرادة فعلية بطواعية ورغبة وعن إدراك. والمعروف أن جرائم الإنترنت أو الكمبيوتر عمومًا في بدايتها كانت عبارة عن نشر محتوى غير أخلاقي؛ عن طريق نشر الإباحة والمحتوى المخالف للآداب العامة، إلى أن تحوَّل الأمر لنشر الشائعات والأخبار الكاذبة والمضللة Nouvelles fausses et trompeuses والترويج لها.

ليصل رِكاب التطور بتبِعاته من إحداث الثورة في تكنولوجيا المعلومات والاتصالات إلى منتهاه الخبيث ببزوغ الجريمة المعلوماتية والإلكترونية، التي لها كثير من المخاطر على المجتمع؛ وأبرز هذه المخاطر: انتهاك حرمة الحياة الخاصة، ونهب الأموال عن طريق خرق الحسابات البنكية الخاصة، وتقليد وتزوير السلع contrefaçon de marchandises، والاعتداء على الحريات، وغيرها من الجرائم المستحدثة. ولعل ما يزيد من صعوبة وضع

تعريف جامع مانع للجرائم المعلوماتية أنَّها دائمًا في تطور مستمر؛ فتضارب المعلومات المتاحة عبر الإنترنت وعدم ضبط سياسات الاستخدام وكثرة المستخدمين جعل من هذه الجرائم خطرًا وتهديدًا واضحًا ومتنوعًا في أشكاله وأساليبه.

أضف إلى ذلك أنَّ أنظمة العدالة الجنائية غير مجهَّزة للتعامل مع هذه النوعية من الجرائم؛ الأمر الذي يجعل من محاولة حصرها ومواجهتها من الصعوبة البالغة. ومن زاوية أخرى: تُعدُّ الجريمة ظاهرة اجتماعية يرتبط وجودها بوجود المجتمعات، فمتى وُجِدت المجتمعات وجد الأفراد برغباتهم وأهوائهم وأهدافهم المختلفة التي قد تتضارب وتتعارض أحيانًا، ممَّا يجعل البعض يرى في الاعتداء على الآخرين سبيلًا لتحقيق أهدافه الخاصة، فالجريمة قديمة قدم الوجود الإنساني(١).

ولا يخفى على كلِّ ذي لبٍّ خطورة الجريمة المعلوماتية أو الإلكترونية وتطورها، وخصوصًا في الآونة الأخيرة؛ نظرًا لما يشهده العالم من أزمة أصابت الضمائر الإنسانية والأزمات الاقتصادية المتتالية، والتي نخرت باطن الشعوب وثرواته؛ الأمر الذي دفع البعض ليجنح نحو تحقيق أموال بأي طريقة كانت وبصرف النظر عن الضرر الواقع على أقران المجتمع والدولة. وهو ما دفع رأيًا في الفقه الفرنسي إلى القول بأنه أدَّى استخدام تكنولوجيا المعلومات والاتصالات l'utilisation des TIC في العديد من المجالات إلى تحسُّن في راحتنا اليومية، وبالرغم من ذلك فقد صاحب ذلك للأسف مخاطر جديدة وتهديدات خطيرة، وكانت الخسائر المالية les pertes financières الناجمة عن الجرائم الإلكترونية dues à la cybercriminalité مرتفعة للغاية (٢).

**ونعود فنقول:** إنَّ الجريمة المعلوماتية أو الإلكترونية هي ظاهرة حديثة نسبيًّا، تطورت بتطور الحاسب الآلي وتكنولوجيا المعلومات والاتصالات، ودائمًا المقترف لهذه الجريمة ما

---

**(١)** راجع، **مليكة بن العربي وآخرين:** السلوك الإجرامي من منظور سيكولوجي، بحث منشور بمجلة القبس للدراسات النفسية والاجتماعية، العدد (١٤)، المجلد الأول، ٢٠٢٢م، ص٣٤.

(2) **Jean Cazeneuve**, La cybercriminalité: l'émergence d'un nouveau risque, AJ Pénal, 2012, p.268.

يستخدم أدوات متطورة تفوق الأدوات المستخدمة لدى أجهزة الدولة والشركات والأفراد، ويستغل ثغرات دقيقة في الأنظمة ليدخل من خلالها ويخترقها ليجد ضحيته ويستخدم سلطانه عليها دون هوادة. ولذلك يذهب رأي في الفقه(١) إلى القول بأنَّ الجريمة المعلوماتية هي صنف جديد من الجرائم؛ ذلك أنه مع ثورة المعلومات والاتصالات ظهر نوع جديد من المجرمين انتقلوا بالجريمة من صورتها التقليدية إلى أخرى إلكترونية، قد يصعب التعامل معها.

ويضيف أنَّه يمكن تعريف الجريمة المعلوماتية على أنها: كلُّ فعل غير مشروع يتورط في ارتكابه الحاسب الآلي، أو هو الفعل الإجرامي acte criminel الذي يُستخدَم في اقترافه الحاسب الآلي كأداة رئيسية من خلال الاتصال بالإنترنت، وهدفها: اختراق الشبكات أو تخريبها أو التحريف أو التزوير أو السرقة والاختلاس أو قرصنة وسرقة حقوق الملكية الفكرية أو التشهير. والجريمة المعلوماتية ذات طبيعة خاصة لتعلُّقها بأساليب المعالجة الإلكترونية للبيانات من تجميع وتجهيز للبيانات بغية الحصول على معلومات.

لذلك يذهب رأي في الفقه(٢) إلى تعريف الجريمة المعلوماتية على أنها: تلك الجرائم التي تتمثَّل في الاستخدام غير المشروع للحاسبات Utilisation illégale d'ordinateurs، أو بمعنى آخر الاستخدام غير المشروع للحاسبات، التي تتخذ صورة فيروس يهدف إلى تدمير الثروة المعلوماتية(٣). ومن ناحية أخرى عرَّف مؤتمر الأمم المتحدة العاشر(٤) لمنع الجريمة ومعاملة المجرمين الجريمة المعلوماتية أو التقنية على أنها: "كل جريمة يمكن ارتكابها بواسطة

---

**(١)** راجع بالتفصيل في هذا الرأي، **أشرف حسن محمد جواد:** الجريمة المعلوماتية والإلكترونية، أنوعها وخصائصها وطرق الوقاية منها، مجلة الدراسات المالية والمصرفية، الأكاديمية العربية للعلوم المالية والمصرفية، مركز البحوث المالية والمصرفية، المجلد (٢٣)، العدد الأول، ٢٠١٥م، ص٢٩.

**(٢)** راجع هذا التعريف، **عبدالفتاح حجازي بيومي:** جرائم الكمبيوتر والإنترنت في القانون الغربي والنموذجي، دراسة قانونية متعمقة في القانون المعلوماتي، الناشر دار الكتب القانونية، القاهرة، ٢٠٠٧م، ص٢٠.

(٣) راجع، **عبد الفتاح حجازي بيومي:** مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، ٢٠٠٦م، ص٢١.

**(٤)** راجع بالتفصيل، أوراق مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة المجرمين المنعقد في فيينا، خلال الفترة من ١٠ وحتى ١٧ إبريل ٢٠٠٠م.

نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوب à l'intérieur d'un système informatique.

ونلاحظ على هذا التعريف أنه اهتمَّ بالأداة المستخدمة في ارتكاب الجريمة، وتناسى دوافع وأغراض المجرم، بل إنه تناسى المجني عليه والثغرات التي يرتكز عليها المجرم في ارتكاب الجريمة. ويذهب رأي في الفقه(١) إلى القول بأن الجريمة المعلوماتية هي جريمة يُستخدم الحاسب الآلي كوسيلة أو كأداة لارتكابها أو يمثل إغراءً بذلك، أو جريمة يكون الكمبيوتر نفسه ضحيتها. ويذهب رأي(٢) آخر إلى القول بأنها: "كلُّ فعل تكون للمعلوماتية دورٌ مهمٌّ في ارتكابه أو محلٌّ له، ومعاقَب عليه بموجب القانون".

ومن جانب آخر يذهب رأي في الفقه الفرنسي(٣) إلى القول بأنه ليس هناك تعريف عام للجريمة الإلكترونية، ويرى الكثير أنَّ هذا المفهوم يُغطي في الواقع تصرفات أوسع بكثير، بل وتُعَد الجريمة السيبرانية/ الإلكترونية La cybercriminalité، التي تُسَمَّى أيضًا جرائم الكمبيوتر/ الجريمة المعلوماتية criminalité informatique، هي مفهوم واسع جدًّا يجمع معًا "جميع الجرائم الجنائية toutes les infractions pénales التي من المُحتمل أن تُرتَكَب susceptibles de se commettre عن طريق نظام كمبيوتر/ نظام معلوماتي sur ou au moyen d'un système informatique مُتَّصِل بشكل عام بشبكة مُعينة généralement connecté à un réseau".

**ومن وجهة نظرنا نقول:** إنَّ تعريف الجريمة المعلوماتية يصعب ضبطه وإحكامه في نصٍّ تشريعي؛ نظرًا لتطور الجريمة بتطوُّر الوسائل المستخدمة في طرائق ارتكابها، وبالتالي

---

(١) راجع، **محمد نصر محمد:** الوسيط في الجرائم المعلوماتية، مركز الدراسات للنشر والتوزيع، الطبعة الأولى، القاهرة، ٢٠١٥م، ص٣٣.

(٢) راجع، **عاصم الأمين قسم السيد الطاهر:** جرائم المعلوماتية وفقًا للقانون السوداني، دراسة مقارنة، مجلة الدراسات القانونية والاقتصادية، العدد الأول، المجلد التاسع، ٢٠٢٣م، ص١٤٦٠.

(3) Jean Cazeneuve, La cybercriminalité: l'émergence d'un nouveau risque, AJ Pénal, 2012, p. 268.

ظهور بعض الجرائم في المستقبل يُقيِّده تطبيق النصوص على أحكام الجريمة المستحدثة. لذلك نرى أنَّ وضع تعريف جامع مانع للجريمة المعلوماتية يكتنفه صعوبة كبيرة، وذلك من زاويتين.

**أُولى هذه الزوايا:** أنَّ العالم اليوم يعيش فترة من التقدم التقني في مجال الاتصالات

وتكنولوجيا المعلومات غير مسبوقة، وبمرور الوقت سيصبح كل شيء متاحًا افتراضيًّا، ويبدو أنَّ الإنسان سوف يحل محله أجيال كثيرة من الذكاء الاصطناعي، هذا التطور مكَّن المعلومة من الانتشار والمعرفة من الدراسة وسرعة التداول؛ لذلك يصعب حصر أنواع وطرق الاختراقات والجرائم المعلوماتية، على الأقل فيما هو قادم من عالم مليء بتكنولوجيا يصعب السيطرة عليها؛ لتداخلها وتشابكها إلى حدٍّ كبير.

**ومن زاوية ثانية:** أنَّ مجرمي ومنتهكي المعلوماتية يستخدمون عجزًا لدي مخترعي ومؤمِّني هذه التقنيات، وبمساعدة الآليات المشروعة يندسُّون بداخل المستخدمين العاديين ليظفروا بجريمة يصعب فعلًا على القائمين بحماية أنظمة الشبكات والمعلومات اكتشافها.

ناهيك عن أنَّ تعريف الجريمة المعلوماتية يحتاج لمزيد من الضبط والصياغة الصحيحة حتى يستغرق على الأقل أغلب الجرائم المستحدثة التي سيكشِف عنها المستقبل المليء بمزيد من الانتهاكات والاختراقات Violations et intrusions.

لذلك يذهب رأي في الفقه[١] في محاولة لتعريف الجريمة المعلوماتية إلى أن: الجريمة المعلوماتية Criminalité informatique، هي نشاط جرمي يقترن بالتقنية المعلوماتية وأجهزة الكمبيوتر، ويكون له أثر سلبي يمس الأفراد في جميع مناحي حياتهم، سواء بغرض تحقيق مكسب مادي أو غير ذلك من الأغراض التي يسعى الجاني الوصول إليها، من خلال إتقانه ومعرفته بخبايا المجال المعلوماتي وتقنياته. والحقيقة أنَّ جرائم المعلوماتية تُعدُّ تحديًا صعبًا وواقعًا ملموسًا ينتهج وينخر في مقدرات الأمم، يكفي أن نقول: إنَّ الجرائم المعلوماتية تمس

---

**(١)** راجع في هذا التعريف، **مارية بوجداين، مريم آل سيدي الغازي:** تحديات مواجهة الجرائم المعلوماتية وآليات الحماية، بحث منشور بمجلة العلوم الجنائية، المركز المغربي للدراسات والاستشارات القانونية وحل المنازعات، العدد السابع، ٢٠٢١م، ص٩٧.

الأمن القومي للدولة وبعضها يكاد يعصف بوجود الدولة نفسها، وهو ما يعرف بالحروب السيبرانية Les cyberguerres.

## المبحث الأول
## أنواع الجرائم المعلوماتية

يذهب رأي في الفقه[١] إلى القول بأنَّ الجريمة المعلوماتية يمكن تصنيفها إلى ثلاثة أنواع؛ **أولها:** الاعتداء على المكونات المادية للنظام المعلوماتي Composants physiques du système informatique، **وثانيها:** الاعتداء على المكونات المنطقية للنظام المعلوماتي، **وثالثها:** الاعتداء على البيانات الموجودة داخل النظام المعلوماتي système informatique.

ويذهب رأي في الفقه الفرنسي إلى القول بأنه يمكن تمييز ثلاثة أنواع من الجرائم المعلوماتية إلى جرائم تكنولوجيا المعلومات والاتصالات الخاصة، ولا سيما انتهاكات أنظمة المُعالجة الآلية للبيانات les atteintes aux systèmes de traitement automatisé de données، والمُعالجة غير المُصَرَح بها للبيانات الشخصية les traitements non autorisés de données personnelles؛ (مثل: النقل غير القانوني/ غير المشروع la cession illicite للمعلومات الشخصية)، وجرائم البطاقات المصرفية les infractions aux cartes bancaires، وعمليات التشفير غير المصرح بها أو غير المعلنة les chiffrements non autorisés ou non déclarés أو الاعتراضات les interceptions، والجرائم المتعلقة بتكنولوجيات المعلومات والاتصالات، ولاسيما استغلال الأطفال في المواد الإباحية la pédopornographie، والتحريض على الإرهاب l'incitation au terrorisme والكراهية

(١) راجع الرأي، **شريهان ممدوح حسن:** الجرائم المعلوماتية وسبل مواجهتها على المستويين الوطني والدولي، المجلة الإلكترونية الشاملة متعددة المعرفة لنشر الأبحاث، العدد (٢١)، يناير ٢٠٢٠م، ص١١، وما بعدها.

العنصرية على الإنترنت la haine raciale sur Internet، والاعتداء على الناس، والاعتداء على الممتلكات les atteintes aux biens، والجرائم التي تيسرها تكنولوجيا المعلومات والاتصالات، بما في ذلك عمليات الاحتيال عبر الإنترنت les escroqueries en ligne أو غسل الأموال le blanchiment d'argent أو التزوير la contrefaçon أو أي انتهاك آخر للملكية الفكرية(١).

بيد أنه نظرًا للتطور السريع الحاصل في طرق ارتكاب الجرائم المعلوماتية نقول إنه يصعب حصرها على وجه الدقة؛ لظهور أنواع مستحدثة ومعقَّدة في بعض الأحيان تختلف كليًّا عن الجرائم التقليدية. لذلك سنحاول جاهدين بحث وتقسيم أنواع الجريمة المعلوماتية وإجمالها في ثلاثة أنواع، وذلك بالنظر إلى المصلحة المعتدَّى عليها؛ لذلك سوف نقسمها إلى جرائم واقعة على شرف الأشخاص، والجرائم التي تمثل اعتداءً على الأموال infractions qui constituent une atteinte aux biens، وأخيرًا الجرائم الواقعة على الدولة.

## المطلب الأول

## جرائم الشرف الواقعة على الأشخاص

يُعرَّف الشرف بأنه: مجموعة من الشروط التي يتوقَّف عليها المركز الأدبي للفرد، أو أنها العاطفة المكنونة في صميم الشخص التي تخلع احترامه لنفسه عن طريق شعوره بأداء واجبه، ومهاجمة الإنسان في استقامته خدش لشرفه(٢). والحقيقة أنَّ حقَّ الإنسان في صيانة شرفه وعرضه والمحافظة على كرامته من الحقوق الأساسية اللصيقة بالشخصية القانونية، بغض النظر عن مكانة الإنسان في المجتمع؛ لذلك يُجرِّم القانون أيَّ اعتداء يقع على كرامة الشخص وشرفة واعتباره، عبر الوسائط الإلكترونية. جدير بالذكر أنَّ المحافظة على هذا الحق يصطدم مع كفالة الدولة حرية التعبير والرأي والنقد وتداول المعلومات والنشر.

---

(1) Jean Cazeneuve, op. cit., p. 268.

(٢) راجع، **هدى أبوبكر سالم باجبير**: السب الإلكتروني.. حُكمه وصوره وعقوبته في الفقه والقانون، مجلة الفقه والقانون، العدد السادس والستون، إبريل ٢٠١٨م، ص٤٥.

والحقيقة أنَّ المشرع المصري من خلال نص المادة (٩٥) من قانون الإجراءات الجنائية[١] قرَّر أنه: "لقاضي التحقيق أنْ يأمر بضبط جميع الخطابات والرسائل والجرائد والمطبوعات والطرود lettres, journaux, publications, colis 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 في جنحة معاقَب عليها بالحبس لمدة تزيد على ثلاثة أشهر، وفي جميع الأحوال يجب أن يكون الضبط أو الاطلاع أو المراقبة أو التسجيل بناءً على أمر مسبب ولمدة لا تزيد على ثلاثين يومًا قابلة للتجديد لمدة أو مدد أخرى مماثلة". **ومن وجهة نظرنا:** أنه على الرغم من الضوابط التي تضمنتها المادة سالفة البيان وغاية المشرع في كفالة الحماية الواجبة للمراسلات والخطابات وإلزامية الحصول على أمر مسبَّب ولمدة معينة لمراقبة وتسجيل المحادثات الخاصة، إلَّا أن المشرع تناسي أيضًا خطورة هذه الجريمة التي تتعدى –من وجهة نظرنا– المصلحة التي أولاها المشرع بالحماية؛ وهي حرية المراسلات والمكاتبات Liberté de correspondance.

ويبدو أنَّ المشرع المصري عند إقرار هذه القانون في بداية الخمسينات وتعديلاته في بداية السبعينات من القرن الماضي لم يتنبأ بما حادث من تطور غير مسبوق في عالم الاتصالات وتقنية المعلومات. على أيّ حال يمكن تصنيف الجرائم الواقعة على الشرف إلى جريمة انتهاك حرمة الحياة الخاصة، والتحرش الجنسي عبر الإنترنت Harcèlement sexuel en ligne، وكذلك السب والقذف الإلكتروني.

## الفرع الأول
## جريمة انتهاك حرمة الحياة الخاصة

(١) قانون الإجراءات الجنائية رقم ١٥٠ لسنة ١٩٥٠م، والصادر بتاريخ ١٩٥١/٩/٣م، والمنشور بالوقائع المصرية بالعدد (٩٠)، والمعمول به اعتبارًا من ١٩٥١/١١/١٤م، بشأن إصدار قانون الإجراءات الجنائية.

لا شكَّ أنَّ الحياة الخاصة للإنسان تُمثِّل أهمية كبيرة له؛ فالعيش في سلام وبعيدًا عن العلانية له من الفوائد التي لا يمكن حصرها(١). لذلك يذهب رأي في الفقه(٢) إلى القول بأن: "حرمة الحياة الخاصة هي قطعة غالية من كيان الإنسان لا يمكن انتزاعها منه وإلَّا تحوَّل إلى أداة صماء عاجزة عن القدرة على الإبداع الإنساني، فالإنسان بحكم طبيعته له أسراره الشخصية، ومشاعره الذاتية، وخصائصه المتميزة، ولا يمكن للإنسان أن يتمتَّع بهذه الملامح إلا في مناخ يحفظها ويهيئ لها سبيل البقاء".

لذلك نقول: إنه تسمو حماية حرمة المسكن Protection de l'inviolabilité du logement بذاتها على إعمال مقتضى قواعد التجريم والعقاب والغاية منها؛ ففي حماية حرمة المسكن يكون الأمن والاستقرار في المجتمع، "فمَنْ أَصْبَحَ آمِنًا فِي سِرْبِهِ مُعَافًى فِي جَسَدِهِ عِنْدَهُ قُوتُ يَوْمِهِ فَكَأَنَّمَا حِيزَتْ لَهُ الدُّنْيَا بِحَذَافِيرِهَا" صدق رسول الله ﷺ، وهو ما تحرص عليه الدولة المصرية في إدارة مجتمعاتها الآمنة والمستقرة؛ وبذلك تتحقق حماية الحقوق والحريات فيها، التي هي غاية الدستور والقوانين والقضاء في هذه الدولة القانونية...". والحقيقة أنَّ المشرع المصري أولى اهتمامًا بالغًا بحرمة الحياة الخاصة؛ لذلك نجد نص المادة (٥٧) من الدستور الحالي(٣) تنص أنه: "للحياة الخاصة حرمة، وهي مصونة لا تُمَس، وللمراسلات البريدية، والبرقية، والإلكترونية، والمحادثات الهاتفية Correspondance postale, télégraphique, électronique, conversations téléphoniques، وغيرها من وسائل الاتصال حرمةٌ، وسريتها مكفولة، ولا تجوز مصادرتها، أو الاطلاع عليها، أو رقابتها إلَّا بأمر قضائي مسبب، ولمدة محددة، وفي الأحوال التي يبينها القانون، كما تلتزم الدولة بحماية حق المواطنين في

(١) راجع في هذا المعنى، **شيلان محمد شريف:** المواجهة الجنائية لانتهاك حرمة الحياة الخاصة، مجلة كلية القانون للعلوم القانونية والسياسية، جامعة كركوك، العراق، المجلد (١٢)، العدد (١٤)، ٢٠٢٣م، ص٥٨٠.

(٢) راجع، **أحمد فتحي سرور**: الحماية الجنائية للحق في الحياة الخاصة، القاهرة، دار النهضة العربية، ١٩٧٦م، ص٥٤ وما بعدها.

(٣) راجع الدستور الحالي لسنة ٢٠١٤، الصادر بتاريخ ٢٠١٤/١/١٨م، والمنشور بالجريدة الرسمية بالعدد(٣) مكررًا (أ) بتاريخ ٢٠١٤/١/١٨م، والمعمول به اعتبارًا من ٢٠١٤/١/١٨م، بشأن إصدار دستور جمهورية مصر العربية المعدل لسنة ٢٠١٤م.

استخدام وسائل الاتصال العامة بكافة أشكالها، ولا يجوز تعطيلها أو وقفها أو حرمان المواطنين منها، بشكل تعسفي arbitrairement، وينظم القانون ذلك".

جدير بالذِّكر أنَّ فرنسا من أهم الدول الساعية لتأمين حماية حقوق المواطنين وحرياتهم في كافة المجالات؛ ومنها: الحماية من تكنولوجيا المعلومات؛ حيث أصدرت العديد من القوانين، ومنها قانون المعلوماتية والحريات لعام ١٩٧٨م، وأكملت بإنشاء سلطة إدارية مستقلة هي اللجنة الوطنية للمعلومات والحريات Commission nationale de l'informatique et des libertés، كما قامت بإدخال العديد من التعديلات على القانون الجنائي؛ حيث تضمن في المواد (٤١) و(٤٤) الحماية الشخصية، وتناول الجرائم والأحكام الخاصة بالعقاب، وقد قدَّم قانون العقوبات الحديث في العديد من مواده تعديلات تعلَّقت جميعها بحماية البيانات الشخصية؛ مثل: حماية المراسلات، وإفشاء البيانات الاسمية، وتغيير الغرض المحدد لجمع البيانات الاسمية données nominales، والمعالجة غير المشروعة للبيانات traitement illicite des données[(١)].

والجدير بالذِّكر أنَّ الحق في الخصوصية privacy التقليدي يتمثل في حق الفرد في الاحتفاظ بأسراره الخاصة؛ مثل: السر الطبي والسر المصرفي، وحرمة المسكن، والحق في حماية المعلومات الخاصة والمراسلات والصورة Le droit à la protection des informations privées, de la correspondance et de l'image، والحق في حماية أفكاره ومشاعره، إلَّا أن التطور الهائل في تقنيات الحاسب الآلي والإقبال على استخدام شبكة الإنترنت قد أدَّى لظهور مفهوم الحق في خصوصية المعلومات Le concept du droit à la confidentialité des informations في عصر المعلوماتية L'ère de l'information (aussi connue comme ère numérique ou ère informatique)

(١) **فاضلي سيد علي:** آثار التطور التكنولوجي على حماية الحق في الخصوصية في النظام الأوربي لحماية حقوق الإنسان، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد(٥)، العدد(٢)، ٢٠٢٠م، ص١٦٤٣.

وبات هذا الحق يشمل سرية مراسلات البريد الإلكتروني وحماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي.

**مما سبق نستخلص** عناصر الحق في حرية الحياة الخاصة inviolability of private life، والتي لا يمكن حصرها في نطاق معين، ولكنَّنا نذكر أهمها؛ وهي: حرمة المسكن، والحق في حرية المراسلات والمحادثات، والحق في حرمة الحياة العائلية، والحق في حرمة الحياة الصحية، والحق في حرمة صورة الإنسان.

**ومن وجهة نظرنا نقول:** إنَّه بالرغم من اتفاق كافة التشريعات[١] على الحق في حرمة الحياة الخاصة، وباعتباره أحد أنواع الحقوق الشخصية، إلَّا أنه يصعب حصرها؛ لاختلاف هذا الحق من بلد لبلد آخر، وبالتالي يصعب وضع تعريف جامع مانع للحق في الحياة الخاصة.

ولكننا يمكننا وضع تعريف منضبط إلى حدٍّ كبير لحرمة الحياة الخاصة، التي تعني: "حرية الفرد في عدم إفشاء معلوماته الشخصية المعالجة إلكترونيًّا Disclosure of personal information processed electronically والاحتفاظ بكلِّ ما يتعلق بحياته

(١) راجع من هذه التشريعات، الدستور الإماراتي من خلال المواد (٢٦، ٣١، ٣٦) من دستور الإمارات العربية المتحدة لسنة ١٩٧١م، والصادر بتاريخ ١٩٧١/٧/١٨م، والمنشور بالجريدة الرسمية بالعدد رقم (١) السنة الأولى، بتاريخ ١٩٧١/١٢/٣١م، والمعمول به اعتبارًا من ١٩٧١/١٢/٢م، وقانون العقوبات الإماراتي – قانون اتحادي – رقم ٣ لسنة ١٩٨٨م، والصادر بتاريخ ١٩٨٧/١٢/٨م، والمنشور بالجريدة الرسمية بالعدد (١٨٢)، السنة السابعة عشرة، والمعمول به اعتبارًا من ١٩٨٨/٣/٢٠م، والقانون الاتحادي لسنة ٢٠١٢م، بشأن مكافحة جرائم تقنية المعلومات، وتُعدُّ دولة الإمارات العربية المتحدة من أوائل الدول التي لها قصب السبق في حماية هذا الحق، وتُعدُّ أيضًا الشريعة الإسلامية بأحكامها من أوائل التشريع التي أهتمت بالحق في الخصوصية، والاتفاقيات والمعاهدات والإعلانات الدولية اهتمَّت أيضًا بالحق في الخصوصية، وأهمها الإعلان العالمي لحقوق الإنسان، وأهمها حق الفرد في المحافظة على السر الطبي والسر المصرفي والاحتفاظ بأسراره الخاصة.

الخاصة، المتمثلة في: المعلومات العائلية والمهنية والصحية والغرامية ودخله ومعتقداته الدينية croyances religieuses، بل يعني الحق في أن يعيش الإنسان بعيدًا عن العلانية"[١].

بيد أنَّ أركان جريمة انتهاك حرمة الحياة الخاصة منها المادي والمعنوي، والأول منهما يعني الوجه الظاهر للجريمة، ولا تقوم تلك الجريمة إلَّا بتوافره؛ إذ بغير ماديات ملموسة لا يتحقق الاعتداء على المصلحة التي يحميها القانون.

نعود فنقول بأنَّ الركن المادي لجريمة انتهاك حرمة الحياة الخاصة L'élément matériel du délit de violation de l'inviolabilité de la vie privée يتمثَّل في سلوك مادي ونتيجة وعلاقة سببية؛ لذلك يتمثَّل السلوك الإجرامي في هذه الجريمة كما ذهب المشرع المصري بنص المادة (٣٠٩) مكررًا من قانون العقوبات[٢] على أنه: "يُعاقب بالحبس مدة لا تزيد على سنة كلُّ من اعتدى على حرمة الحياة الخاصة للمواطن، وذلك بأن ارتكب أحد الأفعال الآتية في غير الأحوال المصرح بها قانونًا أو بغير رضاء المجني عليه:

(أ) استرق السمع أو سجَّل أو نقل عن طريق جهاز من الأجهزة أيًّا كان نوعه محادثاتٍ جرت في مكان خاص أو عن طريق التليفون، (ب) التقط أو نقل بجهاز من الأجهزة أيًّا كان نوعه صورةَ شخص في مكان خاص، فإذا صدرت الأفعال المشار إليها في الفقرتين السابقتين أثناء اجتماع على مسمع أو مرأى من الحاضرين في ذلك الاجتماع؛ فإنَّ رضاء هؤلاء يكون مفترضًا، ويعاقب بالحبس الموظف العام الذي يرتكب أحد الأفعال المبينة بهذه المادة اعتمادًا على سلطة وظيفته، ويحكم في جميع الأحوال بمصادرة الأجهزة Confiscation des appareils وغيرها مما يكون قد استخدم في الجريمة، كما تحكم بمحو التسجيلات المتحصلة عنها أو إعدامها".

---

(١) راجع قريبًا من ذلك، **إبراهيم شمس الدين:** وسائل مواجهة الاعتداءات على الحياة الشخصية في مجال تقنية المعلومات، دار النهضة العربية، القاهرة، ٢٠٠٥م، ص٥٧.

(٢) راجع، قانون العقوبات المصري رقم ٥٨ لسنة ١٩٣٧ م، والصادر بتاريخ ١٩٣٧/٧/٣١م، والمنشور بالوقائع المصرية بالعدد (٧١)، بتاريخ ١٩٣٧/٨/٥م، والمعمول به بتاريخ ١٩٣٧/١٠/١٥م، وهذه المادة معدلة بالقانون رقم ٩٥ لسنة ١٩٩٦م المنشور بالجريدة الرسمية بتاريخ ٣٠ / ٠٦ / ١٩٩٦م.

وشدَّد المشرع المصري أيضًا[١] في إقرار عقوبة رادعة للمنتهك لحرمة الحياة الخاصة بقوله: "يُعاقب بالحبس مدةً لا تقل عن ستة أشهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تُجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين كلُّ من اعتدى على أيٍّ من المبادئ أو القيم الأسرية Principes ou valeurs de la famille في المجتمع المصري أو انتهك حرمة الحياة الخاصة، أو أرسل بكثافة العديد من الرسائل الإلكترونية لشخص معين دون موافقته، أو منح بيانات شخصية إلى نظام أو موقع إلكتروني لترويج السلع أو الخدمات Pour promouvoir des biens ou des services دون موافقته، أو نشر عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات معلومات أو أخبارًا أو صورًا وما في حكمها تنتهك خصوصية أي شخص دون رضاه، سواء كانت المعلومات المنشورة Informations publiées صحيحة أو غير صحيحة".

ونص في المادة (٢٥) من ذات القانون على أنه "يُعاقب بالحبس مدةً لا تقل عن سنتين ولا تجاوز خمس سنوات، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز ثلاثمائة ألف جنيه، أو بإحدى هاتين العقوبتين، كلُّ من تعمَّد استعمال برنامج معلوماتي أو تقنية معلوماتية في معالجة معطيات شخصية Technologie de l'information dans le traitement des données personnelles للغير لربطها بمحتوى منافٍ للآداب العامة، أو لإظهارها بطريقة من شأنها المساس باعتباره أو شرفه". ويذهب أيضًا –المشرع المصري– في قانون العقوبات من خلال نص المادة (٣٠٩) مكررًا (أ)[٢] إلى القول بأنه "يُعاقب بالحبس كلُّ من أذاع أو سهَّل إذاعة أو استعمل ولو في غير علانية تسجيلًا أو مستندًا متحصَّلًا عليه بإحدى الطرق المبيَّنة بالمادة السابقة أو كان بغير رضاء صاحب الشأن، ويعاقب بالسجن مدة لا تزيد على خمس سنوات كلُّ من هدد بإفشاء أمر من الأمور التي تم التحصُّل عليها بإحدى الطرق

(١) راجع، المادة (٢٥) من القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات الصادر بتاريخ ٢٠١٨/٨/١٤م، والمنشور بالوقائع المصرية بالعدد (٣٢) مكررًا (ج) بتاريخ ٢٠١٨/٨/١٤م، والمعمول به من تاريخ ٢٠١٨/٨/١٥م.

(٢) راجع، قانون العقوبات المصري رقم ٥٨ لسنة ١٩٣٧ م، الصادر بتاريخ ١٩٣٧/٧/٣١م، والمنشور بالوقائع المصرية بالعدد (٧١)، بتاريخ ١٩٣٧/٨/٥م، والمعمول به بتاريخ ١٩٣٧/١٠/١٥م، وتعديلاته.

المشار إليها لحمل شخص على القيام بعمل أو الامتناع عنه، ويعاقب بالسجن الموظف العام الذي يرتكب أحد الأفعال المبينة بهذه المادة اعتمادًا على سلطة وظيفته، ويحكم في جميع الأحوال بمصادرة الأجهزة وغيرها مما يكون قد استخدم في الجريمة أو تحصل عنها، كما يحكم بمحو التسجيلات المتحصلة عن الجريمة أو إعدامها". من هذه النصوص نستطيع أن نستخلص صور السلوك الإجرامي المكون للركن المادي لجريمة انتهاك حرمة الحياة الخاصة، والتي تتمثل في نشر أخبار[١] أو صور أو تعليقات تتصل بأسرار الحياة الخاصة أو العائلية، حتى ولو كانت هذه الأخبار والصور والتعليقات Actualités, Photos, avis صحيحة لكونها تتصل بأسرار الحياة الخاصة ودون رضاء المجني عليه.

**والصورة الثانية** من صور السلوك الإجرامي لجريمة انتهاك حرمة الحياة الخاصة هي فعل التقاط أو نقل صور شخص في مكان خاص من شأنها المساس باعتباره وشرفه، والمقصور بالالتقاط تثبيت الصورة على مكان يُعدُّ حساسًا لدى المجني عليه، وذلك في مكان خاص وليس عامًّا، ونقلها أو حيازتها على جهاز؛ وذلك دون رضاء المجني عليه. **والصورة الثالثة** تعمد استعمال برنامج معلوماتي أو تقنية معلوماتية في معالجة معطيات شخصية للغير لربطها بمحتوى منافٍ للآداب العامة؛ وذلك بطريقة خبيثة De manière malveillante لإيهام الغير بأن هذا الشخص يفتقد للشرف ويمارس أفعالًا مشينه يرفضها المجتمع.

**والصورة الرابعة** تتمثل في كلِّ اعتداء على أيٍّ من المبادئ أو القيم الأسرية في المجتمع المصري، أو انتهاك لحرمة الحياة الخاصة، أو إرسال بكثافة للعديد من الرسائل الإلكترونية لشخص معيَّن دون موافقته à son insu /Sans son consentement. **والصورة الخامسة** وهي استراق السمع؛ وهو الاستماع سرًّا لمحادثات متبادلة عن طريق أجهزة الاتصال والمحادثات Appareils de communication et conversations صادر من شخص ما أو متبادل بين شخصين مختلفين أو أكثر دون رضاء أيٍّ منهم، وأن يتم هذا الاستراق في الأحوال غير المصرح بها قانونًا.

---

(١) يقصد بالنشر: تمكين عدد غير محدد من الناس من العلم والاطلاع على فحوى الخبر أو الصور أو تعليقات تتصل بالحياة الخاصة أو الأسرية للمجني عليه، ويستوي أن يكون النشر بأي وسيلة من الوسائل.

أما الركن المعنوي لجريمة انتهاك حرمة الحياة الخاصة فيتمثَّل في الإرادة المكوِّنة للسلوك الإجرامي والعلم بكافة العناصر التي تكون الجريمة، وهي –أي انتهاك حرمة الحياة الخاصة– جريمة عمدية؛ لذلك يتطلب لعقاب الجاني أن يعلم بالصفة الخاصة للمكان والأخبار والصور التي يقوم بنشرها، وأنها تمس الحياة الخاصة للمجني عليه، فضلًا عن اتجاه إرادة الجاني إلى ارتكاب الفعل المُجرم والنتيجة الإجرامية Le résultat criminel[١].

**خلاصة الموضوع** أنَّ جريمة انتهاك حرمة الحياة الخاصة أحاطها المشرع المصري بمزيد عناية؛ نظرًا للمصلحة المعتدى عليها –القيم الأسرية والأخلاقية في المجتمع المصري، والشرف والاعتبار، والنظام العام والآداب العامة–، وقرر المشرع المصري جزاءً يكفل الردع بنوعيه –الخاص والعام– للجاني والمجتمع، ونصَّ على ركنين مكونين لها بما يستوجب معاقبة مرتكبها؛ وهما الركن المادي المتمثل في السلوك الإجرامي، والركن المعنوي Comportement criminel et élément moral وهو العمد واتجاه إرادة الجاني لارتكاب الفعل المؤثَّم، وتحقيق النتيجة وهو إلحاق الضرر بالمجني عليه وأسرته.

ومن زاوية أخيرة قرَّر المشرع المصري في مواد قانون العقوبات عقوبةً أصلية؛ وهي الحبس أو الغرامة أو كليهما، وعقوبة تكميلية؛ تتمثل في المصادرة للأجهزة المستخدمة في ارتكاب الجريمة Dispositifs utilisés dans la commission du crime ومحو البيانات والمعلومات Effacement de données et d'informations التي كانت محلًّا للجريمة.

## الفرع الثاني
## جريمة التحرش الجنسي الإلكتروني

يُعدُّ التحرش الجنسي Harcèlement sexuel من النقائص التي تجعل صاحبها ينحدر إلى قاع المبادئ الأخلاقية، بل يُعدُّ قتلًا للضمائر والسلوك القويم للإنسان السوي. فيذهب رأي

(١) راجع قريبًا من هذا المعنى، **فضل الله محمد الحسن فضل الله:** جريمة انتهاك حرمة الحياة الخاصة في التشريع الإماراتي، دراسة تحليلية، مركز جيل البحث العلمي، مجلة جيل الأبحاث القانونية المعمقة، العدد (٤٤)، نوفمبر ٢٠٢٠م، ص٤٨.

في الفقه[١] إلى تعريف التحرش الجنسي على أنه: "ذلك السلوك الذي يتعرَّض له الضحية، ويكون ذا طابع جنسيٍّ لا ترغب فيه ولا تُرحب به".

ويذهب رأي آخر في الفقه[٢] إلى القول بأن جريمة التحرش الجنسي يمكن تعريفها على أنها: "الفعل الذي يقع من خلال التعسف في استعمال السلطة باستخدام الأوامر والتهديدات أو الإكراه Utilisation d'ordres, de menaces ou de coercition بغرض الحصول على منفعة أو امتيازات أو مزايا ذات طبيعة جنسية Dans le but d'obtenir un avantage, des privilèges ou des avantages de nature sexuelle.

ويضيف هذا الرأي أنَّ الأصوات تعالت في الولايات المتحدة في أواخر السبعينيات من القرن الماضي لتجريم ظاهرة التحرش الجنسي وإقرار لوائح ونصوص خاصة بالتحرش الجنسي، واعتباره تمييزًا على أساس الجنس؛ لذلك قامت لجنة فرص التشغيل المتساوية بالولايات المتحدة الأمريكية بإقرار لوائح خاصة لمحاربة هذه الظاهرة.

ويذهب رأي آخر في الفقه[٣] لمحاولة تعريف جريمة التحرش الجنسي على أنه "سلوك مخالف للقانون يستهدف به الجاني تحقيق غرضٍ جنسيٍّ من الضحية".

ويذهب رأي في الفقه[٤] إلى تعريف التحرش الجنسي على أنه: "ذلك السلوك المتمثل بالقول أو الفعل أو الإشارة الصادرة من الجاني اتجاه المجني عليه، ذكرًا كان أم أنثي، والذي يشكل خدشًا للحياء العرضي للمجني عليه أو عليها، ويحمل في طياته دلالة جنسية واضحة".

---

(١) راجع في هذا التعريف، **عبد الرحمن محمد العيسوي:** سبل مكافحة الجريمة، دار الفكر الجامعي، ٢٠٠٦م، ص٢٠٠.

(٢) راجع في هذا التعريف، **السيد عتيق:** جريمة التحرش الجنسي، دراسة جنائية مقارنة، القاهرة، دار النهضة العربية، ٢٠٠٣م، ص١٥٥، ص٩١.

(٣) راجع، **محمد جبر السيد عبد الله جميل:** جريمة التحرش الجنسي وعقوبتها في التشريع الإسلامي والقانون، دراسة مقارنة، الطبعة الأولى، بيروت، دار الكتب العلمية، ٢٠١٩م، ص٤٢، وما بعدها.

(٤) راجع في هذا التعريف، **عادل يوسف عبد النبي الشكري، وآخرين:** الحماية الجزائية للأفراد في جريمة التحرش الجنسي، دراسة مقارنة، المجلد (١٣)، العدد (٤٤)، ٢٠٢٠م، ص١٠١.

والحقيقة أنَّ الجاني قد يتمثل سلوكه في ارتكاب أفعالِ تتبُّعٍ وملاحقة، سواء بالألفاظ المباشرة أو غير المباشرة الجنسية أو الخادشة للحياء عبر الهاتف أو الإنترنت أو ما يستجد من وسائل، أو بإرسال رسائل تحمل صورًا أو نصوصًا أو نقوشًا جنسية Moyens ou en envoyant des messages avec des images, des textes ou des inscriptions à caractère sexuel.

وهو ما ذهب إليه المشرع المصري من خلال نص المادة (٣٠٦ مكررًا أ)[١] على أنْ "يُعاقب بالحبس مدةً لا تقل عن سنتين ولا تجاوز أربع سنوات، وبغرامة لا تقل عن مائة ألف جنيه ولا تزيد عن مائتي ألف جنيه، أو بإحدى هاتين العقوبتين، كلُّ من تعرَّض للغير في مكان عام أو خاص أو مطروق بإتيان أمور أو إيحاءات أو تلميحات جنسية أو إباحية، سواء بالإشارة أو بالقول أو بالفعل بأية وسيلة، بما في ذلك وسائل الاتصالات السلكية أو اللاسلكية أو الإلكترونية، أو أية وسيلة تقنية أخرى، وتكون العقوبة الحبس مدة لا تقل عن ثلاث سنوات ولا تجاوز خمس سنوات، وبغرامة لا تقل عن مائتي ألف جنيه ولا تزيد على ثلاثمائة ألف جنيه، أو بإحدى هاتين العقوبتين، إذا تكرَّر الفعل من الجاني من خلال الملاحقة والتتبع للمجني عليه، وفي حالة العود تضاعف عقوبتا الحبس والغرامة في حديهما الأدنى والأقصى".

وجدير بالذِّكر أنَّ المشرع المصري في قانون العقوبات من خلال المادة (١/٣٠٦ مكررًا ب) شدَّد على عقاب المتحرش بنصه على أنه: "يُعدُّ تحرشًا جنسيًّا إذا ارتُكبت الجريمة المنصوص عليها في المادة (٣٠٦ مكررًا أ) من هذا القانون بقصد حصول الجاني من المجني عليه على منفعة ذات طبيعة جنسية، ويعاقب الجاني بالسجن مدة لا تقل عن خمس سنوات ...".

والحقيقة أنَّ المشرع من خلال الفقرة الثانية من المادة (٣٠٦ مكررًا ب) قد شدَّد العقوبة إذا صدرت من شخص له على المجني عليه ولاية أو سلطة معنوية؛ كالرئيس في العمل، أو سلطة أبوية أو أسرية أو دراسية، وذلك بقوله: "... فإذا كان الجاني ممن نُصَّ عليهم في الفقرة الثانية من المادة (٢٦٧) من هذا القانون أو كانت له سلطة وظيفية أو أسرية أو دراسية Autorité de carrière, de famille ou d'études على المجني عليه أو مارس عليه أي

(١) راجع المادة (٣٠٦ أ مكررًا) من قانون العقوبات، والمعدلة بتاريخ ٢٠٢١/٨/١٥م.

ضغط تسمح له الظروف بممارسته عليه، أو ارتكبت الجريمة من شخصين فأكثر أو كان أحدهم على الأقل يحمل سلاحًا، تكون العقوبة السجن مدة لا تقل عن سبع سنوات".

والحقيقة أننا نرى أنه يُعدُّ تحرشًا جنسيًّا كل إمعان في مضايقة المجني عليه بتكرار أفعال أو أقوال أو إشارات من شأنها أن تخدش حياءه بقصد حمله على الاستجابة لرغباته أو رغبات غيره الجنسية، وخصوصًا إذا حمل الجاني سلاحًا، أو إذا كان المجني عليه طفلًا لم يكمل (١٨) الثامنة عشر من عمره، أو كان الجاني من أصول المجني عليه أو من محارمه، أو من المتولين تربيته أو رعايته، أو ممن لهم سلطة عليه، أو كان خادمًا عنده أو عند من تقدَّم ذكرهم".

ويبدو لنا أنَّ جريمة التحرش الجنسي لا تتطلَّب وجود الجاني والمجني عليه في مكان واحد، فالتكنولوجيا الحديثة عندما تُبرز وجهها القبيح تأتي بما لا يُحمد عقباه. فالتحرش الجنسي الإلكتروني Harcèlement sexuel en ligne يقع عبر وسائل إلكترونية ووسائل التواصل، في توجيه الرسائل التي تحتوي على مواد تُسبِّب الإزعاج للمتلقي، سواء أكانت هذه المواد تلميحًا بالرغبة في التعرف على المتلقي لأهداف جنسية، أو كانت تحتوي على عبارات أو شتائم جنسية أو صورًا أو مشاهد فيديو جنسية Phrases ou insultes à caractère sexuel, images ou scènes vidéo à caractère sexuel عبر وسائل التواصل الإلكتروني المختلفة Par divers moyens de communication électroniques.

وجدير بالذِّكر أنَّ توجيه العبارات أو الشتائم الجنسية Phrases ou insultes à caractère sexuel يتم بواسطة القول، الذي يُعرَّف بأنه: الصوت الذي خرج من الفم في صورة كلمات أو ألفاظ جنسية للتعبير عن معني معين، ويمثل القول أداة التعبير الشفوية التي تُترجِم أحاسيس وأفكار الفرد إلى كلمات تخاطب حاسة السمع لدى الآخرين(١).

والإشارة تُعدُّ من وسائل التعبير عن الفكرة الشفوية Moyens d'expression de l'idée orale، وهي: ما اصطلح على التعبير بها عن المعاني والشعور من حركات الجوارح

(١) راجع، **جميل عبد الباقي الصغير**: الإنترنت والقانون الجنائي، الأحكام الموضوعية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، ٢٠٠١م، ص٨٨.

وأجزاء الجسم، والتي تُستنتج من الظروف المحيطة بالواقعة[١]. والفعل يُقصَد به: كلُّ مظهر تنفيذي لإرادة الإنسان والتعبير عمَّا يجول بخاطره من أفكار، ويعتمد هذا المظهر على أعضاء الجسم ووضعه، أو بمعنى آخر: هو كلُّ حركة عضوية إرادية أو إشارة يفصح بها مرتكبها عن معنى معين[٢].

والحقيقة أنَّ هذه الجريمة لا يُشترَط فيها أن يكون الجاني والمجني عليه في مكان واحد أو دولة واحدة، كما أنَّ المجتمع المعلوماتي مجتمع منفتح عبر شبكات تخترق الزمان والمكان دون أن تخضع لأي رقابة. بل إنَّ هذه الجريمة تتسم بأنها تُرتكَب في الخفاء في أغلب الأحيان، ولا وجود لأي أثر كتابي أو مادي ملموس يدل على ارتكاب جريمة التحرش الجنسي عبر الوسائط الإلكترونية بحكم أنها تقع في بيئة افتراضية، كما أنها تتميز بسهولة إخفاء هوية الجاني على شبكة الإنترنت.

وجدير بالذِّكر أنَّ هذه الجريمة تفترض صدور فعل مادي من الجاني؛ لأن القانون لا يعاقب على مجرد الأفكار والنوايا حبيسة الضمير الإنساني مهما كانت خبيثة وخسيسة ولئيمة ما لم تُترجَم هذه النوايا الإجرامية Intentions criminelles إلى أفعال موجودة في الواقع. ويتمثَّل الركن المادي لجريمة التحرش عمومًا في قيام الجاني بارتكاب الأفعال التي يجرمها القانون؛ باعتبارها جريمة جنسية ماسةً بالعِرض أو مشاعر الحياء، سواء أكان فاعلًا أصليًّا فيها، وذلك بقيامه بالأفعال التنفيذية، أم بوصفه شريكًا سواء بالتحريض أو الاتفاق أو المساعدة[٣]. والركن المادي لجريمة التحرش الجنسي عبر الوسائط الإلكترونية يتمثَّل في توجيه

---

(١) راجع، **محمد بن حميد بن مضحي المزمومي:** جريمة التحرش الجنسي في النظام السعودي، دراسة مقارنة، مجلة العلوم القانونية والاقتصادية، كلية الحقوق، جامعة عين شمس، القاهرة، المجلد (٦١)، العدد (٢)، ٢٠١٩م، ص١٠٤٢.

(٢) راجع، **طارق سرور:** قانون العقوبات القسم الخاص، جرائم الاعتداء على الأشخاص، دار النهضة العربية، ٢٠٠٣م، ص٣٢٦.

(٣) راجع، **مريم العوني:** جريمة التحرش الجنسي في القانون، رسالة ماجستير، كلية العلوم القانونية والاقتصادية والاجتماعية، جامعة القاضي رياض بمراكش، المغرب، ٢٠١٥م، ص٤٥.

رسائل مكتوبة أو هاتفية أو تسجيلات أو صور ذات طبيعة جنسية أو لأغراض جنسية، والوسائل المذكورة تعتبر دلائل قوية يمكن الاعتماد عليها في إثبات هذه الجريمة.

بيد أنه لا يكفي للمساءلة على نشاط إجرامي Activité criminelle أن يقوم الفاعل أو الجاني بنشاط مادي فقط، بل لا بدَّ من توافر الركن المعنوي، ويتمثل في القصد والعمد الجنائي؛ تحقيق الرغبات الجنسية Accomplissement des désirs sexuels، أو الحصول على رغبات ذي طابع جنسي Désirs de nature sexuelle.

ولذلك لا بدَّ أن تتوفر في الجاني إرادة تحقيق هذا الفعل، ثم العلم بأن الواقعة مجرمة، ويتحقق الركن المعنوي بمجرد توجيه هذه الرسائل؛ ذلك أن جريمة التحرش الجنسي عبر الوسائط الإلكترونية هي من الجرائم العمدية يُشترَط لقيامها ركنٌ معنويٌّ يتمثَّل في القصد الجنائي Intention criminelle الذي يقوم على عنصري العلم والإرادة؛ وهو القصد العام، إضافة إلى القصد الجنائي الخاص المتمثل في الحصول على رغبات ذات طابع جنسي.

والحقيقة أنَّ إثبات الركن المعنوي لجريمة التحرش الجنسي عبر الوسائط الإلكترونية de harcèlement sexuel par les médias électroniques من خلال تحديد الأفعال الموصوفة بالتحرش، وبلوغ الجاني لنتيجته الإجرامية المقصودة المتمثلة في تلبية رغبات جنسية أو الوصول إلى هدف جنسي، يُعدُّ من الصعوبة بمكان، ويستعصي في غالب الأحيان، ما عدا الأفعال الموصوفة بالتحرش التي تحمل دلالة واضحة لا لبس فيها؛ كإرسال عبارات أو صور جنسية للضحية قصد الحصول على نزوات جنسية.

## الفرع الثالث

## جريمتا السبِّ والقذف الإلكتروني

تُعدُّ جريمة السب والقذف والتهديد بإفشاء الأسرار من الجرائم الواقعة على حرمة الحياة الخاصة، وهذه الجرائم تؤثر على سمعة الإنسان وشرفه، وخاصة إذا تناولت الإناث؛ حيث قد يؤدي الأمر إلى فقدان حياتهم، خاصة في المجتمعات التي يسودها الجهل وعدم الإيمان بالسلطة القضائية في إيصال كلِّ ذي حقٍّ حقَّه. ونقول: إنَّ انتشار هذه الجرائم واسع وسريع،

خاصةً عند المواقف الاستفزازية Positions provocantes التي تحدث بشكل يومي مع الكثير من البشر، وخاصة في الأماكن المكتظة سكانيًّا، وهي كثيرة الحدوث على مواقع التواصل الاجتماعي. وجدير بالذِّكر أنَّ جريمة القذف بالوسائط الإلكترونية تختلف في الغالب عن جريمة القذف التقليدية Le délit traditionnel de diffamation استنادًا للقواعد العامة؛ وذلك لاختلاف وسيلة ارتكابها[١][٢].

ويذهب رأي في الفقه[٣] إلى تعريف جريمة القذف بأنَّها: "إسناد واقعة في مكان عام أو على مسمع ومرأى من شخص آخر غير المجني عليه تستوجب عقابَ من تُنسب إليه أو تؤذي سُمعته". ويذهب رأي آخر في الفقه[٤] إلى تعريف جريمة القذف المعلوماتي على أنها: "إسناد واقعة معيَّنة Attribution d'un fait إلى الغير بإحدى الوسائل المعلوماتية، من شأنها لو كانت صادقة لأوجبت عقابَ من أُسندت إليه أو احتقاره عند أهل وطنه. وعرف المشرع من خلال نص المادة (٣٠٢) من قانون العقوبات[٥] القذف على أنه: "يُعدُّ قاذفًا كلُّ من أسند لغيره بواسطة إحدى الطرق المبينة بالمادة (١٧١) من هذا القانون أمورًا لو كانت صادقة لأوجبت عقاب من أسندت إليه بالعقوبات المقررة لذلك قانونًا أو أوجبت احتقاره عند أهل وطنه، ومع ذلك فالطعن في أعمال موظف عام أو شخص ذي صفة نيابية عامة أو مكلف بخدمة عامة لا يدخل تحت حكم الفقرة السابقة إذا حصل بسلامة نية de bonne foi وكان لا يتعدَّى أعمال

---

(١) راجع، **ميثاء إسحاق عبد الرحيم الشيباني:** المسؤولية الجزائية عن جريمتي السب والقذف بالوسائل الإلكترونية، طبقًا للمرسوم رقم (٥) لسنة ٢٠١٢م، بشأن قانون مكافحة جرائم تقنية المعلومات، رسالة ماجستير، كلية القانون جامعة الإمارات العربية المتحدة، ٢٠١٨م، ص٨.

(٢) راجع، المحكمة الاقتصادية في الدعوى رقم ٦٩٠ لسنة ٢٠١٢ قضائية، الصادر بجلسة ٢٠١٢/١١/٢٤م، متاح عبر الموقع الإلكتروني التالي: https://www.eastlaws.com، وقت الاطلاع: ٢٠٢٣/٤/١٥م، الساعة ٤م.

(٣) راجع في هذا التعريف، **هيا محمد عبد الله محمد الحميدي:** جريمتا القذف والسب الإلكتروني في القانون القطري، دراسة تحليلية مقارنة، رسالة ماجستير، كلية القانون جامعة قطر، ٢٠٢١م، ص١١.

(٤) راجع في هذا التعريف، **عمار عباس الحسيني:** جرائم الحاسوب والإنترنت، الجرائم المعلوماتية، الطبعة الأولى، الناشر مكتبة زين الحقوقية والأدبية، لبنان، ٢٠١٧م، ص٣٨٠.

(٥) راجع المادة (٣٠٢) من قانون العقوبات، والمعدلة بتاريخ ٢٠٠٦/٧/١٥م.

الوظيفة أو النيابة أو الخدمة العامة، وبشرط أن يثبت المتهم حقيقة كلِّ فعل أسنده إلى المجني عليه، ولسلطة التحقيق أو المحكمة، بحسب الأحوال، أنْ تأمر بإلزام الجهات الإدارية بتقديم ما لديها من أوراق أو مستندات معزِّزة لما يقدمه المتهم من أدلة لإثبات حقيقة تلك الأفعال، ولا يقبل من القاذف إقامة الدليل لإثبات ما قذف به إلا في الحالة المبينة بالفقرة السابقة".

ومن زاوية أخرى قرَّر المشرع المصري من خلال نص المادة (٣٠٦) من قانون العقوبات أنَّ: "كلَّ سبٍّ لا يشتمل على إسناد واقعة معينة بل يتضمن بأي وجه من الوجوه خدشًا للشرف أو الاعتبار يُعاقَب عليه في الأحوال المبينة بالمادة (١٧١) بغرامة لا تقل عن ألفي جنيه ولا تزيد على عشرة آلاف جنيه". وجدير بالذكر أنَّ المشرع من خلال نص المادة (٣٠٦ مكررًا أ) من قانون العقوبات[١] قد شدَّد العقوبة بالنسبة للسب في حالة العود بقوله بأنه: "يُعاقب بالحبس مدةً لا تقل عن سنتين ولا تجاوز أربع سنوات، وبغرامة لا تقل عن مائة ألف جنيه ولا تزيد عن مائتي ألف جنيه، أو بإحدى هاتين العقوبتين، كلُّ من تعرَّض للغير في مكان عام أو خاص أو مطروق بإتيان أمور أو إيحاءات أو تلميحات جنسية أو إباحية Propos, insinuations ou allusions à caractère sexuel ou pornographique سواء بالإشارة أو بالقول أو بالفعل بأية وسيلة، بما في ذلك وسائل الاتصالات السلكية أو اللاسلكية أو الإلكترونية communications et télécommunications életroniques، أو أية وسيلة تقنية أخرى، وتكون العقوبة الحبس مدة لا تقل عن ثلاث سنوات ولا تجاوز خمس سنوات، وبغرامة لا تقل عن مائتي ألف جنيه ولا تزيد على ثلاثمائة ألف جنيه، أو بإحدى هاتين العقوبتين إذا تكرر الفعل من الجاني من خلال الملاحقة والتتبع للمجني عليه، وفي حالة العود تُضاعف عقوبتا الحبس والغرامة في حدَّيْهما الأدنى والأقصى".

ويمكننا استخلاص عناصر الركن المادي لجريمة السب في السلوك الإجرامي، والنتيجة الإجرامية، وعلاقة السببية بين السلوك والنتيجة le lien de causalité entre le comportement et le résultat.

(١) راجع المادة (٣٠٦ مكررًا أ) من قانون العقوبات، والمعدلة بتاريخ ٢٠٢١/٨/١٥م.

فالسلوك الإجرامي والمتمثل في النشاط الإجرامي يبدأ بالرمي بما يخدش الشرف والاعتبار، الذي يمكن أن ينشأ بكافة الطرق والوسائل؛ حيث إنَّ المشرع المصري لم يشر إلى طريقة محدَّدة لذلك، وإنما ترك المسألة على إطلاقها؛ إذ يمكن أن يكون بصورة القول أو الكتابة أو الرسم أو الإشارة، ويستوي أن يكون الرمي بما يخدش الشرف والاعتبار صريحًا أو ضمنيًّا.

لذلك نقول: إنَّ القول أو الصياح، والفعل أو الإيماء، والكتابة أو الرسوم أو الصور، وغيرها من طرق التعبير الأخرى يمكن أن تُكوِّن الركن المادي لجريمة القذف. إن الفعل المادي المكوِّن لجريمة السبِّ العلني عبر الإنترنت هو الفعل ذاته المكوِّن لجريمة القذف، والذي يتمثَّل في تعبير يتخذ العلانية وسيلةً له، ولا تختلف الجريمتان إلَّا من حيث موضوع هذا التعبير، فموضوع التعبير في جريمة القذف عبر الإنترنت diffamation sur Internet يتمثل في واقعة توجب العقاب أو الاحتقار، أمَّا التعبير في جريمة السب العلني عبر الإنترنت le délit d'insulte publique via Internet فهو ليس واقعةً، بل خدشًا للشرف أو الاعتبار.

ومعنى ذلك أنَّ القاذف يبوح علنًا بواقعة يعرفها أو يزعم معرفتها، أما من يرتكب جريمة السب العلني عبر الإنترنت فإنَّه يبوح علنًا بأمور لا تصدق وصف الوقائع qualification des faits، ولا يمكن إرجاعها إلى دائرة المعرفة، وإنما إلى دائرة الشعور؛ أي ليست من قبيل ما يعرفه المرء، وإنما هي من قبيل ما يشعر به، فليس كلُّ تعبير عن شعور عدائي عبر الإنترنت Sentiment d'hostilité en ligne يعتبر سبًّا علنًا[١]. لذلك نقول إنَّ السب هو خدش شرف شخص أو اعتباره وعدًا بإلصاق صفة عيب أو لفظ خارج أو مُشين إليه؛ لذلك يُعدُّ من قبيل السب القول عن الشخص بأنه لصٌّ ونصاب ومزور وعربيد وعاهر.

---

(١) راجع، **هيا محمد عبد الله محمد الحميدي:** جريمتا القذف والسب الإلكتروني في القانون القطري، دراسة تحليلية مقارنة، رسالة ماجستير، مرجع سابق، ص٣٨، راجع أيضًا، **عبد السلام عليلي:** جريمة القذف عبر مواقع التواصل الاجتماعي، دراسة تحليلية مقارنة بين التشريع الجزائري والتشريعات الأجنبية والعربية، مجلة الدراسات القانونية والاقتصادية، المجلد (٥)، العدد (٢)، ٢٠٢٢م، ص٥٨١.

ومن زاوية أخرى ذهبت محكمة النقض المصرية[١] إلى إقرارها الحق في إقامة الدعوى "السب والقذف" لأي شخص غير المجني عليه طالما ألحقه ضرر، وذلك بقولها: "... وكان من المقرر أنه ليس في القانون ما يمنع أن يكون المضرور من الجريمة شخص آخر غير المجني عليه ما دام قد ثبت قيام هذا الضرر وكان ناتجًا عن الجريمة مباشرة، وكانت المدعية بالحق المدني الأولى قد أقامت دعواها بصفتها مضرورة من عبارات السب والقذف التي وجهتها الطاعنة إليها من خلال الرسالة الصوتية المرسلة عبر تطبيق الواتس أب على هاتف زوجها –المدعي بالحق المدني الثاني la deuxième partie civile–، فإن ما تثيره الطاعنة في هذا الخصوص يضحى لا محلَّ له ...".

وجدير بالذكر أنَّ المشرع من خلال نص المادة (٧٦) من قانون تنظيم الاتصالات[٢] قرَّر أنه "مع عدم الإخلال بالحق في التعويض المناسب يُعاقب بالحبس وبغرامة لا تقل عن خمسمائة جنيه ولا تجاوز عشرين ألف جنيه أو بإحدى هاتين العقوبتين كلُّ من: استخدم أو ساعد على استخدام وسائل غير مشروعة لإجراء اتصالات Moyens illégaux d'établir des contacts، تعمد إزعاج أو مضايقة غيره بإساءة استعمال أجهزة الاتصالات Utilisation abusive des appareils de communication".

وجدير بالذِّكر أنَّ الركن المعنوي الذي يمكن تعريفة بأنه: المسك الذهني أو النفسي للجاني باعتباره محورًا للقانون الجنائي، الذي يحدد القاضي فيه نية الجاني اتجاه ارتكاب جريمة القذف وذلك لتقدير مدى خطورته والعقاب الذي يستحقه لإصلاحه أن أمكن؛ لذلك لا بدَّ من توافر العلم والإرادة لدى الجاني، لأن جريمة القذف جريمة عمدية infraction intentionnelle، تتطلَّب لمعاقبة الجاني القصد بارتكاب سلوك إجرامي Comportement

(١) راجع حكم محكمة النقض –جنائي– في الطعن رقم ١١٤٤٨ لسنة ٩٠ قضائية –جنح اقتصادي–، الصادر بجلسة ١٤/ ٣/ ٢٠٢١م .

(٢) راجع قانون تنظيم الاتصالات رقم ١٠ لسنة ٢٠٠٣م، الصادر بتاريخ ٢٠٠٣/٢/٤م، والمنشور بالجريدة الرسمية بالعدد رقم (٥) مكررًا (أ)، بتاريخ ٢٠٠٣/٢/٤م، والمعمول به اعتبارًا من ٢٠٠٣/٢/٥م.

criminel ومعرفةً بأن هذا السلوك يُشكِّل جريمة القذف، وأن تتجه إرادة الجاني برمي المجني عليه بالعبارات المشينة، ويستوي أن يكون الرمي بأي وسيلة(١).

## المطلب الثاني
## جرائم تقع على الأموال

بداية نشير إلى أنَّ المعلومات التي تُعالج آليًّا، وتأخذ حكمها البيانات المخزنة سواء في برامج الحاسوب أو في ذاكرته، تدخل ضمن الأموال؛ وبالتالي تتمتع بالحماية الجنائية المقررة.

والحقيقة أنَّ أغلب الجرائم التي تقع على الأموال تتسم بدهاء الجاني الشديد بعكس الجرائم الإلكترونية الواقعة على الأشخاص، التي غالبًا ما يكون المجرم لدية ثغرة أو معاناة في شخصيته أو مسلكًا نفسيًّا خاطئًا اعتاد على ارتكابه. ولا يخفى على كلِّ ذي لب انتشار الجرائم الواقعة على الأموال في الآونة الأخيرة؛ بسبب امتهان البعض وتمرُّسه في تعلم اختراق الأجهزة والحسابات بقصد الحصول على الأموال Obtention de fonds. وتتمثَّل الجرائم الواقعة على الأموال في الاحتيال باستعمال طرق وهمية Utiliser des méthodes fictives لاصطياد الحسابات ضعيفة التأمين، واستغلال ثغرات تركها المبرمج أو النظام الإلكتروني، وأيضًا جريمة السرقة المعلوماتية Le crime de vol d'informations.

(١) راجع، **محمد ممدوح بدير**: مكافحة الجريمة المعلوماتية عبر شبكة الإنترنت والاستدلال كوسيلة لإثبات الجريمة المرتكبة عبر الإنترنت، دراسة مقارنة، مركز الدراسات العربية، الطبعة الأولى، ٢٠١٩م، ص١٠٠.

## الفرع الأول
## جريمة الاحتيال الإلكتروني

لعلَّ الظروف الاقتصادية التي يمر بها العالم تكون السبب المعروف لدينا في ازدياد وتيرة ارتكاب الجريمة المعلوماتية، بالإضافة لأزمة الضمير Pour la crise de conscience التي تعيشها المجتمعات؛ الأمر الذي يُنبئ بانهيار لأركان الدولة في محورها الأساسي وهو الفرد. ونظرًا لترسُّخ فكرة جني المال السريع لدى البعض من مرتكبي هذه الجرائم المعلوماتية يلجأ المجرم إلى استخدام احتيال إلكتروني، عن طريق استعمال طرق احتيالية Méthodes frauduleuses، مستعينًا باسم كاذب أو منتحلًا صفة على غير الحقيقة بغرض الحصول على مال منقول أو منفعة؛ كالاختلاس وسرقة الأموال détournement de fonds عن طريق الحصول على البيانات الشخصية، مثل رقم الحساب والبطاقات المصرفية ، لذلك يذهب رأي في الفقه[١] إلى القول بأن الطرق الاحتيالية Méthodes frauduleuses هي: "ادعاءات كاذبة تدعمها مظاهر كاذبة أو أعمال خارجية، من شأنها حمل المجني عليه للتصديق وتسليم المال".

وجدير بالذكر أنَّ الجريمة المعلوماتية تتصف من حيث طبيعتها بأنَّ لها بُعدًا ماديًّا يتمثل في السيطرة على مال الغير، وهو ما يمثل الركن المادي للجريمة L'élément matériel du crime، وبُعدًا نفسيًّا يتمثَّل في الإيهام والخداع والغش الذي يقوم به الجاني للسيطرة على عقل وفكر المجني عليه، أو بمعنى آخر تشويه الحقيقة في ذهن المجني عليه يدفعه لقبول تصرفات يكون من شأنها إلحاق أضرار وخسائر مادية؛ لذلك قيل –وبحق– بأن الجريمة المعلوماتية "جريمة عمدية ذات طابع ذهني"[٢].

أمَّا فيما يتعلق بمحلِّ الجريمة فيتمثَّل في المعلومات التي يُغيِّرها ويحرفها الجاني باستخدام طرق احتيالية، أبرزها الخداع والغش، باستخدام مجموعة من المفاتيح والشفرات المعقدة التي

---

(١) راجع في هذا التعريف، **رمسيس بهنام:** القسم الخاص في قانون العقوبات، دار المعارف، الإسكندرية، ١٩٨٢م، ص٥٠٧.

(٢) راجع، **نسرين محسن نعمة:** جريمة الاحتيال المعلوماتي، دراسة مقارنة، بحث منشور بمجلة الكوفة للعلوم القانونية والسياسية، كلية القانون، جامعة الكوفة، المجلد ١١، العدد ٣٦، ٢٠١٨م، ص٢٨٦.

تتسم بتكنولوجيا عالية الدقة والتداخل، هذا بخصوص القيم المالية، وقد تُرتكب الجريمة المعلوماتية، ويتم الاعتداء على قيمٍ معنوية غير ملموسة بالتلاعب بالأرصدة البنكية والحسابات Manipulation des soldes et des comptes bancaires ووسائل الدفع الإلكتروني Méthodes de paiement électronique حتى بعد تأمينها.

لذلك نجد رأيًا في الفقه يذهب إلى القول بأنَّ: الاحتيال filoutage تقنيةٌ عبر الإنترنت تهدف إلى الحصول على معلومات سرية (كلمة مرور ومعلومات مصرفية وما إلى ذلك) من أجل اغتصاب هوية الضحية usurpantion de l'identité de la victime". ويضيف أنَّ هذا المصطلح أتى من الجمع بين كلمتي الصيد phreaking، والاستخدام الاحتيالي لخطوط الهاتف utilisation frauduleuse des lignes téléphoniques[١].

إذن فالمجرم المعلوماتي شخص يتسم بالدهاء والقدرة على متابعة ثغرات وسائل الاتصالات وتكنولوجيا المعلومات بطريقة احترافية، وغالبًا ما يجيد التحدث بكثير من اللغات، وقد يكون شخصًا حدثَ له انهيار في أعماله التجارية أو خسران وظيفته في المؤسسة التي كان يعمل بها؛ وبالتالي يأتي ويخترق ويغش ويحتال على الأنظمة الإلكترونية لمجرد عقاب المجتمع أو مكان عمله السابق، أو حتى مجرد إثبات شيء خاص في أعماق نفسه وهو خاطئ. ومن زاوية أخرى نصَّت الاتفاقية الأوربية حول الجريمة الافتراضية "اتفاقية بودابست لعام ٢٠٠١م" من خلال المادة الثامنة[٢] منها على الاحتيال المرتبط بالحاسوب، بأنه يُعدُّ مرتكبًا لجريمة الاحتيال المعلوماتي Le crime de fraude informatique "كلُّ من يقوم بالتأثير في المعلومات المبرمجة عن طريق برمجة غير سليمة، أو عن طريق التدخل أثناء تطبيق البرنامج، أو عن طريق استعمال بيانات غير سليمة أو غير مكتملة Utilisation de données incorrectes ou incomplètes أو بأية طريقة أخرى؛ مما يترتَّب عليه حدوث

(1) Explication donnée par F. Duflot, « Phishing: les dessous de la contrefaçon », RLDI 2006/01, no 366, p. 54.

(٢) راجع نصوص اتفاقية بودابست، متاحة عبر الموقع الإلكتروني التالي:

WWW.CONVENTIONS.CO.INT، وقت الاطلاع ٢٠٢٣/٣/١م، الساعة ٥ ص.

أضرار لممتلكات الغير، على أن يكون ذلك بنية إثراء نفسه أو غيره بربح غير مشروع Profit illégal.

وجدير بالذكر أنَّ التحايل أو الغش المعلوماتي وفقًا للمادة (٢٦٣ – أ) من قانون العقوبات الألماني، فإنَّ "كلُّ من يُؤثر عمدًا على نتيجة مُعالجة البيانات بطريقة تُلحق الضرر بمُمتلكات الغير بقصد إثراء نفسه يكون مُعرضًا للمُلاحقة القضائية بتهمة الاحتيال المعلوماتي fraude informatique (بعقوبة الغرامة، أو بالسجن لمدة تصل إلى خمسة سنوات، والتي في الحالات الخطيرة بشكل خاص قد تصل إلى عشر سنوات)"[١]. وبالتالي، فإنَّ الأمر يتعلق بالتلاعب بالعمليات التقنية والفنية manipuler les processus techniques التي يتم فيها تحقيق نتائج عمل مُعينة من خلال تسجيل البيانات وربطها وفقًا لبرامج مُعينة.

**ومن ناحية أخرى**، يتم تسجيل ما يُسمَّى بالتلاعب بإدخال البيانات manipulation de saisie؛ أي الإدخال المُباشر أو غير المُباشر لبيانات غير صحيحة أو غير مُكتملة données incorrectes ou incomplètes، وكذلك الإدخال غير المُصَرَّح به للبيانات من قِبَل شخص غير مُصَرَح له.

**مما سبق نستخلص أنَّه** لقيام جريمة الاحتيال المعلوماتي لا بدَّ أن يقوم المجرم عن قصد وبدون وجه حق، وعلى نحو يسبب خسارة في ممتلكات الغير، بإدخال أو تعديل أو حذف أو كتم لبيانات الحاسوب، وبنية احتيال غير شريفة وبسوء نية بغرض الحصول دون وجه حق على منفعة اقتصادية لنفسه أو لغيره[٢]. ويذهب رأي في الفقه[٣] إلى ذكر أمثله كثيرة لطرق الاحتيال الإلكتروني؛ منها: أنه في الآونة الأخيرة، وعلى نطاق واسع، تلقى دافعو الضرائب

(1) Selon l'article 263a du code pénal, quiconque influence délibérément le résultat d'un traitement de données de manière à porter atteinte au bien d'autrui dans l'intention de s'enrichir est passible de poursuites pour fraude informatique (amende, d'emprisonnement pouvant aller jusqu'à cinq ans, dans les cas particulièrement graves jusqu'à dix ans).

(2 (Frédérique CHOPIN, Cybercriminalité, op. cit., § ٣٤, P. 27.

(3 (**Christiane Féral-Schuhl**, Praxis Cyberdroit, op. cit., p. 70 et s.

contribuables رسائل بريد إلكتروني يُزعَم أنها مُرسَلَة من قبل السلطات الضريبية "مصلحة الضرائب" l'administration fiscale، التي تُعلِن لهم عن استرداد ضرائب تبلغ بضع مئات

من اليورو، بشرط قيامهم بتأكيد التفاصيل والبيانات المصرفية coordonnées bancaires الخاصة بهم حتى يُمكن تنفيذ المُعاملة عن طريق التحويل المصرفي.

وكذلك، في ٧ نوفمبر ٢٠١٧، حذر موقع Service-public.fr مُستخدمي الإنترنت من إرسال رسائل بريد إلكتروني احتيالية l'envoi de mails frauduleux باستخدام شعاره، ودعوتهم لتنزيل نموذج "استمارة" للحصول في غضون ٢٤ ساعة على بطاقة V3 الحيوية الجديدة، ودعواتهم كذلك لإرسال نسخة من وثيقة هويتهم "بطاقة الهوية"، وكذلك إثبات العنوان "وثيقة إثبات محل الإقامة" justificatif de domicile. وفي الولايات المتحدة، في منتصف عام ٢٠١٣، استخدم مجموعة من المُخترقين يُعرفون باسم "FIN4" أساليب التصيد الاحتيالي méthodes de spear phishing لإرسال رسائل بريد إلكتروني بالتظاهُر بأنه مُحاور للشخص موثوق به من أجل الحصول على كلمات مرور؛ وبالتالي كان المُخترقون قادرين على الوصول إلى المعلومات من الأشخاص projet confidentiel d'acquisition واستخدامها. **ويضيف هذا الرأي:** أنه نتيجة لهذه الممارسات الاحتيالية وكثرتها تعاونت Microsoft في عام ٢٠١١ مع Cert-Lexsi و PayPal لتطوير جهاز يُسمَّى "مُبادرة التصيد الاحتيالي Phishing initiative" الذي يجعل من المُمكن منع/ حظر مواقع التصيُّد الاحتيالي bloquer les sites d'hameçonnage، وذلك بفضل التقارير الواردة من مُستخدمي الإنترنت، عبر Internet Explorer المتصفحات الأخرى المُشاركة.

## الفرع الثاني
## جريمة السرقة المعلوماتية

تُعدُّ السرقة عمومًا من الجرائم التي تنخر كاهل الأمم، بل ويقود مرتكبوها العديد من القيم الإنسانية السامية؛ فالسرقة التقليدية تعني إخراج المال من حيازة مالكه وإدخاله في حيازة

الجاني. وذهب المشرع المصري من خلال نصِّ المادة (٣١١) من قانون العقوبات إلى وصف السرقة بأنَّ: "كلُّ من اختلس منقولًا مملوكًا لغيره فهو سارق".

والحقيقة أنَّ العالم يشهد تسارعًا وتناميًا كبيرًا في الإنتاج والنقل والتوزيع والاستهلاك Production, transport, distribution et consommation بدافع المال وإدارة الأعمال؛ مما أظهر تداولَ الكثير من المعلومات والأموال بشكل سريع وميسر.

وجدير بالذِّكر أنَّ السبب في هذا التطور هو بزوغ التكنولوجيات الجديدة، التي لا تتوقَّف عن التحديث، ولكن على الجانب الآخر ظهر المجرم المعلوماتي الخطر ليلحق بأفعاله الدنيئة أضرارًا بأموال الأشخاص وحتى الدول. وتتمثل المعوقات في جريمة السرقة الإلكترونية في صعوبة اكتشاف هذه الجريمة؛ لأنها لا تترك أثرًا خارجيًّا، فهذه الجريمة لا عنف فيها، وإنما هي أرقام وبيانات تتغير وتُمحَى من السجلات المخزنة في ذاكرة الحاسبات الآلية، التي ليس لها أي أثر خارجي مرئي. يضاف إلى صعوبة مواجهة سرقة المال المعلوماتي أنَّ الجريمة تتسم بالغموض وتبعد عن العشوائية وتتميز بالتنظيم، وغالبًا ما يتكون الفعل الإجرامي ويتشارك فيه أكثر من شخص، وتحتاج إلى جهاز حاسوبي مزوَّد بخدمة الإنترنت، ومجرم يتسم بالذكاء الشديد، يهدف إلى تحقيق ربح، فضلًا عن أنَّ هذه الجريمة تتسم بانعدام العنف عند ارتكابها؛ فتتم بمجرد الضغط على بعض مفاتيح الحاسب الآلي، بعكس السرقة التقليدية.

نعود فنقول: إنَّ المال المعلوماتي هو كلُّ ما يُشبع حاجة الفرد أو الجماعة ولو كانت معنوية؛ وبالتالي فالمال صفة يسبغها القانون على كل شيء يصلح أن يكون محلًّا لحق من الحقوق المالية، وإذا خُلع على الشيء هذه الصفة أصبح متقوِّمًا؛ أي ذا قيمة قابلة لأن تُقدَّر بالنقود[١]. والحقيقة أنَّ اختلاس المال المعلوماتي ومدى جواز انطباق الاختلاس على هذا المال المعلوماتي أثار إشكاليات كثيرة، ودون الخوض في تفصيل ذلك، فإن هناك حالات يتم فيها سيطرة الجاني على المال دون اللجوء إلى أي حركة مادية؛ حيث يقتصر دوره عند مجرد تهيئة السبل، وهذا القول يمكن تطبيقه في إطار السرقة المعلوماتية Vol d'informations

(١) **محمد عبد الله العوا:** جرائم الأموال عبر الإنترنت، دكتوراه، كلية الحقوق.الإسكندرية، ٢٠١٣م، ص٦٤.

عندما يقف دور الجاني في تهيئة الطريق أمام المعلومات للانتقال دون أن يتدخل بسلوك إيجابي لإتمام الانتقال؛ كمن يخترق الشبكة المعلوماتية الخاصة بأحد المؤسسات ثم يعطي أمرًا بنسخ المعلومات السرية على أيٍّ من الدعامات الممغنطة التي قام بإعدادها لهذا الغرض، ويأخذ دوره المراقب لسرد المعلومات ونسخها على الدعامات، فهذا المفهوم يختلف عن الاختلاس بالصورة التقليدية.

وجدير بالذِّكر أنَّ فعل الاختلاس الذي يمكن تطبيقه على البيانات والمعلومات يتطلَّب إزالة تصرف المالك في المال برفعه ونقله، وهذا غير متحقق في اختلاس المعلومات والبيانات؛ حيث يمكن سرقة هذه المعلومات عن طريق الالتقاط الذهني سواء عن طريق السمع أو البصر(١). وعلى عكس ذلك، يذهب رأي في الفقه(٢) –ونحن نؤيده– إلى القول بأنَّ الاستيلاء على المعلومة سواء بتخزينها أو نقلها واستثمارها سوف يؤدي إلى حرمان صاحبها من منفعتها الاقتصادية؛ أي يباشر عليها تصرفات الحيازة ضد إرادة صاحبها، وبالتالي بالإمكان حيازة المعلومة Possession d'informations، وهي من الأشياء المعنوية القابلة للحيازة choses morales qui sont possessibles.

ويذهب المشرع المصري من خلال المادة (٢٣) من قانون مكافحة جرائم تقنية المعلومات La loi sur la lutte contre les délits informatiques(٣) إلى أنه "يُعاقب بالحبس مدةً لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن ثلاثين ألف جنيه، ولا تجاوز خمسين ألف جنيه أو بإحدى هاتين العقوبتين، كلُّ من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في الوصول Moyens de technologies de l'information d'accès بدون وجه حقٍّ

(١) راجع في ذلك، **محمد عبد المحسن بن طريف، وآخرين:** جريمة السرقة المعلوماتية، مجلة الدراسات والبحوث القانونية، المجلد (٧)، العدد (٢)، ٢٠٢٢م، ص٢١.

(٢) **محمد شوابكة:** جرائم الحاسوب والإنترنت، الجريمة المعلوماتية، دار الثقافة، عمان، ٢٠١١م، ص١٥٨.

(٣) راجع، القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات الصادر بتاريخ ٢٠١٨/٨/١٤م، والمنشور بالوقائع المصرية بالعدد (٣٢) مكررًا (ج) بتاريخ ٢٠١٨/٨/١٤م، والمعمول به من تاريخ ٢٠١٨/٨/١٥م.

إلى أرقام أو بيانات أو بطاقات البنوك والخدمات Numéros, données ou cartes de banques et de services أو غيرها من أدوات الدفع الإلكترونية Instruments de paiement électronique.

فإن قصد من ذلك استخدامها في الحصول على أموال الغير أو ما تتيحه من خدمات؛ يُعاقَب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين، وتكون العقوبة الحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتي ألف جنيه، أو إحدى هاتين العقوبتين، إذا توصَّل من ذلك إلى الاستيلاء لنفسه أو لغيره على تلك الخدمات أو مال الغير".

## المطلب الثالث

## جرائم تقع على أمن الدولة

بداية نشير إلى أنَّ هذه الجرائم تقع باستعمال النظام المعلوماتي، سواء لإفشاء الأسرار التي تخصُّ مصالح الدولة ونظام الدفاع الوطني، أو الإرهاب، أو التجسس.

لذلك عملت الدولة المصرية كغيرها من الدول على تحقيق حماية فعَّالة لأمنها وكيانها الوطني من مخاطر العدوان عليه؛ حيث تعتبر الجرائم الواقعة على أمن الدولة الخارجي –ومن أهمها جريمة التجسس والإرهاب الإلكتروني cyberterrorisme– من أخطر أنواع الجرائم الماسَّة بأمن الدولة؛ نظرا للضرر الذي يلحق بالدولة باعتبارها عضوًا في المجتمع الدولي ولها علاقات مع غيرها من الدول. لذلك نجد المشرع المصري في قانون مكافحة جرائم تقنية المعلومات من خلال نص المادة (٣٢) منه نصَّ على تشديد العقوبة بقوله: "إذا وقعت أيُّ جريمة من الجرائم المنصوص عليها في هذا القانون بغرض الإخلال بالنظام العام أو تعريض سلامة المجتمع وأمنه للخطر Mettre en danger la sûreté et la sécurité de la communauté أو الإضرار بالأمن القومي للبلاد أو بمركزها الاقتصادي، أو منع أو عرقلة ممارسة السلطات العامة لأعمالها، أو تعطيل أحكام الدستور أو القوانين أو اللوائح، أو الإضرار بالوحدة الوطنية والسلام الاجتماعي Atteinte à l'unité nationale et à la paix sociale؛ تكون العقوبة السجن المشدَّد". يُضاف إلى ذلك أنَّ العدوان على الدولة يَنال

من كيان المجتمع entité communautaire وينتهك كيان الدولة في دنيا الأوطان، بل محوها ماديًّا وأدبيًّا. وتتمثل الجرائم الواقعة على الدولة في: جريمة التجسس الإلكتروني لصالح جماعة أو دولة أجنبية، وجريمة الإرهاب الإلكتروني بالدعوة إلى إحداث فوضى وانتهاكات من شأنها تهديد آمن وسلامة وممتلكات الدولة والأفراد.

## الفرع الأول

## جريمة التجسس الإلكتروني

لعل الهاجس الأكبر لأيّ دولة هو اختراق أنظمتها الأمنية من قِبل دول أخرى –وكثيرًا ما يحدث ذلك– فالأمن السيبراني وارتباطه بالأمن القومي La cybersécurité et son lien avec la sécurité nationale أصبح أحد أهم الأولويات التي تشغل بال دول العالم، وأصبحنا –وبحق– في ظلِّ حرب لا يُسمع فيها صوت الرصاص، فسيادة العالم أصبح يُنظَر إليها بمنظور مختلف عمَّا سبق، فالمعيار تبدَّل من امتلاك الصناعة والأموال إلى امتلاك أنظمة سيبرانية قويَّة قادرة على حماية الأمن القومي، الذي تحرص كلُّ الدول على حمايته وتطويره بشكل مستمر. وعلى الجانب الآخر فإنَّ كثرة استخدام الدخول إلى الشبكة العنكبوتية وذيوعها، وبساطة تكلفتها وعدم تعقُّد استخدامها، أدَّى إلى شيوع كثيرٍ من الجرائم؛ لعلَّ أخطرها جريمة التجسس الإلكتروني، التي تُنذِر بضعف أنظمة المراقبة في كثير من الدول. والحقيقة أنَّ أنظمة المراقبة تصطدم بحقِّ الأفراد في الأمن الشخصي وحريتهم في التعبير عن آرائهم والدخول الآمن Entrée sécurisée.

لذلك لا بدَّ من توازنٍ مفهوم بين حرية الأفراد في الدخول واستخدام الشبكة وحقِّ الدولة في المحافظة على أمنها من الهجمات السيبرانية Cyberattaques، خاصة مع عمل الدولة على غرس مبادئ الإخلاص والأخلاق وحبِّ الوطن والانتماء بأنَّ أعمال التجسس على الدولة Actes d'espionnage contre l'État من الأمور المنافية والقبيحة، فضلًا عن تجريمها

قانونًا. لذلك ذهب رأي في الفقه[١] إلى تعريف التجسس بأنه: "نشاط فردي تترتَّب عليه آثار سلبية جمَّة على الأمن الوطني، ويتم من خلال فعل يقوم به فاعل الجريمة، ويُعبِّر من خلاله وبكامل إرادته وحريته عن رغبته بمساعدة دولة أجنبيَّة أو أكثر؛ بهدف إلحاق أكبر ضرر بسلامة وطنه ومصالحه المُهمة. والحقيقة أننا نعقِّب على هذا التعريف بقول بسيط وهو: إنَّ الهدف من ارتكاب جريمة التجسُّس قد لا يكون إلحاق الضرر بوطن الجاسوس الدنس، وإنما قد يتمثَّل في باعث جني الأموال إلى حدٍّ كبير، أو الحصول على متعة جنسية، أو الانتقال للبلد أو المؤسسة التي يتجسَّس لصالحها المجرم.

**ومن وجهة نظرنا** أنَّ التجسس الإلكتروني يُمثِّل عدوانًا وتهديدًا وتخويفًا، سواء أكان ماديًّا أو معنويًّا، باستخدام وسائل إلكترونية، يصدر من دولة ما أو جماعة معينة أو أفراد على الإنسان بغير حق؛ وذلك باستخدام شبكات سلكية ولاسلكية، أو الأقمار الصناعية، أو شبكات الهواتف المحمول، أو حتى المراقبة الذاتية ونقل المعلومات.

وجدير بالذِّكر أنَّ جريمة التجسس الإلكتروني يمكن أن تتمثَّل في صور عديدة لا يمكن حصرها؛ أبرزها: الحصول على سرٍّ من أسرار الدفاع عن البلاد بقصد تسليمه وإفشائه إلى دولة أجنبية، والتي تتمثل في التقارير والوثائق الصادرة من أجهزة المخابرات العامة والحربية Services de renseignements généraux et militaires والقوات المسلحة وقطاع الأمن الوطني Secteur de la sécurité nationale وهيئة الرقابة الإدارية ، والتي تتضمَّن معلومات وبيانات تتعلق بالقوات المسلحة وأماكن تمركزها وسياسات الدولة الداخلية والخارجية، والتخابر مع من يعملون لمصلحة دولة أجنبية؛ بقصد الإضرار بمركز البلاد الحربي والسياسي والدبلوماسي والاقتصادي وبمصالحها القومية، باستخدام البريد الإلكتروني أو أي وسيلة أخرى من وسائل الاتصال.

---

(١) راجع في هذا التعريف، **أحمد فتحي سرور**: الوسيط في قانون العقوبات –القسم الخاص– دار النهضة العربية، القاهرة، ٢٠١٩م، ص٢٢.

لذلك ذهبت محكمة النقض المصرية[١] إلى القول بأنه: "... والبيّن ممَّا تقدَّم أن تلك الجريمة يتطلَّب تحققها توافر ركنين؛ أحدهما مادي، ويتمثل في الفعل المادي إما التسليم أو الإفشاء لدولة أجنبية أو لمن يعملون لمصلحتها سرًّا من أسرار الدفاع عن البلاد، أو التوصل بأية طريقة إلى الحصول على سرٍ من أسرار الدفاع عن البلاد لتسليمه أو إفشائه إلى دولة أجنبية أو لمن يعملون لمصلحتها، وثانيهما معنوي، ويتمثل في القصد الجنائي العام بشقيه العلم والإرادة؛ أي أن يكون الجاني عالمًا بأن ما يحصل عليه هو سرٌّ من أسرار الدفاع عن البلاد –وفق ما أوضحته المادة (٨٥) من قانون العقوبات السالف بيانها– وأن تتجه إرادته إلى الحصول عليه لتسليمه أو إفشائه إلى دولة أجنبية أو لمن يعملون لمصلحتها...".

ونقول: إنَّه في جريمة التجسُّس الإلكتروني يتمثل الركن المادي المكون لهذه الجريمة في قيام الجاني بفعل التخابر مع دولة أجنبية، وهو ما يعني حصول اتفاق أو تفاهم غير مشروع بين الجاسوس والدولة الأجنبية، هدفه تقديم الجاسوس أسرار الدفاع الخاصة بالدولة بحوزته للدولة الأجنبية، ويمثل هذا السلوك الجريمة بغضِّ النظر عن تحقق النتيجة أم عدم تحقُّقها، والمتمثل في القيام بالأعمال العدوانية ضدَّ الدولة.

وجدير بالذِّكر أنه يستوي أن تكون الدولة المعادية هي التي تواصلت منذ البداية مع الجاني أم هو نفسه من بادر بسلوكه الخبيث بالتواصل، ويستوي أيضًا وسيلة التواصل، سواء المراسلات أو الخطابات أو أي وسيلة أخرى. أمَّا الركن المعنوي فيتمثَّل في القصد الجنائي العام والخاص، ويتشكَّل الأول منهما في اتجاه إرادة الجاني إلى ارتكاب فعل يُشكِّل تخابرًا مع دولة أجنبية، وأن فعله هذا يُكوِّن جريمة التجسس بما يعاقب عليه القانون، وأن يكون عالمًا بأن الدولة التي يتعاون معها أو أي شخص آخر يُكوِّن جريمة التخابر، وإلَّا فلا يتوافر القصد العام

(١) راجع، حكم محكمة النقض في الطعن رقم ٣٢٦١١ لسنة ٨٦ قضائية، والصادر بتاريخ ٢٠١٧/٩/١٦م، مكتب فني ٦٨، ص٥٨١، ق ٦٢، متاح عبر الموقع الإلكتروني التالي: https://emj-eg.com، (الموسوعة القانونية لوزارة العدل المصرية)، بتاريخ ٢٠٢٣/٤/٢٠م، الساعة ٥ ص.

لديه، أمَّا القصد الجنائي فيكون عندما يتوافر لدى الجاسوس قصد إمداد الدولة الأجنبية بالوثائق والمعلومات؛ بغية تدمير أو بث الضعف في أجهزة دولة الجاسوس(١).

## الفرع الثاني
## جريمة الإرهاب الإلكتروني

يُعدُّ الإرهاب من أخطر الظواهر التي تُهدِّد أمن الدول الخارجي والداخلي ، فبثُّ الرعب بين المواطنين وتخويفهم وقتلهم وانتشار الفوضى داخل الدولة بلا شك يُمثِّل تهديدًا خطيرًا(٢). والحقيقة أنَّ ظهور الإنترنت وإتاحته للجميع سهَّل تكوين تشكيلات قادرة على التدريب في الخفاء، وسهَّل أيضًا تلاقي المجرمين؛ لذلك نقول: إنَّ التقارب بين علم التحكم الآلي والإرهاب Cybernétique et terrorisme أو التزاوج بين الإرهاب والتكنولوجيا يُمثِّل الناتج القبيح؛ وهو الإرهاب الإلكتروني.

ومن زاوية أخرى ذهب رأي في الفقه إلى تعريف الإرهاب بأنه: استخدام العنف أو الترويع أو التهديد لخلق حالة من الرعب في المجتمع؛ بهدف الإخلال بالنظام العام وتعريض سلامة المجتمع للخطر(٣).

---

(١) راجع، **إلهام خليفة، جمال غرسي:** التجسس الإلكتروني كجريمة ماسَّة بأمن الدولة في التشريع الجزائري، مجلة دفاتر السياسة والقانون، المجلد (١٤)، العدد الأول، ٢٠٢٢م، ص١٥٦، وما بعدها.

(٢) راجع قريبًا من ذلك، **بدرة هويمل الزين:** الإرهاب في الفضاء الإلكتروني، دراسة مقارنة، رسالة دكتوراة، كلية القانون، جامعة عمان العربية، الأردن، ٢٠١٢م، ص١، وما بعدها.

(٣) راجع في هذا التعريف، **المعتصم منجي محمود القطيشان:** جريمة الإرهاب باستخدام الوسائل الإلكترونية، رسالة ماجستير، كلية الحقوق جامعة الإسراء الخاصة، عمان، الأردن، ٢٠٢٢م، ص٩.

وذهب المشرع من خلال نص المادة (٨٦) من قانون العقوبات[١] إلى تعريف الإرهاب على أنه: "يقصد بالإرهاب في تطبيق أحكام هذا القانون: كلُّ استخدام للقوة أو العنف أو التهديد أو الترويع Recours à la force, à la violence, aux menaces ou à l'intimidation، يلجأ إليه الجاني تنفيذًا لمشروع إجرامي فردي أو جماعي Entreprise criminelle individuelle ou collective، بهدف الإخلال بالنظام العام أو تعريض سلامة المجتمع وأمنه للخطر ، إذا كان من شأن ذلك إيذاء الأشخاص أو إلقاء الرعب بينهم أو تعريض حياتهم أو حرياتهم أو أمنهم للخطر Mettant en danger leur vie, leurs libertés ou leur sécurité، أو إلحاق الضرر بالبيئة، أو بالاتصالات أو المواصلات أو بالأموال أو بالمباني أو بالأملاك العامة أو الخاصة أو احتلالها أو الاستيلاء عليها، أو منع أو عرقلة ممارسة السلطات العامة أو دور العبادة أو معاهد العلم لأعمالها، أو تعطيل تطبيق الدستور أو القوانين أو اللوائح".

وذهب رأي في الفقه[٢] إلى تعريف الإرهاب الإلكتروني بأنه: "العدوان أو التخويف أو التهديد المادي أو المعنوي Agression, intimidation, menace physique ou morale الصادر عن الدول والجماعات أو الأفراد على الإنسان، في دينه أو نفسه أو عرضه أو عقله أو ماله بغير حق، باستخدام الموارد المعلوماتية الوسائل الإلكترونية بشتَّى صنوف العدوان وصور الإسناد. لذلك يذهب رأي في الفقه[٣] إلى القول بأنه يُعدُّ الفضاء الإلكتروني Cyberespace عنصرَ جذبٍ مهمًّا للتنظيمات الإرهابية Organisations terroristes على اختلاف أنواعها وتباين أفكارها؛ نظرًا لما يتيحه لها من وسيلة إعلام عالمية، هي في الوقت نفسه سلاح خطير، وتقوم هذه التنظيمات باستخدام الفضاء الإلكتروني في الدعاية

(١) المعدلة بتاريخ ١٩٩٢/٧/٢٨م.

(٢) راجع، **مدحت رمضان عبد الحليم**: الحماية الجنائية للتجارة الإلكترونية، دراسة مقارنة، الطبعة الأولى، دار النهضة العربية، ٢٠٠١م، ص١٥٢.

(٣) راجع في ذلك، **السيد عوض**: الجريمة في مجتمع متغير، المكتبة المصرية، الإسكندرية، ٢٠٠٤م، ص٢٠١، وما بعدها.

والتجنيد والتمويل وجمع المعلومات Propagande, recrutement, financement et collecte d'informations، وتنسيق الهجمات الإرهابية Coordination des attaques terroristes، وحشد المتعاطفين من مختلف دول العالم.

ويبدو أنَّ الغرض الإرهابي يتمثَّل في اتجاه إرادة الجاني إلى ارتكاب فعل أو الامتناع عن فعل، متى كان هذا الارتكاب أو الامتناع مجرَّمًا قانونًا؛ وذلك بقصد إحداث نتيجة إرهابية مباشرة أو غير مباشرة، أو عَلِمَ الجاني بأنَّ من شأن الفعل أو الامتناع عن الفعل تحقيق نتيجة إرهابية Atteindre un résultat terroriste.

وجدير بالذِّكر أن النتيجة الإرهابية تتمثَّل في إثارة الرعب بين مجموعة من الناس أو إزهاق الأرواح، أو التسبب في أذى بدنيٍّ جسيم، أو إلحاق ضرر ذي شأن بالممتلكات أو بالبيئة، أو الإخلال بأمن المجتمع الداخلي أو الدولي Atteinte à la sécurité de la communauté interne ou internationale، أو معاداة الدولة، أو التأثير على السلطات العامة في الدولة أو دولة أخرى أو منظمة دولية في أدائها لأعمالها، أو الحصول من الدولة أو دولة أخرى أو منظمة دولية على منفعة أو مَزيَّة من أيِّ نوع.

وذهبت محكمة النقض(١) إلى وصف التنظيم الإرهابي بقولها: "لمَّا كان ذلك، وكان البيِّن من استقراء نصِّ المادتين (٨٦ مكررًا)، و(٨٦ مكررًا/ أ) من قانون العقوبات أنَّ المشرع أطلق وصف التنظيم الإرهابي على جمعية أو هيئة أو منظمة أو جماعة أو عصابة Une association, un organisme, une organisation, un groupe ou un gang تهدف إلى تعطيل أحكام الدستور أو القوانين أو منع إحدى مؤسسات الدولة أو سلطاتها العامة من ممارسة أعمالها، أو الاعتداء على الحرية الشخصية للمواطن أو غيرها من الحريات والحقوق العامة التي تكفل الدستور والقانون بحمايتها، أو الإضرار بالوحدة الوطنية أو السلام الاجتماعي، وذلك كله إذا كان العنف أو القوة أو التهديد Violence, force ou menace باستعمالها من بين الوسائل التي قد تلجأ إليها هذه الجماعة لتحقيق أهدافها...".

(١) راجع، حكم محكمة النقض في الطعن رقم ١٩٩٠ لسنة ٨ قضائية، الصادر بجلسة ٢٠٢٠/٢/٤م .

والحقيقة أنَّ محكمة النقض[١] ذهبت إلى إيضاح أركان جريمة الإرهاب Éléments du crime de terrorisme بصفه عامه بقولها: "لمَّا كان الحكم قد عرض لدفع الطاعن بعدم توافر أركان جريمة الانضمام إلى جماعة أُسِّست على خلاف القانون وأَطرُحِه بقوله: وحيث إنه عن الدفع بانتفاء أركان الجرائم محلَّ الاتهام، فهذا الدفع في غير محله ومردود؛ ذلك أنه وبعد الحادث الإرهابي الذي نال من مديرية أمن... أعلن مجلس الوزراء المصري اعتبار جماعة... جماعة إرهابية وتنظيمها تنظيمًا إرهابيًّا وفق نص المادة (٨٦) من قانون العقوبات.

وتوقع العقوبة المقررة قانونًا على كلِّ من يشترك في التنظيم، أو يُروِّج لها بالقول والكتابة أو أي وسيلة أخرى، وبقصد الإرهاب في تطبيق هذا القانون، كلُّ استخدامٍ للقوة أو العنف أو التهديد أو الترويج يلجأ إليه الجاني لتنفيذ مشروع إجرامي فردي أو جماعي، بهدف الإخلال بالنظام العام أو تعريض سلامة المجتمع وأمنه للخطر، إذا كان من شأن ذلك إيذاء الأشخاص أو إلقاء الرعب بينهم أو تعريض حياتهم للخطر أو إلحاق الضرر بالبيئة أو بالاتصالات أو الأموال أو المباني أو الأملاك العامة أو الخاصة أو احتلالها أو الاستيلاء عليها أو تعطيل الدستور أو القوانين أو اللوائح، وكانت الجرائم المنصوص عليها في المادتين (٨٦ مكررًا)، و(٨٦ مكررًا أ) من قانون العقوبات تتحقَّق بتوافر عنصرين؛ أولهما: عنصر مادي Élément matériel يتمثل في مظاهر القوة أو العنف أو التهديد أو الترويج Manifestations de force, de violence, de menace ou de promotion الحاصلة من الجاني، فالسلوك الإجرامي في جريمة الإرهاب يتخذ شكل العنف بمعناه الواسع بما يشير إليه من معاني مختلفة تتضمَّن استخدام القوة أو التهديد أو الترويج لها على النحو الذي حدده القانون.

وثانيهما: يتمثل في القصد الجنائي العام، وهو إدراك الجاني لما يفعله وعلمه بشروط الجريمة؛ فيتعين اتجاه إرادة الجاني إلى استخدام القوة أو العنف أو التهديد أو الترويج مع علمه بأن هذا السلوك من شأنه أن يؤدي إلى المساس بالحقوق والمصالح التي حددتها المادة (٨٦).

---

(١) راجع، حكم محكمة النقض في الطعن رقم ٢٩٩٥٣ لسنة ٨٦ قضائية، الصادر بجلسة ٢٠١٧/٤/٢٧م، مكتب فني ٦٨، رقم الصفحة ٣٠٣، رقم القاعدة ٣٨ .

فيشترط أن يكون الهدف من العمل الإرهابي هو الإخلال بالنظام العام أو تعريض سلامة الوطن للخطر؛ وبذلك يشمل كل الأعمال الإجرامية Actes criminels أو أن تكون من شأنها خلق حالة من الرعب في عقول أشخاص معينة أو لدى جماعة من الأشخاص، ويستخلص القصد الجنائي من مضمون أعمال الإرهاب التي ارتكبها الجاني التي اعتبرها المشرع صورة للسلوك الإجرامي ونتيجة له...".

وذهب المشرع من خلال نص المادة (٣٤) من قانون مكافحة جرائم تقنية المعلومات إلى أنه: "إذا وقعت أي جريمة من الجرائم المنصوص عليها في هذا القانون بغرض الإخلال بالنظام العام Violation de l'ordre public أو تعريض سلامة المجتمع وأمنه للخطر أو الإضرار بالأمن القومي للبلاد أو بمركزها الاقتصادي أو منع أو عرقلة ممارسة السلطات العامة لأعمالها أو تعطيل أحكام الدستور أو القوانين أو اللوائح أو الإضرار بالوحدة الوطنية والسلام الاجتماعي Atteinte à l'unité nationale et à la paix sociale، تكون العقوبة السجن المشدد".

## المبحث الثاني
## تحديات مواجهة الجريمة المعلوماتية

قلنا إنَّ الجريمة المعلوماتية تتسم بالعالميَّة، فهي عابرة للقارات لا تعترف بالحدود الجغرافية للدول؛ لذلك تهتم أغلب الدول بمكافحتها والقضاء عليها حماية لأمنها السياسي والاقتصادي والاجتماعي. والحقيقة أنَّ تطور وسائل الاتصالات وتزايد استخدام التكنولوجيا أدَّى إلى الثقة في هذه الوسائل، وسهَّل الدخول إلى أجهزة الحاسب الآلي؛ مما نتج عنه تزايد الاتصالات المجهولة من قِبل مستخدمي ومرتكبي جرائم تكنولوجيا المعلومات.

والتحدي الأكبر لمواجهة الجريمة المعلوماتية يتلَّخص في غياب آليات الرقابة وسهولة محو البيانات وحذفها؛ حيث إننا نتعامل مع بعض النبضات المغناطيسية أو الكهربائية، يضاف لذلك استقلالية المكان والحضور في مكان الجريمة المعلوماتية.

فضلًا عن أن الجريمة المعلوماتية ينتج عنها خسائر ضخمة تفوق في آثارها الجريمة التقليدية، يكفي أن نذكر أنَّ الجريمة المعلوماتية تُسوِّق لبعض القيم الدخيلة على المجتمعات، وتُهدِّد القيم والنظام الأخلاقي، خاصة في المجتمعات المحافظة أو المغلقة.

وعلى الجانب الآخر تبرز التحديات التشريعية في وضع نظام قانوني منضبط وفعَّال للحدِّ من هذه الجرائم، يأتي في مقدمتها الاختصاص القضائي وملاحقة وتسليم المجرمين، مع الوضع في الاعتبار أنَّ أدوات الجريمة ومسرحها وصعوبة الإثبات التي تتسم بها الجريمة المعلوماتية تُشكِّل تحديات كبيرة، فضلًا عن نقص خبرة جهات الملاحقة والتحقيق والمحاكمة، فهي جريمة تُكتَشف بعد وقت طويل من ارتكابها وبالصدفة. من كلِّ ذلك سوف نتناول هذه التحديات؛ وذلك من خلال مطلبان ، نتناول في أولها الجهود الدولية لمكافحة الجريمة المعلوماتية، وفي ثانيها نتناول الجهود الإقليمية لمكافحة الجريمة المعلوماتية .

## المطلب الأول

## الجهود الدولية لمكافحة الجريمة المعلوماتية

لا شكَّ أنَّ الجريمة المعلوماتية خطرها يتعدَّى أنها مجرد جريمة، وإنما آثارها قد تصل إلى محو دولة أو منطقة اقتصاديًّا وسياسيًّا واجتماعيًّا؛ لذلك تتعاون الدول من أجل مواجهة هذه الجريمة المتجددة المخاطر. ولعلَّ الإشكالية الأبرز حينما يرتكب المجرم المعلوماتي جريمةً في بلد وتنتج آثارها في بلد آخر، ويمر خلال ارتكاب الجريمة بأكثر من دولة، هنا لا بدَّ من تكثيف الجهود للحد من هذه الظاهرة والقضاء عليها.

والحقيقة أنَّ التعاون الدولي بين البلدان يتم بإحدى طريقين، إما بشكل رسمي أو بشكل غير رسمي وديٍّ ينشأ من العلاقة الجيدة بين الدولتين بطريقة سريعة ومنجزة. أما التعاون الرسمي بين الدول التي طالها آثار الجريمة المعلوماتية فيعتمد في المرتبة الأولى على اتفاقيات ومعاهدات رسمية بين الدول، أهمها اتفاقيات ملاحقة وتسليم المجرمين وآليات التحقيق.

ولعلَّ من أهمِّ الاتفاقيات التي اهتمَّت بالتعاون: اتفاقية بودابست ٢٠٠١م، التي أكَّدت اتخاذ التدابير التشريعية والتنظيمية لضمان ملاحقة مرتكبي هذه الجرائم وكشفها، وتوفير قواعد

ملائمة للتحرّي والتحقيق والضبط والتفتيش والمحاكمة مع التركيز على أهمية التعاون المحلي والإقليمي والدولي، وتوحيد الجهود الدولية في مجال مكافحة جرائم الإنترنت.

أولًا: ضرورة الاتفاق على تحديد مبدأ الطبيعة القانونية للجريمة الإلكترونية.

الحقيقة أنَّ تحديد مفهوم موحَّد للجريمة المعلوماتية أمرٌ بالغُ الأهمية لتوافق الأحكام والمبادئ المطبَّقة على الفعل الإجرامي المرتكَب في أكثر من دولة، فعدم وجود اتفاق عامٍّ مشترك بين الدول حول نماذج إساءة استخدام نظام المعلومات وشبكة المعلومات الواجب تجريمها يُشكِّل تحديًا كبيرًا(١)؛ والسبب في ذلك أنَّ ما يكون تجريمه في دولة معينة وهو منافٍ للعادات والتقاليد والقيم الأخلاقية والاجتماعية قد يكون مباحًا في دولة أخرى(٢).

ومن هنا بدأت بعض الأصوات ترتفع للمطالبة بضرورة سنِّ قوانين لحماية المعلومات على الشبكات، بالإضافة إلى إدراك الدول والحكومات لحجم المخاطر التي تزداد معها جرائم الإنترنت؛ فأُنشئت جهات رسمية لمكافحة هذه الجرائم وسُنَّت قوانين لحماية شبكة المعلومات، بالإضافة إلى أنَّ وعي هذه الدول بمدى خطورة هذه الجرائم العابرة للحدود كان نتيجةً لإبرام عدة اتفاقيات ومعاهدات دولية في مجال مكافحة هذه الجرائم التي باتت تهددها، خاصة مع ازدياد استعمال التكنولوجيا الحديثة يومًا بعد يوم، وأهمها الاتفاقية الأوربية لمكافحة جرائم الإنترنت، ومعاهده بودابست ٢٠٠١.

وجدير بالذِّكر أنه تعدُّ كلٌّ من معاهدة بودابيست والمعاهدة الأوربية من أهم المعاهدات التي أبرمت لمكافحة جرائم الإنترنت في إطار التعاون الدولي، فقد تم توقيع هذه المعاهدة في بودابستت ٢٠٠١ اقتناعًا من المجلس بأن هذه الاتفاقية ستوفر ما يلزم لردع أيِّ عمل موجَّه

(١) راجع في هذا المعنى، **شوقي يعيش تمام، عزيزة شبري:** تفعيل مبدأ عالمية النص الجنائي في التصدي للجريمة المعلوماتية، مجلة الاجتهاد القضائي، العدد الخامس عشر، سبتمبر ٢٠١٧م، ص٩٣.

(٢) راجع في هذا المعنى، **عبد الفتاح بيومي حجازي:** الإثبات الجنائي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة، ٢٠٠٧م، ص١٨٨.

ضد السرية والنزاهة، وتوفير نظم الحاسوب والشبكات والبيانات، واتخاذ ما يكفي من الإجراءات والصلاحيات لمكافحة هذه الجرائم(١).

وجدير بالتنبيه أنَّ هذه المعاهدة أكَّدت الحاجة لاتخاذ تدابير تشريعية لمكافحة جرائم المعلوماتية Prendre des mesures législatives pour lutter contre les délits informatiques ومخاطرها على الدول، والدعوة إلى مكافحة كافة الأنشطة الإجرامية التي تستهدف أمن المعلومات، كما تكفل للحكومات حقَّ المراقبة وتلزم الدول بمساعدة بعضها البعض في جمع الأدلة.

أمَّا المعاهدة الأوروبية لمكافحة جرائم الإنترنت Traité européen contre la criminalité sur Internet فقد استلزمت الدول الموقِّعة عليها بسنِّ الحد الأدنى من القوانين الضرورية للتعامل مع جرائم التقنية العالية، بما في ذلك الدخول غير المصرَّح به إلى شبكة ما والتلاعب بالبيانات، وجرائم الاحتيال والتزوير التي لها صلة بالكمبيوتر، وصور القاصرين الإباحية وانتهاكات حقوق النسخ الرقمي.

وجدير بالذِّكر أنه قد تبنَّت دول مجموعة الدول G7-P8 في قمة واشنطن عام ١٩٩٨ عشرة مبادئ وخطة عمل لمكافحة جرائم التكنولوجيا المتقدمة Principes et plan d'action pour lutter contre la criminalité technologique avancée: "تنص المبادئ المُعتمدة على [...] تكييف القوانين القمعية الوطنية، وتعزيز القُدرات التقنية، وتحسين المُساعدة القانونية المُتبادلة، وكذلك الالتزام بالموارد لتدريب وتجهيز طاقم البحث والتحقيق، وإنشاء نقطة اتصال على المُستوى الوطني المسئول عن تلقي طلبات التحقيقات والدراسات الاستقصائية القادمة من الخارج Demandes d'enquêtes et d'investigations en provenance de l'étranger(٢).

---

(١) راجع في هذا المعنى، **خليل يوسف جندي:** المواجهة التشريعية للجريمة المعلوماتية على المستويين الدولي والوطني، دراسة مقارنة، مجلة كلية القانون للعلوم القانونية والسياسية، المجلد (٧)، العدد (٢٦)، ٢٠١٨م، ص٩٨، وما بعدها.

(2) Christiane Féral-Schuhl, Praxis Cyberdroit, op. cit., p. 449, 447 et 260 et s.

أمَّا الاتفاقية الأمريكية المتعلقة بجرائم الحاسب الآلي والإنترنت Convention américaine sur les délits informatiques et Internet لسنة ١٩٩٩م، فقد أوجبت هذه الاتفاقية تبنِّي معايير موحَّدة لمواجهة هذه الجرائم وفرض عقوبات تتناسب مع درجة خطورتها، وأيضًا بيَّنت الجرائم المعلوماتية؛ وهي المتمثلة في التوصيل غير المصرَّح به، وتعديل وحذف البيانات بهدف الإضرار بالمؤسسات التي تملك هذه الخدمات، أو حذف البيانات بتغييرها لإعطاء معلومات كاذبة(١).

ثانيًا: تفعيل التطور الحاصل في مبدأ نطاق تطبيق القانون الجنائي الوطني من حيث المكان.

لا شكَّ أنه عند وقوع الجريمة في إقليم دولة؛ كمصر، وكان كلٌّ من الجاني والمجني عليه مواطنًا مصريًّا، فمن المؤكد حينئذ أنَّ قانون العقوبات المصري والمحاكم المصرية هي الوحيدة المختصة بنظر الدعوى الجنائية، ولكن إذا لم يكن أحد هذه العناصر مصري الجنسية، فمن الممكن أنْ ينطبق عليه قانون جنائي آخر وفقًا للمعايير الخاصة بتطبيق قانون العقوبات من حيث المكان، والتي تأخذ بها بعض الدول، ويكون هناك تنازع في تطبيق القوانين الجنائية بين القانون الجنائي الوطني، والقانون الجنائي لدولة أخري.

وذهب المشرع الفرنسي من خلال نص المادة (١١٣-٢) من قانون العقوبات على أن "قانون العقوبات الفرنسي يُطبَّق على الجرائم المُرتكبة على أراضي الجمهورية، ويتم اعتبار أن الجريمة قد تم ارتكابها على أراضي الجمهورية عندما يكون أحد الأفعال المكونة لها قد وقع في هذا الإقليم"(٢).

---

(١) **وائل محمد نصيرات:** الجهود الدولية في مكافحة الجرائم المعلوماتية والصعوبات التي تواجهها، بحث مقدم للمؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية ICACC، جامعة الإمام محمد بن سعود الإسلامية، كلية علوم الحاسب والمعلومات، المملكة العربية السعودية الرياض، نوفمبر ٢٠١٥م، ص١٢٩ وما بعدها.

(2) Frédérique CHOPIN, Cybercriminalité, op. cit., §476, PP. 249-251.

ويذهب رأي في الفقه[١] إلى القول بأنَّ مبدأ الإقليمية principe de territorialité يعني: أنَّ القانون الواجب التطبيق عند وقوع أيَّة جريمة هو قانون البلد الذي وقعت فيه الجريمة بغضِّ النظر عن جنسية مرتكبها، سواء أكان مرتكب الجريمة وطنيًّا أم أجنبيًّا.

والحقيقة أنَّ الدول أغلبها تأخذ بمبدأ إقليمية القوانين، وتستثني من ذلك بعض الجرائم، حتى لو ارتُكبت خارج إقليمها بتوازن منضبط بين حقِّ الدولة في فرض سلطتها على إقليمها وبين جرائم تمس بناء الدولة السياسي والاقتصادي، وهو ما ذهب إليه المشرع المصري من خلال نص المادة الثانية من قانون العقوبات[٢] بقوله: "تسري أحكام هذا القانون أيضًا على الأشخاص الآتي ذكرهم: (أولًا) كلُّ من ارتكب في خارج القطر فعلًا يجعله فاعلًا أو شريكًا في جريمة وقعت كلها أو

بعضها في القطر المصري، (ثانيًا) كلُّ من ارتكب في خارج القطر جريمة من الجرائم الآتية:

(أ) جناية مخلة بأمن الحكومة ممَّا نُصَّ عليه في البابين الأول والثاني من الكتاب الثاني من هذا القانون، (ب) جناية تزوير ممَّا نُصَّ عليه في المادة (٢٠٦) من هذا القانون، (ج) جناية تقليد أو تزييف أو تزوير عملة ورقية أو معدنية ممَّا نُصَّ عليه في المادة (٢٠٢)، أو جناية إدخال تلك العملة الورقية أو المعدنية المقلدة أو المزيفة أو المزورة إلى مصر أو إخراجها منها أو ترويجها أو حيازتها بقصد الترويج أو التعامل بها ممَّا نُصَّ عليه في المادة (٢٠٣) بشرط أن تكون العملة متداولة قانونًا في مصر". والاستثناءات الواردة على مبدأ إقليمية القوانين Le principe de territorialité des lois: مبدأ العينية، الذي يُقصد به سريان قانون العقوبات على جرائم معينة تقع في خارج البلاد بغض النظر عن جنسية الفاعل في تلك الجرائم؛ بسبب تعلُّقها بمصالح جوهرية للدولة؛ ومن هذه الجرائم: تلك الماسَّة بأمن الدولة، وجريمة تزوير أو تزييف عملة الدولة أو عملة متداولة قانونًا في الدولة.

---

(١) راجع في هذا التعريف، **محمد فوزي إبراهيم**: نطاق تطبيق قانون العقوبات من حيث المكان على الجرائم المرتكبة في المحطات الفضائية، مجلة البحوث القانونية والاقتصادية، كلية الحقوق جامعة المنصورة، العدد (٧٥)، مارس ٢٠٢١م، ص٦٤.

(٢) معدلة بتاريخ ١٩٥٦/٢/٢٦م.

ونرى أنَّ الجريمة المعلوماتية تدخل في نطاق الجرائم المُستثناة من تطبيق مبدأ الإقليمية لأسباب لا تخفي على كلِّ ذي لب؛ فهي تُشكِّل خطرًا كبيرًا على قيم ومبادئ المجتمعات Valeurs et principes des communautés فضلًا عن آثارها الضارة السياسية والاقتصادية. وهو ما ذهب إليه المشرع والقضاء الفرنسي بخصوص المحتوى غير المشروع الذي يتم نشره عبر الإنترنت مُتاحًا، أو يمكن الوصول إليه من فرنسا، وفيما يتعلَّق بجريمة التشهير العلني "السب والقذف العلني" المُرتكبة عبر الإنترنت، والمسائل المُتعلقة بجرائم الصحافة المُرتكبة عبر الإنترنت أو عن طريق استخدامه، ولا سيما عندما يتم الإعلان –الركن المُكوِّن للجريمة– عبر الإنترنت، ويُمكن الوصول إليها من فرنسا.

وهو ما تم إقراره في مرسوم صدر بتاريخ ١١ أكتوبر ٢٠١٢، خلُصَ فيه رئيس المحكمة الابتدائية الكبرى في نونتير tribunal de grande instance de Nanterre إلى أن "المحاكم الفرنسية مُختصة بالفصل في الضرر الكامل الناجم عن الانتهاكات المزعومة للحق في الصورة atteintes alléguées à son droit à l'image بواسطة مواقع أجنبية"(١).

ولذلك نجد –تماشيًا مع هذا الموقف– أنَّ الدائرة الجنائية أعادت في حكم صدر بشأن نشر أقوال "بيانات – تعليقات" يُزعم أنها مُهينة ضدَّ مواطنين بريطانيين مُقيمين في موناكو، تأكيدَ هذا التحليل من خلال البحث فيما إذا كان الموقع الإلكتروني أو التعليقات "الأقوال" المعنيَّة Le site web ou les commentaires "propos" en question مُوجَّهة بشكل جيد للجمهور الفرنسي، وحيث إنَّ هذا الموقع يُمكن الوصول إليه من الأراضي الوطنية فإن ذلك لا يُميز في حدِّ ذاته عملية النشر على الأراضي الفرنسية، والذي يجعل القاضي الفرنسي مُختصًا، وتُعدُّ السمعة التي يدعيها الأطراف المَعنيون فقط في قطاع الأعمال غير كافية في هذا الصدد(٢). وأخيرًا، أكَّدت الدائرة الجنائية رفض الدفع بعدم الاختصاص rejet de l'exception d'incompétence المستنَد إليه من قِبل "الذي احتج به" مُدير النشر في موقع على شبكة الإنترنت تستضيفه سويسرا، والذي تمت مُقاضاته في فرنسا بسبب التحريض على

(1) TGI Nanterre, ord. ME, 11 oct. 2012, www.legalis.net.
(2) Crim. 6 mars 2018, no 16 - 87.533.

التمييز العنصري discrimination raciale ضدَّ الجالية المسلمة la communauté musulmane.

ثالثًا: ضرورة الإقرار في بعض الحالات بحجية التشريعات والأحكام الجنائية غير الوطنية.

المعروف أنَّ التشريع الوطني وتطبيقه من قبل القضاء المختص –الجنائي– يُعدُّ مظهرًا من مظاهر حقِّ الدولة في فرض سياستها على إقليمها والمواطنين الموجودين على أرضها.

يضاف إلى ذلك أنَّ أغلب قوانين وقواعد القانون الجنائي Lois et normes du droit pénal تُعدُّ من النظام العام، بما لا يجوز الاتفاق على ما يخالفها.

ولكن نظرًا للانتشار السريع، وكون الجريمة المعلوماتية عالمية عابرة للقارات، فإن الضرورة تقتضي الاعتراف في بعض الأحيان بحجية التشريعات والأحكام غير الوطنية L'autorité de la législation et des dispositions non nationales[(١)].

وهو ما ذهب إليه المشرع الفرنسي بقوله: "تنص المادة (١١٣–٥) من قانون العقوبات على أنَّ: "قانون العقوبات الفرنسي يُطبَّق على أي شخص ارتكب جريمة على أراضي الجمهورية؛ كشريك في جريمة أو جنحة ارتُكِبَت في الخارج إذا كانت الجناية أو الجنحة يُعاقَب عليها في نفس الوقت بموجب القانون الفرنسي والقانون الأجنبي، وإذا تم إثباتها بصدور قرار نهائي من المحكمة الأجنبية"، ويتعلق هذا الحكم بجرائم الإنترنت المُرتكبة على الأراضي الفرنسية وخارجها Délits sur Internet commis sur le territoire français et à l'étranger"[(٢)].

ولكننا نلاحظ أن جلَّ التشريعات الجنائية المطبقة حاليًّا في معظم دول العالم ترتكز على الصفة الإقليمية فيما يتعلق بتطبيق قواعد الإجراءات الجنائية عن طريق السلطات غير

---

(١) راجع في هذا المعنى، **محمد بن أحمد علي المقصودي:** الجرائم المعلوماتية: خصائصها وكيفية مواجهتها قانونًا، المجلة العربية للدراسات الأمنية، جامعة نايف العربية للعلوم الأمنية، المجلد (٣٣)، العدد (٧٠)، ٢٠١٧م، ص١٢٣.

(2 )Frédérique CHOPIN, Cybercriminalité, op. cit., §480, PP. 252-254.

الوطنية؛ لذلك فلا مناص من الاتفاقيات الثنائية والجماعية بين الدول؛ لتسهيل تحقيق جرائم المعلوماتية، ورغم إبرام بعض الاتفاقيات[١] إلَّا أنها لم تف بالغرض في حلِّ مشكلات الاختصاص Problèmes de compétence، وتبادل الأدلة الجنائية، وتسليم المجرمين Échange de preuves medicals et extradition؛ لذلك تبقى الحاجةُ جدَّ ماسة إلى تشريعات جنائية أكثر مرونة حتى تواكب سرعة التقدم التكنولوجي وعصر المعلوماتية[٢].

ناهيك عن أنه رغم تنوع الجهود إلَّا أنها تشترك جميعًا في أنها تتضمن مجرد توجيهات وتوصيات للجهات المسئولة في تسجيل العناوين الإلكترونية.

## المطلب الثاني
## الجهود الإقليمية لمكافحة الجريمة المعلوماتية

ذهبت الدول العربية إلى إقرار قانونٍ وميثاقٍ استرشادي Loi et charte d'orientation من أجل الاستعانة بنصوصه عند إقرار تشريعات داخلية لمكافحة جرائم المعلومات والاتصالات، وهو المعروف بالقانون العربي النموذجي الموحَّد لمكافحة سوء استخدام تكنولوجيا

(١) ومن أهمِّ هذه الاتفاقات والمؤتمرات والقوانين نذكر: المؤتمر الخامس "جنيف ١٩٧٥م"، والمؤتمر الدولي السادس بكركاس "فنزويلا" المنعقد في غضون عام ١٩٨٠م، ومؤتمر الأمم المتحدة السابع لمنع الجريمة ومعاملة المجرمين، ومؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة السجناء بشأن الجرائم ذات الصلة بالكمبيوتر "هافانا"، لعام ١٩٩٠م، وقانون الأنسيترال بشأن التجارة الإلكترونية لعام ١٩٩٦م، والمنظمة العالمية للملكية الفكرية "وايبو" (WIPO)، واتفاقية برن الدولية لحماية المصنفات الأدبية والفنية، واتفاقية تربسل لعام ١٩٤٤م، ومجموعة الدول الثمانية G8، والاتفاقية الخاصة بحماية الأفراد من إساءة استخدام البيانات المعالجة إلكترونيًّا لعام ١٩٨١م، والمعاهدة الأوروبية في مكافحة جرائم الإنترنت "اتفاقية مجلس أوروبا بشأن الإجرام السيبيري لعام ٢٠٠١م"، والمؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات ١٩٩٤م، بالبرازيل بشأن جرائم الكمبيوتر، والاتفاقية الأمريكية المتعلقة بجرائم الحاسب الآلي والإنترنت لسنة ١٩٩٩م.

(٢) راجع، **عبد الفتاح بيومي حجازي:** الإثبات الجنائي في جرائم الكمبيوتر والإنترنت، مرجع سابق، ص١٩٢، راجع أيضًا في هذا المعنى، **شوقي يعيش تمام، عزيزة شبري:** تفعيل مبدأ عالمية النص الجنائي في التصدي للجريمة المعلوماتية، مرجع سابق، ص١٠١.

المعلومات والاتصالات La loi type arabe unifiée pour lutter contre l'utilisation abusive des technologies de l'information et de la communication، الذي تم إقراره من قِبل وزراء العدل العرب في اجتماعهم المشترك في ٢٢/ ٥/ ٢٠٠٣م[١].

ومما تجدر الإشارة إليه أنَّ العديد من الدول العربية لم تُصدر قانونًا يتعلق بالجريمة المعلوماتية، سواء ارتكبت عن طريق الكمبيوتر أو عن طريق الإنترنت، ولا يزال الخلاف قائمًا حول أفضلية تعديل التشريعات العقابية لكي تستوعب نماذج الجريمة المعلوماتية، أم أنه من الأفضل تعدل قوانين حماية الملكية الفكرية كي تستوعب هذه الأنشطة من السلوك ويتم تجريمها، أم من الأفضل إصدار تشريعات جديدة خاصة بالجريمة المعلوماتية؟ حتى إنَّ الأمر لا يتوقف هنا بل يتعداه؛ حيث إنَّ عدم اتفاق الأنظمة القانونية المختلفة على صورة موحَّدة للسلوك الإجرامي في الجريمة المعلوماتية يغري قراصنة الحاسب الآلي بتنظيم أنفسهم وارتكاب جرائمهم دون التقيد بالحدود الجغرافية؛ الأمر الذي يؤكد حتمية التعاون الدولي لمكافحة هذه الجريمة.

بيد أن الدول العربية أبرمت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات Convention Arabe sur la lutte contre la Criminalité liée aux Technologies de l'Information؛ وذلك لتعزيز التعاون القضائي والقانوني بين الدول الموقعة والمنضمة إليها[٢]، وذلك في مجالات عديدة؛ منها: تنازع الاختصاص، وتسليم المجرمين، والمساعدة القضائية المتبادلة؛ وذلك من أجل مكافحة جرائم تقنية المعلومات لدرء أخطار هذه الجرائم، حفاظًا على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها[٣].

---

(١) راجع في ذلك، **أشرف محمد نجيب السعيد الدريني:** جرائم الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات، مجلة روح القوانين، العدد الخامس والتسعون، يوليو ٢٠٢١م، ص٢٥٠.

(٢) راجع في هذا المعنى، **محمد أحمد سليمان عيسى:** الجهود الدولية الإقليمية لمواجهة الجرائم الإلكترونية، مجلة العلوم القانونية، كلية القانون جامعة عجمان، السنة الرابعة، العدد الثامن، يوليو ٢٠١٨م، ص٢٠٠.

(٣) أبرمت هذه الاتفاقية بمدينة القاهرة جامعة الدول العربية بجمهورية مصر العربية بتاريخ ٢٠١٠/١٢/٢١م، بين وزراء الداخلية والعدل العرب نيابة عن دولهم ووقعت وصدقت عليها أغلب الدول، ومنها جمهورية مصر العربية وأصبحت جزءًا من تشريعها الداخلي، وذلك بالقرار الجمهوري رقم ٢٧٦ لسنة ٢٠١٤

لذلك نجد رأيًا[١] يذهب إلى القول بأن الاتفاقية تضمنت إستراتيجية تشريعات وطنية[٢]

خاصة بمكافحة جرائم تقنية المعلومات Stratégie législative nationale de lutte contre la criminalité liée aux Technologies de l'Information، كما حرصت على إيجاد آلية وطنية للتعاون والتنسيق بين الجهات المعنية بمكافحة هذه الجرائم، ابتداءً من مرحلة تقييم المخاطر، ورصد ومتابعة تلك الجرائم وتبادل المعلومات بشأنها، مرورًا بعمليات التحري والملاحقة والتحقيق وتبادل المعلومات، وانتهاءً بتقديم مرتكبيها إلى المحاكمة، مع التعاون والتنسيق مع جميع وسائل الإعلام المرئية والمسموعة والمقروءة لتوعية المواطنين بأخطار جرائم تقنية المعلومات Crimes Liés aux Technologies de l'Information، وأضرارها الاقتصادية، والاجتماعية على الفرد والمجتمع، وتوعية العاملين بمراكز المعلومات والاتصالات، ومستخدمي الشبكة العنكبوتية، ومواقع التواصل الاجتماعي بالأساليب والوسائل التي يتبعها قراصنة المعلومات لتحقيق أهدافهم الدنيئة، والسبل الكفيلة بكشفها.

---

الصادر بتاريخ ٢٠١٤/٨/١٩م، والمنشور بالجريدة الرسمية بالعدد رقم (٤٦) بتاريخ ٢٠١٤/١١/١٣م، والمعمول به اعتبارًا من ٢٠١٤/١٠/٨م.

(١) راجع، **محمد أحمد السويحلي:** تكاتف الجهود العربية لمكافحة الجريمة الإلكترونية، مجلة الدراسات المالية والمصرفية، الأكاديمية العربية للعلوم المالية والمصرفية، مركز البحوث المالية والمصرفية، المجلد (٢٣)، العدد الأول، مارس ٢٠١٥م، ص٦.

(٢) من أهم هذه التشريعات، قانون نظام مكافحة المعلوماتية بالمملكة العربية السعودية، بموجب قرار مجلس الوزراء رقم ٧٩ والصادر بتاريخ ١٤٢٨/٣/٧هجريًا، والمصدق عليه بالمرسوم الملكي رقم ١٧م، الموافق ١٤٢٨/٣/٨ هجريًا، والصادر بالقرار رقم ١١٥٦٧/ب، بتاريخ ١٤٢٨/٣/٩ هجريًا، القانون الاتحادي بدولة الإمارات العربية المتحدة رقم ٥ لسنة ٢٠١٢م، والمنشور بالجريدة الرسمية بالعدد (٤٥٠) ملحق السنة الثانية والأربعون، والصادر بتاريخ ٢٠١٢/٨/٢٦م، والمعدل بموجب المرسوم بقانون اتحادي رقم ٢ لسنة ٢٠١٨م، والقانون المصري مكافحة جرائم تقنية المعلومات والاتصالات رقم ١٧٥ لسنة ٢٠١٨م.

وذلك من خلال النشرات التوعوية، والمحاضرات العلمية المتخصصة Conférences scientifiques spécialisées بهذا الشأن، والاستفادة في هذا الجانب من النشرات والأفلام التوعوية Dépliants et films de sensibilisation التي تعدها المنظمات والهيئات الدولية المتخصصة بمكافحة مثل هذه الجرائم، مع متابعة التطورات في مجال التقنيات الرقمية والجرائم المتعلقة بها، وتوظيف أحدث المستجدات الدولية بهذا الشأن في العمل الأمني؛ بما يسهم في الكشف عن جرائم تقنية المعلومات ويقود إلى التوصل لمعرفة مرتكبيها.

## الخاتمة

في خِتام هذه الدراسة، لنا مجموعة من النتائج لِمَا تم بحثه، ثم نُلْحِقُها بعدد من التوصيات؛ راجين من المُشرِّع والقضاء المُوَقَّر الأخذ بها لتقوية ودَعْمِ مواجهة الجريمة المعلوماتية وحصر أنواعها وتلافي أضرارها وبحث جوانبها القانونية؛ وذلك على النحو الآتي:

**أولًا: النتائج:**

اتَّضح للباحث أنه يصعب حصر أنواع الجريمة المعلوماتية؛ نظرًا للتطور والتعقيد السريع والشديد في ارتكابها وانتشارها. تَجلَّى للباحث أنَّ المشرع المصري قد اعتنى بصورة مُثلى بتشديد العقاب على مرتكب جريمة انتهاك حرمة الحياة الخاصة، سواء من خلال نصوص الدستور الحالي وقانون العقوبات أو قانون مكافحة جرائم تقنية المعلومات، ونصَّ على أنها جريمة عمدية يتخذ الركن المادي فيها أحد صور السلوك الإجرامي، والركن المعنوي فيها هو إرادة الجاني والعلم بكافة العناصر التي تكون الجريمة، فضلًا عن اتجاه إرادة الجاني إلى الفعل المُجرم وإلى تحقق النتيجة الإجرامية المترتّبة على السلوك الذي يقوم به، بالإضافة إلى توافر القصد الجنائي العام والخاص.

توصَّل الباحث إلى أنَّ المشرع المصري ما يزال يُطبِّق النصوص التقليدية الواردة في قانون العقوبات، التي تُجرِّم جريمتي السب والقذف، إلى أن تدخل بتعديل المادة (٣٠٦ مكررًا أ) من قانون العقوبات بتاريخ ٢٠٢١/٨/١٥م، بارتكاب الجريمة باستخدام وسائل الاتصالات السلكية أو اللاسلكية أو الإلكترونية، أو أية وسيلة تقنية أخرى. وقد تَبَيَّنَ للباحث أنَّ التجسس الإلكتروني هو إرهاب جديد لا يعتمد على استخدام الأسلحة والمتفجرات في حرب لا يُسمع فيها دوي الرصاص، وإنما تُستغَل التكنولوجية لدوافع سياسية واقتصادية واجتماعية ضدَّ أنظمة تكنولوجية الكمبيوتر والبيانات.

اتضح للباحث أنَّ جُلَّ التشريعات الجنائية المطبَّقة حاليًّا في معظم دول العالم ترتكز على الصفة الإقليمية فيما يتعلق بتطبيق قواعد الإجراءات الجنائية عن طريق السلطات غير الوطنية؛ لذلك فلا مناص من الاتفاقيات الثنائية والجماعية بين الدول لتسهيل تحقيق جرائم المعلوماتية، ورغم إبرام بعض الاتفاقيات إلا أنها لم تف بالغرض في حلِّ مشكلات

الاختصاص وتبادل الأدلة الجنائية وتسليم المجرمين؛ لذلك تبقى الحاجة جد ماسة إلى تشريعات جنائية أكثر مرونة حتى تواكب سرعة التقدم التكنولوجي وعصر المعلوماتية.

تَبَيَّنَ للباحث أنَّ الجريمة المعلوماتية تدخل في نطاق الجرائم المستثناة من تطبيق مبدأ الإقليمية؛ لأنها تُشكِّل خطرًا كبيرًا على قيم المجتمعات ومبادئها، فضلًا عن آثارها الضارة السياسية والاقتصادية.

ثانيًا: وقد انتهينا من خلال بحثنا إلى مجموعة من التوصيات ننادى بها في هذا المقام، منها:

نلتمس –استثناءً وحصرًا للجرائم الإلكترونية وإلزامًا– ضرورة أن يُرفق بأمر القبض على المتهم أمرٌ صادرٌ من النيابة العامة يتيح بموجبه وبرفقة عضو مأمور ضبط قضائي الاطلاع على هاتف المتهم أو أجهزة الحاسب الآلي المضبوطة، وبالأخص إعدادات الخصوصية لصفحة المتهم محلَّ الواقعة، وإجراء اللازم حيالها من تصوير وضبط محتواها ونحو ذلك؛ للوقوف على مدى توافر العلانية من عدمه؛ وذلك تطبيقًا وتدعيمًا لنص المادة (٥٧) من الدستور المصري الحالي والمادة (٩٥) من قانون الإجراءات الجنائية، ولتفادي صعوبة الإثبات.

ضرورة أن تُبادر وتسارع كلُّ دولة بوضع إطار قانوني خاص يُجرِّم استعمال أنظمة المعلوماتية لغايات غير مشروعة، وتحديد أشكال هذا النوع من الجرائم بشكل مفصل ومتجانس بين دول العالم يستوعب نطاق الأفعال المشكِّلة في الواقع لجرائم معلوماتية، بما من شأنه إيجاد تجانس بخصوص هذا النوع من الجرائم، وبالتالي إصباغ صفة العالمية على الجرائم المعلوماتية.

دعوة الفقه لدراسة ومعالجة موضوع المخاطر والتهديدات الناجمة عن الاستخدام غير المشروع لشبكة الإنترنت؛ لمواجهة جرائم تقنية المعلومات، والاعتماد على أساليب وتقنيات متطوِّرة؛ للتمكُّن من الكشف عن هوية مرتكب الجريمة والاستدلال عليه بأقل وقت ممكن، وتقديم الحلول وإيجاد المتشابهات من النماذج المنضبطة؛ لدعم وترسيخ ما يتوافق مع الإنصاف والتوازن بين الحريات المقررة وضبط مرتكبي الجرائم وتقديمهم للعدالة.

# قائمة المراجع

**أولًا: مراجع باللغة العربية:**

**أ- المؤلفات العامة والمتخصصة:**

**إبراهيم شمس الدين:** وسائل مواجهة الاعتداءات على الحياة الشخصية في مجال تقنية المعلومات، دار النهضة العربية، القاهرة، ٢٠٠٥م.

**أحمد فتحي سرور:** الحماية الجنائية للحق في الحياة الخاصة، القاهرة، دار النهضة العربية، ١٩٧٦م.

**أحمد فتحي سرور:** الوسيط في قانون العقوبات – القسم الخاص، دار النهضة العربية، القاهرة، ٢٠١٩م.

**جميل عبد الباقي الصغير:** الإنترنت والقانون الجنائي، الأحكام الموضوعية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، ٢٠٠١م.

**خالد ممدوح إبراهيم:** أمن الجريمة الإلكترونية، الإسكندرية، الدار الجامعية، ٢٠٠٨م.

**رمسيس بهنام:** القسم الخاص في قانون العقوبات، دار المعارف، الإسكندرية، ١٩٨٢م.

**السيد عتيق:** جريمة التحرش الجنسي، دراسة جنائية مقارنة، القاهرة، دار النهضة العربية، ٢٠٠٣م.

**السيد عوض:** الجريمة في مجتمع متغير، المكتبة المصرية، الإسكندرية، ٢٠٠٤م.

**طارق سرور:** قانون العقوبات القسم الخاص، جرائم الاعتداء على الأشخاص، دار النهضة العربية، ٢٠٠٣م.

**عبد الرحمن محمد العيسوي:** سبل مكافحة الجريمة، دار الفكر الجامعي، ٢٠٠٦م.

**عبد الفتاح بيومي حجازي:** الإثبات الجنائي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة، ٢٠٠٧م.

**عبد الفتاح بيومي حجازي:** جرائم الكمبيوتر والإنترنت في القانون الغربي والنموذجي، دراسة قانونية متعمقة في القانون المعلوماتي، دار الكتب القانونية، القاهرة، ٢٠٠٧م.

**عبد الفتاح حجازي بيومي:** مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، دار الفكر الجامعي، الإسكندرية، الطبعة الأولي، ٢٠٠٦م.

**عمار عباس الحسيني:** جرائم الحاسوب والإنترنت، الجرائم المعلوماتية، الطبعة الأولى، الناشر مكتبة زين الحقوقية والأدبية، لبنان، ٢٠١٧م.

**محمد جبر السيد عبد الله جميل:** جريمة التحرش الجنسي وعقوبتها في التشريع الإسلامي والقانون، دراسة مقارنة، الطبعة الأولى، بيروت، دار الكتب العلمية، ٢٠١٩م.

**محمد شوابكة:** جرائم الحاسوب والإنترنت، الجريمة المعلوماتية، دار الثقافة، عمان، ٢٠١١م.

**محمد ممدوح بدير:** مكافحة الجريمة المعلوماتية عبر شبكة الإنترنت والاستدلال كوسيلة لإثبات الجريمة المرتكبة عبر الإنترنت، دراسة مقارنة، مركز الدراسات العربية، الطبعة الأولي، ٢٠١٩م.

**محمد نصر محمد:** الوسيط في الجرائم المعلوماتية، مركز الدراسات للنشر والتوزيع، الطبعة الأولي، القاهرة، ٢٠١٥م.

**مدحت رمضان عبد الحليم:** الحماية الجنائية للتجارة الإلكترونية، دراسة مقارنة، الطبعة الأولي، دار النهضة العربية، ٢٠٠١م.

**ب- الرسائل والدوريات:**

**أشرف حسن محمد جواد:** الجريمة المعلوماتية والإلكترونية، أنوعها وخصائصها وطرق الوقاية منها، مجلة الدراسات المالية والمصرفية، الأكاديمية العربية للعلوم المالية والمصرفية، مركز البحوث المالية والمصرفية، المجلد (٢٣)، العدد الأول، ٢٠١٥م.

**أشرف محمد نجيب السعيد الدريني:** جرائم الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات، مجلة روح القوانين، العدد الخامس والتسعون، يوليو ٢٠٢١م.

**إلهام خليفة، جمال غرسي:** التجسس الإلكتروني كجريمة ماسة بأمن الدولة في التشريع الجزائري، مجلة دفاتر السياسة والقانون، المجلد (١٤)، العدد الأول، ٢٠٢٢م

**أوراق مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة المجرمين** المنعقد في فيينا، خلال الفترة من ١٠ وحتي ١٧ إبريل ٢٠٠٠م.

**خليل يوسف جندي:** المواجهة التشريعية للجريمة المعلوماتية على المستويين الدولي والوطني، دراسة مقارنة، مجلة كلية القانون للعلوم القانونية والسياسية، المجلد (٧)، العدد (٢٦)، ٢٠١٨م.

**شريهان ممدوح حسن:** الجرائم المعلوماتية وسبل مواجهتها على المستويين الوطني والدولي، المجلة الإلكترونية الشاملة متعددة المعرفة لنشر الأبحاث، العدد (٢١)، يناير ٢٠٢٠م.

**شوقي يعيش تمام، عزيزة شبري:** تفعيل مبدأ عالمية النص الجنائي في التصدي للجريمة المعلوماتية، مجلة الاجتهاد القضائي، العدد الخامس عشر، سبتمبر ٢٠١٧م.

**شيلان محمد شريف:** المواجهة الجنائية لانتهاك حرمة الحياة الخاصة، مجلة كلية القانون للعلوم القانونية والسياسية، جامعة كركوك، العراق، المجلد (١٢)، العدد (١٤)، ٢٠٢٣م.

**عادل يوسف عبد النبي الشكري، وآخرين:** الحماية الجزائية للأفراد في جريمة التحرش الجنسي، دراسة مقارنة، المجلد (١٣)، العدد (٤٤)، ٢٠٢٠م.

**عاصم الأمين قسم السيد الطاهر:** جرائم المعلوماتية وفقًا للقانون السوداني، دراسة مقارنة، مجلة الدراسات القانونية والاقتصادية، العدد الأول، المجلد التاسع، ٢٠٢٣م.

**عبد السلام عليلي:** جريمة القذف عبر مواقع التواصل الاجتماعي، دراسة تحليلية مقارنة بين التشريع الجزائري والتشريعات الأجنبية والعربية، مجلة الدراسات القانونية والاقتصادية، المجلد (٥)، العدد (٢)، ٢٠٢٢م.

**فاضلي سيد علي:** آثار التطور التكنولوجي على حماية الحق في الخصوصية في النظام الأوربي لحماية حقوق الإنسان، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد (٥)، العدد (٢)، ٢٠٢٠م.

**فضل الله محمد الحسن فضل الله:** جريمة انتهاك حرمة الحياة الخاصة في التشريع الإماراتي، دراسة تحليلية، مركز جيل البحث العلمي، مجلة جيل الأبحاث القانونية المعمقة، العدد (٤٤)، نوفمبر ٢٠٢٠م.

**مارية بوجداين، مريم آل سيدي الغازي:** تحديات مواجهة الجرائم المعلوماتية وآليات الحماية، بحث منشور بمجلة العلوم الجنائية، المركز المغربي للدراسات والاستشارات القانونية وحل المنازعات، العدد السابع، ٢٠٢١م.

**محمد أحمد السويحلي:** تكاتف الجهود العربية لمكافحة الجريمة الإلكترونية، مجلة الدراسات المالية والمصرفية، الأكاديمية العربية للعلوم المالية والمصرفية، مركز البحوث المالية والمصرفية، المجلد (٢٣)، العدد الأول، مارس ٢٠١٥م.

**محمد أحمد سليمان عيسي:** الجهود الدولية الإقليمية لمواجهة الجرائم الإلكترونية، مجلة العلوم القانونية، كلية القانون جامعة عجمان، السنة الرابعة، العدد الثامن، يوليو ٢٠١٨م.

**محمد بن أحمد على المقصودي:** الجرائم المعلوماتية: خصائصها وكيفية مواجهتها قانونًا، المجلة العربية للدراسات الأمنية، جامعة نايف العربية للعلوم الأمنية، المجلد (٣٣)، العدد (٧٠)، ٢٠١٧م.

**محمد بن حميد بن مضحي المزمومي:** جريمة التحرش الجنسي في النظام السعودي، دراسة مقارنة، مجلة العلوم القانونية والاقتصادية، كلية الحقوق، جامعة عين شمس، القاهرة، المجلد (٦١)، العدد (٢)، ٢٠١٩م.

**محمد عبد الله العوا:** جرائم الأموال عبر الإنترنت، رسالة دكتوراه، كلية الحقوق جامعة الإسكندرية، ٢٠١٣م.

**محمد عبد المحسن بن طريف، وآخرين:** جريمة السرقة المعلوماتية، مجلة الدراسات والبحوث القانونية، المجلد (٧)، العدد (٢)، ٢٠٢٢م.

**محمد فوزي إبراهيم:** نطاق تطبيق قانون العقوبات من حيث المكان على الجرائم المرتكبة في المحطات الفضائية، مجلة البحوث القانونية والاقتصادية، كلية الحقوق جامعة المنصورة، العدد (٧٥)، مارس ٢٠٢١م.

**مريم العوني:** جريمة التحرش الجنسي في القانون، رسالة ماجستير، كلية العلوم القانونية والاقتصادية والاجتماعية، جامعة القاضي رياض بمراكش، المغرب، ٢٠١٥م.

**المعتصم منجي محمود القطيشان:** جريمة الإرهاب باستخدام الوسائل الإلكترونية، رسالة ماجستير، كلية الحقوق جامعة الإسراء الخاصة، عمان، الأردن، ٢٠٢٢م.

**مليكة بن العربي وآخرون:** السلوك الإجرامي من منظور سيكولوجي، بحث منشور بمجلة القبس للدراسات النفسية والاجتماعية، العدد (١٤)، المجلد الأول، ٢٠٢٢م.

**ميثاء إسحاق عبد الرحيم الشيباني:** المسؤولية الجزائية عن جريمتي السب والقذف بالوسائل الإلكترونية، طبقًا للمرسوم رقم (٥) لسنة ٢٠١٢م، بشأن قانون مكافحة جرائم تقنية المعلومات، رسالة ماجستير، كلية القانون جامعة الإمارات العربية المتحدة، ٢٠١٨م.

**نسرين محسن نعمة:** جريمة الاحتيال المعلوماتي، دراسة مقارنة، بحث منشور بمجلة الكوفة للعلوم القانونية والسياسية، كلية القانون، جامعة الكوفة، المجلد ١١، العدد ٣٦، ٢٠١٨م.

**هدى أبو بكر سالم باجبير:** السب الإلكتروني.. حُكمه وصوره وعقوبته في الفقه والقانون، مجلة الفقه والقانون، العدد السادس والستون، إبريل ٢٠١٨م.

**هيا محمد عبد الله محمد الحميدي:** جريمتي القذف والسب الإلكتروني في القانون القطري، دراسة تحليلية مقارنة، رسالة ماجستير، كلية القانون جامعة قطر، ٢٠٢١م.

**وائل محمد نصيرات:** الجهود الدولية في مكافحة الجرائم المعلوماتية والصعوبات التي تواجهها، بحث مقدم للمؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية ICACC، جامعة الإمام محمد بن سعود الإسلامية، كلية علوم الحاسب والمعلومات، المملكة العربية السعودية الرياض، نوفمبر ٢٠١٥م.

**ج – تشريعات وقرارات:**

قانون العقوبات الإماراتي – قانون اتحادي – رقم ٣ لسنة ١٩٨٨م، الصادر بتاريخ ١٩٨٧/١٢/٨م، والمنشور بالجريدة الرسمية بالعدد (١٨٢)، السنة السابعة عشرة، والمعمول به اعتبارًا من ١٩٨٨/٣/٢٠م.

القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات، الصادر بتاريخ ٢٠١٨/٨/١٤م، والمنشور بالوقائع المصرية بالعدد (٣٢) مكررًا (ج) بتاريخ ٢٠١٨/٨/١٤م، والمعمول به من تاريخ ٢٠١٨/٨/١٥م.

القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات، الصادر بتاريخ ٢٠١٨/٨/١٤م، والمنشور بالوقائع المصرية بالعدد (٣٢) مكررًا (ج) بتاريخ ٢٠١٨/٨/١٤م، والمعمول به من تاريخ ٢٠١٨/٨/١٥م.

المؤتمر الخامس "جنيف ١٩٧٥م".

المؤتمر الدولي السادس بكركاس "فنزويلا" المنعقد في غضون عام ١٩٨٠م.

مؤتمر الأمم المتحدة السابع لمنع الجريمة ومعاملة المجرمين.

مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة السجناء بشأن الجرائم ذات الصلة بالكمبيوتر "هافانا"، لعام ١٩٩٠م.

قانون الأنسيترال بشأن التجارة الإلكترونية لعام ١٩٩٦م.

المنظمة العالمية للملكية الفكرية "وايبو" (WIPO).

اتفاقية برن الدولية لحماية المصنفات الأدبية والفنية.

اتفاقية تربسل لعام ١٩٤٤م.

مجموعة الدول الثمانية G8.

الاتفاقية الخاصة بحماية الأفراد من إساءة استخدام البيانات المعالجة إلكترونيًا لعام ١٩٨١م.

المعاهدة الأوروبية في مكافحة جرائم الإنترنت "اتفاقية مجلس أوروبا بشأن الإجرام السيبيري لعام ٢٠٠١م".

المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات ١٩٩٤م بالبرازيل بشأن جرائم الكمبيوتر.

الاتفاقية الأمريكية المتعلقة بجرائم الحاسب الآلي والإنترنت لسنة ١٩٩٩م.

قانون نظام مكافحة المعلوماتية بالمملكة العربية السعودية، الصادر بموجب قرار مجلس الوزراء رقم ٧٩، والصادر بتاريخ ١٤٢٨/٣/٧هجريًا، والمصدق عليه بالمرسوم الملكي رقم ١٧م، الموافق ١٤٢٨/٣/٨ هجريًا، والصادر بالقرار رقم ١١٥٦٧/ب، بتاريخ ١٤٢٨/٣/٩ هجريًا.

القانون الاتحادي بدولة الإمارات العربية المتحدة رقم ٥ لسنة ٢٠١٢م، والمنشور بالجريدة الرسمية بالعدد (٤٥٠) ملحق، السنة الثانية والأربعون، والصادر بتاريخ ٢٠١٢/٨/٢٦م، والمعدل بموجب المرسوم بقانون اتحادي رقم ٢ لسنة ٢٠١٨م.

دستور الإمارات العربية المتحدة لسنة ١٩٧١م، الصادر بتاريخ ١٩٧١/٧/١٨م، والمنشور بالجريدة الرسمية بالعدد رقم (١) السنة الأولى، بتاريخ ١٩٧١/١٢/٣١م، والمعمول به اعتبارًا من ١٩٧١/١٢/٢م.

قانون العقوبات المصري رقم ٥٨ لسنة ١٩٣٧م، الصادر بتاريخ ١٩٣٧/٧/٣١م، والمنشور بالوقائع المصرية بالعدد (٧١)، بتاريخ ١٩٣٧/٨/٥م، والمعمول به بتاريخ ١٩٣٧/١٠/١٥م.

قانون تنظيم الاتصالات رقم ١٠ لسنة ٢٠٠٣م، الصادر بتاريخ ٢٠٠٣/٢/٤م، والمنشور بالجريدة الرسمية بالعدد رقم (٥) مكررًا (أ)، بتاريخ ٢٠٠٣/٢/٤م، والمعمول به اعتبارًا من ٢٠٠٣/٢/٥م.

الدستور المصري الحالي لسنة ٢٠١٤ الصادر بتاريخ ٢٠١٤/١/١٨م، والمنشور بالجريدة الرسمية بالعدد (٣) مكررًا (أ) بتاريخ ٢٠١٤/١/١٨م، والمعمول به اعتبارًا من ٢٠١٤/١/١٨م، بشأن إصدار دستور جمهورية مصر العربية المعدل لسنة ٢٠١٤م.

القرار الجمهوري رقم ٢٧٦ لسنة ٢٠١٤، الصادر بتاريخ ٢٠١٤/٨/١٩م، والمنشور بالجريدة الرسمية بالعدد رقم (٤٦) بتاريخ ٢٠١٤/١١/١٣م، والمعمول به اعتبارًا من ٢٠١٤/١٠/٨م.

قانون الإجراءات الجنائية رقم ١٥٠ لسنة ١٩٥٠م، الصادر بتاريخ ١٩٥١/٩/٣م، والمنشور بالوقائع المصرية بالعدد (٩٠)، والمعمول به اعتبارًا من ١٩٥١/١١/١٤م، بشأن إصدار قانون الإجراءات الجنائية.

**د- أحكام قضائية:**

حكم المحكمة الاقتصادية في الدعوى رقم ٦٩٠ لسنة ٢٠١٢ قضائية والصادر بجلسة ٢٠١٢/١١/٢٤م.

حكم محكمة النقض –جنائي– في الطعن رقم ١١٤٤٨ لسنة ٩٠ قضائية –جنح اقتصادي، والصادر بجلسة ٢٠٢١/٣/١٤م.

حكم محكمة النقض في الطعن رقم ١٩٩٠ لسنة ٨ قضائية، والصادر بجلسة ٢٠٢٠/٢/٤م.

حكم محكمة النقض في الطعن رقم ٣٢٦١١ لسنة ٨٦ قضائية، والصادر بتاريخ ٢٠١٧/٩/١٦م، مكتب فني ٦٨، ص٥٨١، ق٦٢.
حكمة محكمة النقض في الطعن رقم ٢٩٩٥٣ لسنة ٨٦ قضائية، والصادر بجلسة ٢٠١٧/٤/٢٧م، مكتب فني ٦٨، رقم الصفحة ٣٠٣، رقم القاعدة ٣٨.

**هـ- المواقع الإلكترونية:**

. (الموسوعة القانونية لوزارة العدل المصرية)https://emj-eg.com
. (شبكة قوانين الشرق)https://www.eastlaws.com
CONVENTIONS.CO.INT.

**ثانيًا: المراجع الفرنسية:**

I- Ouvrages

**١- المراجع**

1- Cazeneuve Jean, La cybercriminalité: l'émergence d'un nouveau risque, AJ Pénal, 2012.
2- Duflot F., «Phishing: les dessous de la contrefaçon», RLDI 2006/01.
3- Féral-Schuhl Christiane, Praxis Cyberdroit, Livre 7 - Lutte contre la cybercriminalité, Dalloz, 2021.

II- Décrets et réglementations

**٢- المراسيم والتنظيمات القانونية**

1- Décr. no 2017-58, 23 janv. 2017 instituant un délégué ministériel aux industries de sécurité et à la lutte contre les cybermenaces au ministère de l'Intérieur, JO 24 janv., no 29.

III- Jurisprudence

**٣- الأحكام القضائية**

1- TGI Nanterre, ord. ME, 11 oct. 2012, www.legalis.net.
2- Crim. 6 mars 2018, no 16 - 87.533.
3- Cons. const. 21 mars 2019, no 2019-778 DC

IV- Sites Internet

**٤- مواقع الإنترنت**

- https://www.eastlaws.com
- https://emj-eg.com
- https://www.eastlaws.com
- www.legalis.net.