Dirassat & Abhath
The Arabic Journal of Human and Social Sciences

مجلة دراسات وأبحاث
المجلة العربية في العلوم الإنسانية والاجتماعية

EISSN: 2253-0363
ISSN : 1112-9751

الطبيعة الخاصة للجريمة المعلوماتية

The specific nature of cybercrime

حبيباتني بثينة Habibatni boutheina
جامعة الجزائر 1 بن يوسف بن خدة Université d'Alger 1 Benyoucef Ben khedda
boutheinahabibatni25@gmail.com

تاريخ الاستلام : 2019-02-17 تاريخ القبول : 2020-06-13

ملخص:

لقد أضفى التطور الهائل لتقنية المعلومات واندماجها بتقنية الاتصالات فيما بعد طبيعة خاصة على جرائم كانت تقليدية قبل ظهورها، وأدى إلى ظهور أنماط مستحدثة من الأفعال الجرمية تباينت التعبيرات والاصطلاحات للدلالة على هذه الجرائم تباين رافق مسيرة ونشأة تلك التقنية، وأحاط بها الكثير من التساؤلات التي تتعلق بتحديد ماهيتها باعتبارها جريمة مستحدثة ومتميزة عن باقي الجرائم التقليدية من خلال موضوعها وخصائصها، وكذلك تعدد المحاولات الرامية إلى تصنيفها وتحديد صورها المختلفة.

كلمات مفتاحية: الجريمة المعلوماتية، الجريمة الالكترونية، الجريمة السيبرانية، الجريمة المتصلة بتكنولوجيات الإعلام والاتصال، المجرم المعلوماتي، تصنيفات الجريمة المعلوماتية

Abstract :

The tremendous development of information technique and its integration with the communication technique has added a specific nature of crimes that was ancient before its emergence, that led to the appearance and emergence of and new types of criminal acts, the terminologies and the changes that was used to denote these crimes which related to identify its nature considering it a new and special crime different from the rest of ancient crimes through its subject and its characteristic; moreover, the multiplicity of attempts to classify and identify it different forms .

Keywords: information crime, electronic crime, cybercrime, crime related to information and communication technologies, categories of cybercrime.

مقدمة:

لما كانت الجرائم المعلوماتية هي ظاهرة حديثة النشأة لارتباطها بتكنولوجيا حديثة، فقد ترتب عن ذلك إحاطة هذه الظاهرة بكثير من الغموض حتى دعا ذلك الكثيرين إلى القول بأن الجريمة المعلوماتية هي أشبه بالخرافة، وأنه لا يوجد تهديد حقيقي منبعه الحاسبات الآلية، وأن كل سلوك غير مشروع قد يرتبط بالحاسبات الآلية في حقيقتها جرائم عادية، دون أن تتميز بأية سمات خاصة.

ولهذا فقد اعتبرت الجريمة المعلوماتية ما هي إلا امتداد للجرائم التقليدية، وفقا لمنظور تطور الجريمة من حيث الزمان، وبذلك فإنها تتأثر تأثرا واضحا بمراحل التطورات المختلفة التي يمر بها المجتمع وتتفاعل مع معطياته بما يساير هذا التطور، وبالتالي أي ظاهرة مستحدثة تعتبر امتداد لهذا التطور، إلا أنه إذ كان ذلك صحيحا في بعض الحالات فإن كثيرا من الجرائم المعلوماتية تنفرد بمجموعة من الخصائص والسمات التي تميزها عن غيرها من الجرائم التقليدية.

ولما كانت الجريمة المعلوماتية ترتبط بوسائل تقنية المعلومات الحديثة، والتي ما إن انتشرت إلا وأدى ذلك إلى انتشار الجرائم المصاحبة لها، وبهذا الوضع أصبح المشرع أمام أفعال جرمية لم تكن موجودة في السابق، خاصة وأن التطور المستمر لكل من تكنولوجيا المعلومات وتكنولوجيا الاتصالات أدى إلى عدم تبلور مفهوم واضح لماهية الجريمة المعلوماتية، وعدم التوصل إلى نموذج موحد متفق عليه في تحديد أنماط السلوك الإجرامي.

وتظهر أهمية هذا الموضوع في الدور الذي تلعبه وسائل تقنية المعلومات الحديثة في حياتنا اليومية، وتأثيره على مظاهر هذه الحياة في جميع مجالاتها، ومدى الحاجة لبحث ظاهرة جرائم المعلوماتية والعمل

على خلق إطار قانوني لها، يقوم على تعريفها وتصنيفها وضبطها لكونها تختلف عن الجرائم التقليدية.

فلقد بتنا أمام ظاهرة إجرامية تتميز من حيث موضوع الجريمة ووسيلة ارتكابها وسماتها وأنماط السلوك الإجرامي المكون لها، الأمر الذي يدعونا إلى تحديد ماهيتها وأهم تصنيفاتها لكي نتمكن من مواجهتها.

لهذا أحاط بالجريمة المعلوماتية شأنها في ذلك شأن كل ظاهرة جديدة الكثير من التساؤلات والغموض حول ماهيتها وكذا التعرف على أهم تقسيماتها، إذ أنها تمثل خطوة أولى للتعرف على هذه الظاهرة من جميع جوانبها القانونية.

وعليه يستوجب علينا لمعرفة الطبيعة الخاصة للجريمة المعلوماتية الإجابة على الإشكالية التالية: **إلى أي مدى استطاع الفقه والتشريع تجسيد فكرة الذاتية والتميز لتحديد معالم الجريمة المعلوماتية؟.**

ونظرا لطبيعة البحث سأعتمد على المنهج الوصفي التحليلي، وذلك بوصف الجريمة المعلوماتية وتحديد أهم الخصائص المميزة لها، بالإضافة إلى تحليل أهم الاتفاقيات التي تناولت الجريمة المعلوماتية لمعرفة تصنيفات هاته الأخيرة، وذلك من خلال تقسيم الدراسة إلى مطلبين، نتناول في المطلب الأول ماهية الجريمة المعلوماتية، أما المطلب الثاني نخصصه لدراسة المحاولات المختلفة لتصنيفات جرائم المعلوماتية.

2.المطلب الأول: ماهية الجريمة المعلوماتية

لقد أوجدت وسائل التقنية العالية ألوانا جديدة من الجرائم لم تكن موجودة من قبل، إذ أسبغت عليها خصائص مميزتها عن غيرها من الجرائم.

ومما لا شك فيه أن الجرائم الالكترونية تختلف عن الجرائم التقليدية من ناحية الأفعال الإجرامية، إذ يتدخل الجاني من خلال ارتكاب الجريمة في مجال المعالجة الالكترونية للبيانات ومن ثم فليس من المستغرب أن تختلف عن مثيلاتها من الجرائم التقليدية في بعض الصفات التي تميزها عن غيرها، وكذلك أساليب ارتكابها.

فنتيجة التطور المستمر واللامتناهي لتكنولوجيا المعلومات والاتصالات حتى الآن، حال ذلك دون وضع تعريف فقهي جامع وشامل لمفهوم الجريمة الالكترونية، لذلك بذل المهتمون بدراسة هذا النمط الجديد من الإجرام جهدا كبيرا من أجل الوصول إلى تعريف مناسب يتلاءم مع طبيعة الجريمة الالكترونية.

ومما لا شك فيه أن عدم وضع تعريف للجريمة الالكترونية يثير العديد من المشكلات لعل أهمها صعوبة مواجهتها وتعذر إيجاد الحلول المناسبة لمكافحتها.

وعليه سنحاول التطرق إلى ماهية الجريمة الالكترونية، حيث نتعرض لمختلف التعريفات التي استند عليها الفقهاء في تعريفهم للجريمة الإلكترونية، ثم نتناول خصائص الجريمة الالكترونية.

1.2 الفرع الأول: تعريف الجريمة المعلوماتية

المتتبع لظاهرة الجريمة المستحدثة التي أوجدتها ثورة الاتصالات وتقنية المعلومات عبر العالم، سواء على النطاق العربي أو الدولي، يلحظ أزمة تتعلق بالمصطلح اللازم والكافي لنعت هذا النوع المستحدث من الجرائم، وعلى وجه يكفي للدلالة على حقيقة المسمى[1].

ومثلما تعددت التسميات التي أطلقت على هذا النوع من الجرائم كذلك تعددت التعريفات، إذ لم يتفق الفقه على تعريف محدد للجرائم المتصلة بتكنولوجيات الإعلام والاتصال، إذ انعكست هذه الظاهرة في نشأتها نسبيا على اتجاهات العديد من الفقهاء الجنائيين حول وضع تعريف جامع وموحد لها، بل أن البعض ذهب إلى ترجيح عدم وضع تعريف بحجة أن هذا النوع من الجرائم ما هو إلا جريمة تقليدية ترتكب بأسلوب الكتروني[2].

إذ تعد مسألة وضع تعريف للجريمة المعلوماتية من المسائل الشائكة التي تقف كحجر عائق أمام رجال القانون، إذ أنه وحتى الآن يصعب وضع تعريف عام وشامل لها، وهذا ما أكدته قمة برلين[3].

ولقد بذل المهتمون بدراسة هذا النمط الجديد من الإجرام جهدا كبيرا من أجل الوصول إلى تعريف مناسب يتلاءم مع طبيعة الجريمة الالكترونية، إلا أن كثيرا من هذه المحاولات قد باءت بالفشل حتى أنه قيل أن هذه الجريمة تقاوم التعريف[4].

وسنحاول الوصول إلى التعريف الذي يتلاءم مع طبيعة هذه الجريمة، وذلك بعد التعرض للاتجاهات المختلفة في تعريف هذه الجريمة، إذ تقسم هذه التعريفات إلى طائفة التعريفات التي تستند على معيار واحد كتعريفها بدلالة وسيلة ارتكابها أو بالاستناد إلى محل أو موضوع الجريمة ، وتشتمل أيضا تعريفات قائمة على معيار شخصي، وتعريفات أخرى قائمة على معايير متعددة.

-أولا: التعريفات التي تستند إلى أداة ارتكاب الجريمة:

يستند أنصار هذا الاتجاه في تعريفهم لجرائم الحاسوب إلى وسيلة ارتكاب الجريمة فيشترطون وجوب ارتكابها بواسطة الكمبيوتر، ومن هذه التعريفات الأستاذة L D Ball أنها "فعل إجرامي يستخدم الكمبيوتر في ارتكاب كأداة رئيسية"[5]، ويعرفها tiedermann بأنها "كل فعل غير مشروع يرتكب باستخدام الحاسوب"[6].

وكذلك يعرفها مكتب التقنية بالولايات المتحدة الأمريكية بأنها "الجريمة التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسا"[7]، كما اعتمد نظام مكافحة جرائم المعلوماتية السعودي لسنة 2007 هذا الاتجاه لتعريف تلك الجرائم إذ عرفها بأنها "أي فعل يرتكب متضمنا استخدام الحاسب أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام"[8].

ومن جانب آخر ذهب جانب من الفقه في إطار تعريف الجريمة المعلوماتية بالاستناد إلى الوسيلة المرتكبة إلى ضرورة ربط الجريمة وغاياتها، فجعلها جريمة معلوماتية ليس فقط باستخدام الحاسب الآلي فقط كوسيلة رئيسية، بل لابد لتحقيق المفهوم بنظرهم من ظهور الغاية لدى الفاعل لتحقيق شيء معين، ومن قبيل هذه التعريفات تعريف الفقيه Masse إذ يقول أن الجريمة المعلوماتية هي" اعتداءات غير مشروعة ترتكب بواسطة المعلوماتية بغرض تحقيق ربح"[9].

وقد وجه لهذه التعريفات النقد، ومن هذه الانتقادات ما يراه الأستاذ John Taberو Michael Rostoker و Robert Rines أنه يستوجب لتعريف الجريمة الرجوع إلى العمل الأساسي المكون لها وليس فحسب الوسائل المستخدمة لتحقيقه، ويعزز هذا النقد الأستاذ Anderson أنه ليس لمجرد أن الحاسب قد استخدم في الجريمة أن نعتبرها من الجرائم المعلوماتية[10]، كما أنتقد التعريف الذي ربط الجريمة بغايتها لأنه اعتد بالباعث على الجريمة في حين أن القانون الجنائي لا ينظر إلى البواعث على ارتكاب الجريمة ومع ذلك جاء قاصرا أيضا في تحديد الباعث، إذ أن هناك الرغبة في الانتقام والتدمير[11].

ومن جانبنا نرى أن هذا الاتجاه غير صائب إذ أنه يغفل جانبا كبيرا من الجرائم المعلوماتية وهي التي تكون محلها مفردات الحاسب الآلي المعنوية منها تحديدا أي نظم المعالجة الآلية للمعطيات، كما أن هذا التعريف غير منطقي لأنه لم يبين أنه خاص ببعض الجرائم التي لا يتصور وقوعها إلا بواسطة الحاسب الآلي، كما نرى أن استخدام الحاسب الآلي لا يضيف إلى السلوك غير مشروع جديد، فهو مجرد وسيلة.

- ثانيا: التعريفات التي تستند إلى محل أو موضوع ارتكاب الجريمة

لم يركز أصحاب هذا الاتجاه اهتمامهم على الوسيلة المستخدمة في الجريمة وإنما ركزوا على موضوع الجريمة، أي عندما يكون الكمبيوتر هو محل الجريمة، ولا نعني بذلك سرقة الحاسب الآلي، وإنما تشمل كل شيء غير ملموس مرتبطا بالكمبيوتر أي الكيان المنطقي كالمعلومات المخزنة في الذاكرة[12].

وقد عرفتها الدكتورة هدى قشوش بأنه "كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات[13]، كما عرفها البعض على النحو التالي: "كل سلوك سلبي أو إيجابي يتم بموجبه الاعتداء على البرامج أو المعلومات للاستفادة منها بأية صورة كانت"[14]، ويعرف خبراء منظمة التعاون الاقتصادي والتنمية الجريمة المعلوماتية "بأنها كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات و/أو نقلها"[15].

ويظهر لنا من خلال هذه التعريفات أنها وفقت لحد ما، إذ جعلت المصلحة المحمية في هذه الجريمة هي المعطيات، كما لم تحصر الجريمة المعلوماتية على جهاز الحاسب الآلي وحده بل اعتمدت في التعريف اللغة المعلوماتية أي كل ما يتعلق بالمعالجة الآلية للمعطيات، الأمر الذي يؤدي إلى إمكانية احتواء الأجهزة العالية التقنية الأخرى كالهواتف الذكية والتي من المتصور وقوع أو حدوث سلوك إجرامي بها أيضا.

- ثالثا: التعريفات التي تستند إلى سمات الجاني الشخصية

هناك اتجاه فقهي آخر لا يهتم بالوسيلة أو موضوع الجريمة المعلوماتية ويعرفها بوصفها مرتبطة بالمعرفة التقنية أو الفنية لاستخدام الحاسب الآلي.

ومن هذه التعريفات التي تنهض على أساس سمات شخصية لدى مرتكب الفعل وهي بالتحديد سمة الدراية والمعرفة التقنية تعريف وضعته وزارة العدل الأمريكية في دراسة أعدها معهد ستانفورد للأبحاث واعتمدتها هذه الوزارة في دليلها لعام 1979 والذي يقول "أي جريمة لفاعلها معرفة فنية بالحاسبات تمكنه من ارتكابه"[16]، ومن بين هذه التعريفات أيضا تعريف David Thompson بأنها "أي جريمة يكون متطلبا لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب"[17]، وفي ذات الاتجاه عرفها الدكتور هشام فريد رستم بأنها " أي فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبه"[18].

ويبدو من خلال هذه التعاريف أن الجرائم التي تفتقر إلى هذه الدرجة من المعرفة لا تعد من طائفة الجرائم المعلوماتية، فتعريف الجريمة وفقا لهذا الاتجاه يعد أمرا قاصرا ولا يحيط بحقيقة الأفعال غير المشروعة ولا يساهم في توضيح تلك الجرائم.

-رابعا: التعريفات التي تستند إلى أداة وموضوع ارتكاب الجريمة

توجد تعريفات تعتمد أكثر من معيار، فيعرف جانب من الفقه الجريمة المعلوماتية وفق معايير قانونية متعددة، وعلى ذلك يعرفها الأستاذ Thomas J Smedinghoff بأنها "أي ضرب من النشاط

الموجه ضد أو المنطوي على استخدام نظام الحاسوب"[19]، وقد عرفها أيضا خبراء متخصصون من بلجيكا في معرض ردهم على استبيان منظمة التعاون الاقتصادي والتنمية OECD بأنها "كل فعل أو امتناع من شأنه الاعتداء على الأمواج المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية"[20]، وقد جاء كذلك في توصيات مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين المنعقد في فينا لسنة 2000 تعريف الجريمة المعلوماتية كما يلي: "أية جريمة يمكن ارتكابها بواسطة نظام أو شبكة معلوماتية أو داخل نظام أو شبكة معلوماتية، أو ضد النظام أو الشبكة المعلوماتية"[21]، وفي ذات المقام عرفت الجريمة المعلوماتية بالاعتماد على عدة أسس كالآتي:"كل نشاط إيجابي أو سلبي من شأنه الاتصال دون وجه حق بالكيان المعنوي للحاسب الآلي أو بنظام المعلومات العالمية، أو الإبقاء عليه عند تحققه، أو التأثير عليه بتعطيله أو إضعاف قدرته على أداء وظائفه بالنسخ أو التعديل بالإضافة أو الحذف الكلي أو الجزئي أو بالمناقلة للخصائص الأساسية للبرامج، أو مجرد النسخ أو الوصول إلى البرامج، أو المعلومات المخزنة أو الوصول إليها أثناء نقلها أو إرسالها أو الاتصال بها من غير وجه حق بأي وسيلة كانت"[22].

والملاحظ على هذا التعريف أنه جاء شاملا، حيث اعتبر النشاط الإجرامي الذي يقدم عليه الجاني يكون في شكل فعل إيجابي أو سلبي هذا من جهة، ومن جهة أخرى ذكر محل الجريمة والمتمثل في الكيان المعنوي للحاسب الآلي أو نظم المعلومات العالمية، كما بين مختلف الأفعال غير المشروع، بالإضافة إلى هذا فإن النشاط الإجرامي يتحقق بأية وسيلة كانت.

ومن خلال استعراضنا للتعريفات الفقهية نتوصل إلى أن الإخفاق في تعريف الجريمة المعلوماتية يسمح إلى إضفاء وصف الجريمة المعلوماتية على أي سلوك غير مشروع تكون تقنية المعلومات وسيلة لارتكاب الجريمة، أو تكون موضوعا لها، وعليه فإننا نقترح التعريف التالي: تعد جريمة معلوماتية كل سلوك غير مشروع يرتكب على أنظمة المعالجة الآلية للمعطيات، وكذلك كل جريمة تقليدية يمكن ارتكابها أو يسهل ارتكابها بواسطة وسائل تقنية المعلومات.

وبهذا نكون قد سايرنا المشرع الجزائري في تعريفه للجرائم المتصلة بتكنولوجيات الإعلام والاتصال من خلال المادة الثانية من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها والتي جاءت كما يلي:

يقصد بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال: "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية"[23].

2.2 الفرع الثاني: خصائص الجريمة المعلوماتية وسمات الجاني المعلوماتي

مما لاشك فيه أن الجريمة المعلوماتية تعد من أخطر الجرائم[24]، كما تتميز عن غيرها من الجرائم التقليدية لارتباطها بتكنولوجيات الإعلام والاتصال، الأمر الذي أضفى عليها طابعا خاصا، وسنحاول فيما يلي التطرق إلى خصائصها وسمات الجاني كما يلي:

-أولا: خصائص الجريمة المعلوماتية

إن ضبط خصائص الجريمة المعلوماتية وحصر ما يميز هذا النمط المستحدث نسبيا من الإجرام عن غيره من الإجرام التقليدي، يسهل عمل المشرع ويمكنه من صياغة النصوص التشريعية الملائمة لمكافحة هذه الجرائم.

وللجريمة المعلوماتية مجموعة من الخصائص تميزها عن غيرها من الجريمة التقليدية، وبسبب هذه المميزات فرضت الجريمة المعلوماتية نفسها على فقهاء القانون.

ومن أبرز خصائص الجريمة المعلوماتية يمكن ذكر ما يلي:

أ-الجرائم المعلوماتية من الجرائم العابرة للحدود: فلقد أتاحت شبكة الانترنت إمكانية الاتصال بين عدة حاسبات آلية مهما كانت المسافة الفاصلة بينهما، حيث لم يعد هناك ما يحول دون تبادل المعلومات ونقلها بكميات مذهلة وبسرعة هائلة، وقد أدى ذلك إلى نتيجة مفادها أن عدة أماكن متفرقة في دول مختلفة قد تتأثر بالجريمة المعلوماتية الواحدة وفي آن واحد، حيث أنه غالبا ما يكون الجاني في بلد، والمجني عليه في بلد آخر، كما قد يكون الضرر المتحصل في بلد ثالث في الوقت نفسه، وعليه تعتبر الجريمة المعلوماتية شكلا جديدا من الجرائم العابرة للحدود الوطنية أو الإقليمية أو القارية[25].

ب-صعوبة اكتشاف الجرائم المعلوماتية: نظرا لعدم ترك الجاني آثار خارجية بصورة مرئية أو ملموسة في أغلب الأحيان، وكذلك قدرته على تدمير دليل الإدانة في أقل من الثانية الواحدة، فتغيير بيانات الحاسب الآلي أو التلاعب بالمعطيات وغيرها من الجرائم يتم بواسطة إدخال رموز وأرقام، وهي أمور تقنية تتسم بتعقيدها وصعوبة اكتشافها، وعادة يتم اكتشاف الجريمة بمحض الصدفة، فالرقم المظلم بين حقيقة عدد هذه الجرائم وعدد الجرائم التي تم اكتشافها والإبلاغ عنها، هو رقم خطير[26].

كما يكون للمجني عليه دورا أساسيا في صعوبة اكتشافها، حيث تحرص أغلب الجهات التي تتعرض أنظمتها المعلوماتية للقرصنة

والانتهاك إلى عدم إبلاغ السلطات المختصة تجنبا للإضرار بسمعتها ومكانتها وهز الثقة في كفاءتها[27].

ج-صعوبة إثبات الجريمة المعلوماتية: ففي حال اكتشاف الجريمة المعلوماتية، فإن إثباتها أمر تحيط به الكثير من الصعاب، فالجريمة المعلوماتية تتم في محيط غير تقليدي حيث تقع خارج إطار الواقع المادي الملموس لتقوم أركانها في بيئة الحاسوب والانترنت مما يجعل الأمور تزداد صعوبة وتعقيدا لدى سلطات البحث والتحري والتحقيق، ففي هذا البيئة تكون البيانات والمعلومات عبارة عن نبضات الكترونية غير مرئية تنساب عبر النظام المعلوماتي، مما يجعل أمر محو الدليل وطمسه آليا من قبل المجرم أمرا في غاية البساطة والسهولة[28].

ومما يزيد الأمر صعوبة ضعف خبرة الشرطة ومعرفتهم الفنية بأمور الحاسب الآلي سواء تمثل الضعف في تحليل الدليل المعتبر، أم في انتشال ذلك الدليل[29].

د-سهولة ارتكاب الجريمة المعلوماتية:إن الجرائم المعلوماتية هي جرائم هادئة بطبيعتها، لا تحتاج إلى العنف، بل كل ما تحتاج إليه هو القدرة على التعامل مع جهاز الحاسوب بمستوى تقني يوظف في ارتكاب الأفعال غير المشروعة، كما تحتاج كذلك إلى وجود الانترنت مع وجود مجرم يوظف خبرته أو قدرته على التعامل مع الشبكة للقيام بجرائم مختلفة كاختراق خصوصيات الغير أو التجسس أو الاحتيال[30].

هـ-الجريمة المعلوماتية تتم عادة بتعاون أكثر من شخص: تتميز الجريمة المعلوماتية أنها تتم عادة بتعاون أكثر من شخص على ارتكابها، فغالبا ما يشترك في إخراج الجريمة إلى حيز الوجود شخص متخصص في تقنيات الحاسوب والانترنت، يقوم بالجانب الفني من المشروع الإجرامي، وشخص أخر من خارج المؤسسة المجني عليها لتغطية عملية التلاعب وتحويل المكاسب إليه، والاشتراك في إخراج الجريمة المعلوماتية إلى حيز الوجود قد يكون اشتراكا سلبيا، وهو الذي يتضح بالصمت من جانب من يعلم بالجريمة في محاولة منه لتسهيل إتمامها، وقد يكون اشتراكا ايجابيا وهو الغالب في الكثير من الجرائم ويتمثل في المساعدة الفنية أو المادية[31].

- ثانيا: سمات الجاني المعلوماتي

يتصف المجرم المعلوماتي بخصائص معينة تميزه عن المجرم الذي يرتكب الجرائم التقليدية، وقد جعلت منه محلا للعديد من الأبحاث والدراسات، وسوف نتطرق فيما يلي لأهم سمات المجرم المعلوماتي ونحدد فئاته.

أ-المجرم المعلوماتي كإنسان يتمتع بالمهارة والمعرفة والذكاء[32]: يتميز المجرم المعلوماتي غالبا بالذكاء، حيث يستخدم مقدرته العقلية ولا يلجأ إلى استخدام العنف بل يحقق هدفه الإجرامي بهدوء، فالإجرام المعلوماتي هو إجرام الأذكياء بالمقارنة بالإجرام التقليدي الذي يميل إلى العنف[33].

فالمجرم المعلوماتي مجرم محترف، ذلك أنه لا يمكن للشخص العادي-إلا في حالات قليلة- أن يرتكب جرائم عن طريق الكمبيوتر، فالأمر يقتضي كثيرا من الدقة والتخصص في هذا المجال للتوصل إلى التغلب على العقبات التي أوجده المتخصصون لحماية المنظومة المعلوماتية[34]، إلا أن ذلك لا يعني أن يكون المجرم المعلوماتي على قدر كبير من العلم في مجال تكنولوجيا المعلومات وأن تكون له خبرة كبيرة فيه بل الواقع العلمي أثبت أن بعض أنجح مجرمي المعلوماتية لم يتقلى المهارة اللازمة لارتكاب الجريمة عن طريق التعليم أو الخبرة المكتسبة أثناء العمل في هذا المجال[35].

ب-المجرم المعلوماتي إنسان اجتماعي: المجرم المعلوماتي بصفته إنسان ذكي فهو اجتماعي، فهو لا يضع نفسه في حالة عداء مع المجتمع الذي يحيط به، بل انه إنسان يستطيع التوافق والتصالح مع مجتمعه، فهو شخص مرتفع الذكاء مما يساعده على عملية التكيف مع المجتمع، فالذكاء في نظر الكثيرين ليس سوى القدرة على التكيف، ولا يقصد بذلك التقليل من شأن المجرم المعلوماتي، بل أن خطورته الإجرامية قد تزداد إذا زاد تكيفه الاجتماعي مع توافر الشخصية الإجرامية لديه[36].

ج-المجرم المعلوماتي يتمتع بالسلطة اتجاه النظام المعلوماتي: نعني بالسلطة المزايا والحقوق التي يتمتع بها المجرم المعلوماتي، والتي تمكنه من ارتكاب جريمته، فمعظم مجرمي المعلوماتي لديهم سلطة مباشرة أو غير مباشرة في مواجهة المعلومات محل الجريمة، وقد تتمثل هذه السلطة في الرقم السري الخاص للولوج إلى النظام الذي يحتوي على المعلومات، والتي تمد الفاعل بمزايا متعددة كفتح الملفات وقراءتها وكتابتها ومحو المعلومات أو تعديلها، وقد تتمثل هذه السلطة في الحق استعمال الأنظمة المعلوماتية، أو إجراء بعض التعاملات، أو مجرد الدخول إلى الأماكن التي تحتوي على هذه الأنظمة[37].

د-المجرم المعلوماتي يبرر ارتكابه الجريمة: يتولد لدى المجرم المعلوماتي إحساس وشعور بأن ما يقوم به لا يعتبر من عداد الجرائم، أي أن هذا الفعل لا يمكن أن يصنف بعدم الأخلاقية وخاصة في الحالات التي يقف فيها السلوك عند حد قهر نظام الحاسوب وتخطي الحماية الأمنية، حيث يميز مرتكبو هذه الجرائم بين الإضرار بالأشخاص الأمر الذي يعدونه غاية في أللأخلاقية وبين الإضرار بمؤسسة أو جهة في استطاعتها اقتصاديا تحمل نتائج تلاعبهم[38].

هـ-تعدد أنماط المجرم المعلوماتي: من بين أفضل التصنيفات لمجرمي تقنيات المعلومات التصنيف الذي أورده كل Karl Seger و David وWilliam vonstorch في مؤلفهم جرائم الكمبيوتر الصادر عام 1995 حيث تم تقسيم مجرمي التقنية إلى ثلاثة طوائف: المخترقون، المحترفون والحاقدون، كما أن من بين التصنيفات الهامة التميز بين صغار السن من مجرمي الكمبيوتر، وبين البالغين الذي يتجهون للعمل معا لتكوين المنظمات الإجرامية الخطيرة[39].

وقد توصلت الدراسات والأبحاث التي تناولت المجرم المعلوماتي إلى تصيف المجرم المعلوماتي إلى طائفة صغار السن، طائفة القراصنة، طائفة مجرموا المعلومات أصحاب الآراء المتطرفة، طائفة الموظفون العاملون في مجال الأنظمة المعلوماتية، طائفة الحكومات الأجنبية[40].

ويمكن القول أن هذه التصنيفات لا تعني أن كل مجرم معلوماتي يندرج تحت فئة محددة دون غيرها من الفئات المذكورة بل يمكن أن يكون المجرم الواحد مزيجا من طائفة وطائفة أخرى.

3.المطلب الثاني: المحاولات المختلفة لتصنيفات جرائم المعلوماتية

لا تخلو محاولات تحديد وتصنيف الجرائم المعلوماتية من الصعوبة، ويرجع ذلك بصفة أساسية إلى التطور التكنولوجي المستمر، فالجريمة المعلوماتية تلاحق هذا التطور التكنولوجي في كل صوره للارتباط الوثيق بينهما.

ولم تقف هذه الصعوبة حائلا دون المحاولة لتحديد الجرائم المعلوماتية وتقسيمها إلى طوائف مختلفة تتميز كل منها بسمات خاصة بها.

ورغم تعدد التقسيمات اختلافها فيما بينها من حيث أشكال السلوك، إلا أننا سوف نتناول أهم تصنيفات الجرائم المعلوماتية التي أجراها بعض فقهاء القانون الجنائي، وتلك التي أجرتها بعض الاتفاقيات والمنظمات الدولية.

1.3 الفرع الأول: محاولات الفقه لتقسيم جرائم المعلوماتية

نظرا لحداثة الظاهرة نسبيا من ناحية، والتطور المتلاحق الذي يطرأ عليها من ناحية أخرى، فقد اختلف الباحثون في تقسيم جرائم المعلوماتية والأفعال التي تدخل في إطار هذه الجرائم، وسوف نعرض لمحاولتين من أهم المحاولات التي قام بهما اثنان من أبرز المهتمين بجرائم المعلوماتية.

-أولا: تقسيم الأستاذ Ulrich Sieber لجرائم المعلوماتية

قسم الأستاذ **Ulrich Sieber** جرائم المعلوماتية إلى ثلاث طوائف رئيسية، تتعلق الأولى بجرائم الحاسب الآلي الاقتصادية، والثانية بجرائم الحاسب الآلي التي تنطوي على اعتداء على حرمة الحياة الخاصة، والثالثة بجرائم الحاسب الآلي التي تهدد المصالح القومية أو السلامة الشخصية للأفراد[41].

أ-طائفة جرائم الحاسب الآلي الاقتصادية: وتمثل هذه الجرائم الطائفة الرئيسية لجرائم المعلوماتية، وقد أخرج الأستاذ Sieber من نطاق هذه الطائفة الأفعال التي قد تضر بنظام الحاسب الآلي سواء عن طريق الصدفة أو الإهمال، وتندرج تحت هذه الطائفة الجرائم الآتية:

-الاحتيال المعلوماتي: الذي يقوم على التلاعب في نظم المعالجة الآلية للحصول بغير حق على أموال أو أصول أو خدمات.

-التجسس المعلوماتي في قطاع نطاق الأعمال: الذي يقوم على اختراق نظام الحاسب الآلي بهدف توظيف واستغلال ما يتم الوصول إليه من معلومات.

-قرصنة برامج الحاسب الآلي.

-الإتلاف المعلوماتي سواء تعلق الإتلاف بالمكونات المنطقية للحاسب الآلي أو بالمكونات المادية له.

- الدخول غير المصرح به إلى نظام الحاسب الآلي.

-الاستعمال غير المصرح به لنظام الحاسب الآلي.

-الجرائم التقليدية في نطاق قطاع الأعمال التي تساعد على ارتكابها، ويدخل في هذا الإطار استخدام الحاسبات الآلية لإخفاء التلاعب الذي يتم من قبل القائمين على إدارة المؤسسات المالية[42].

ب-طائفة الجرائم المتصلة بانتهاك حرمة الحياة الخاصة: لقد اعتمد الأستاذ Sieber في تحديد هذه الطائفة على معيار موضوعي قوامه تحديد الوسيلة المستخدمة في انتهاك الخصوصية، ويمكن التميز طبقا لهذا المعيار بين أربعة أشكال لهذا التهديد[43].

-استخدام بيانات شخصية غير صحيحة: وذلك عن طريق تغيير البيانات الشخصية أو محوها عن طريق أشخاص غير مرخص لهم بذلك، أو القيام بجمع أو معالجة أو نشر بيانات شخصية غير صحيحة[44].

-جمع وتخزين بيانات صحيحة على نحو غير مشروع: يستمد هذا الجمع أو التخزين صفته غير المشروعة إما من الأساليب غير المشروعة المستخدمة للحصول على هذه البيانات، أو من مضمونها[45].

-الإفشاء غير المشروع للبيانات الشخصية وإساءة استخدامها: ويفرق الأستاذ Sieber في هذا الخصوص بين نوعين البيانات الشخصية، وهما البيانات الشخصية المشمولة بالحماية الجنائية التقليدية للأسرار، والبيانات الشخصية غير السرية[46].

-مخالفة القواعد الشكلية التي تدخل في نطاق الحماية التشريعية لخصوصية المعلومات: في كثير من الدول يعد خرق القواعد الشكلية المتعلقة بتنظيم وجمع ومعالجة ونشر البيانات ذات الطبيعة الشخصية جرائم يعاقب عليها القانون[47].

3-طائفة الجرائم المعلوماتية التي تهدد المصالح القومية والسلامة الشخصية للأفراد: إن الجرائم المعلوماتية تمتد لتشمل أنماطا أخرى من الجرائم قد تمس المصالح العليا للدولة كالوصول إلى المعلومات المتعلقة بالأمن القومي، أو قد تمس السلامة الشخصية للأفراد كالتلاعب بالأنظمة المعلوماتية المتصلة بحركة الطيران[48].

ثانيا:تقسيم الأستاذ Martin Wasik لجرائم المعلوماتية

قسم الأستاذ Wasik جرائم المعلوماتية إلى ثلاثة طوائف رئيسية، أدرج تحت كل منها مجموعة من الأفعال غير المشروعة المرتبطة بالحاسبات الآلية، ويمكن تلخيص تقسيم جرائم المعلوماتية في رأي الأستاذ Wasik على النحو التالي:

أ-الدخول والاستعمال غير المصرح بهما لنظام الحاسب الآلي: يندرج تحت هذه الطائفة عدد من الأفعال، تتمثل في: الدخول غير المصرح به إلى المنظومة المعلوماتي، الدخول غير المصرح به إلى نظام الحاسب الآلي بنية ارتكاب جريمة معلوماتية أخرى، الاعتراض غير المشروع لنظام الحاسب الآلي، الأفعال غير المشروعة المتصلة بالمعلومات الشخصية المعالجة آليا، الاستعمال غير المصرح به لنظام الحاسب الآلي[49].

ب-الاحتيال المعلوماتي وسرقة المعلومات: ويندرج تحت هذه الطائفة عدد من الأفعال، وهي:

التلاعب في المعلومات المعالجة آليا بنية تحقيق ربح مادي غير مشروع، وتزوير المعلومات المعالجة آليا بنية استخدامها في أغراض غير مشروعة، والحصول غير المشروع على المعلومات المعالجة آليا، وقرصنة برامج الحاسبات الآلية[50].

ج-الجرائم التي يساعد الحاسب الآلي على ارتكابها والأفعال التي تساعد على ارتكاب جرائم الحاسبات الآلية: ويندرج تحت هذه الطائفة عدة أفعال تتمثل في:

التخريب والإتلاف سواء انصب على المكونات المادية أو المعنوية للحاسبات الآلية، الاستعمال غير المشروع للحاسبات الآلية لإعاقة المستخدمين الشرعيين لنظام الحاسب الآلي عن الوصول إلى المعلومات التي يحتوي عليها، استخدام أنظمة الحاسبات الآلية للاعتداء على سلامة وأمن الأفراد، التهديد بتدمير المكونات المختلفة للحاسب الآلي لابتزاز المجني عليهم، الإفشاء غير المشروع للمعلومات المؤتمن عليها بمقتضى الوظيفة، صناعة وبيع المعدات والأدوات التي تساعد على ارتكاب جرائم الحاسبات الآلية[51].

2.3 الفرع الثاني: محاولات الاتفاقيات والمنظمات الدولية لتقسيم جرائم المعلوماتية

مع تباين وجهة نظر الفقه تعددت الاتفاقيات والمؤتمرات التي عنت برصد ظاهرة الجريمة المعلوماتية وضبطها، والتي اعتمدت على وجهات نظر مختلفة وخرجت بأنواع وصور عديدة للجريمة، ومن قبيل ذلك اتفاقية بودابست، والاتفاقية العربية لجرائم تقنية المعلومات.

-أولا:تصنيف الاتفاقية الأوروبية لجرائم الكمبيوتر والانترنت (بودابست نوفمبر 2001)[52]

أوجدت الاتفاقية نوع جديد من التقسيمات بشأن جرائم الكمبيوتر المختلفة وأحكامها، وتضمن بشكل واضح أربع طوائف رئيسة لجرائم الكمبيوتر، ويجري تقسيم هذه الطوائف على النحو التالي:

أ-الطائفة الجرائم التي تستهدف عناصر أمن المعلومات: وهي السرية والسلامة وتوفر معطيات نظام الكمبيوتر ويقع تحت هذا الصنف ما يلي:

الولوج غير القانوني(المادة 2)، الاعتراض غير القانوني(المادة 3)، الاعتداء على سلامة البيانات(المادة4)، الاعتداء على سلامة النظام(المادة 5)، إساءة استخدام أجهزة الحاسب الآلي(المادة 6).

ب-الطائفة الجرائم المتصلة بالحاسب الآلي: ويقع تحت هذا التصنيف ما يلي:

التزوير المعلوماتي (المادة 7) ، الغش المعلوماتي (المادة 8).

ج-طائفة الجرائم المتصلة بالمحتوى:وتشمل الجرائم المتصلة بالمواد الإباحية للأطفال(المادة 9).

د-طائفة الجرائم المتصلة بحق المؤلف والحقوق المجاورة (المادة 10).

-ثانيا: تصنيف الاتفاقية العربية لجرائم تقنية المعلومات[53]

لم تتعرض الاتفاقية العربية لمكافحة جرائم تقنية المعلومات إلى تقسيم الجرائم إلى طوائف مثلما فعلت الاتفاقية الأوروبية، بل اكتفت بذكر الجرائم التي تندرج تحت طائفة جرائم تقنية المعلومات.

فنصت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على الجرائم التالية:

جريمة الدخول غير المشروع(المادة6)، جريمة الاعتراض غير المشروع(المادة 7)، الاعتداء على سلامة البيانات (المادة8)، جريمة إساءة استخدام وسائل تقنية المعلومات(المادة9)، جريمة التزوير(المادة 10)، جريمة الاحتيال(المادة11)، جريمة الإباحية(المادة 12)، الجرائم

الأخرى المرتبطة بالإباحية(المادة13)، جريمة الاعتداء على حرمة الحياة الخاصة(المادة14)، الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات(المادة15)، الجرائم المتعلقة بالجرائم المنظمة والمرتكبة بواسطة تقنية المعلومات(المادة16)، الجرائم المتعلقة بانتهاك حقوق المؤلف والحقوق المجاورة(المادة17)، الاستخدام غير المشروع لأدوات الدفع الالكترونية(المادة18).

هذه أهم نظريات تصنيف الجرائم المعلوماتية، وفي معرض تقديرها نستطيع القول أن أكثر التقسيمات انضباطية هو تقسيم الجرائم تبعا إلى جرائم ترتكب على نظم المعالجة الآلية للمعطيات وأخرى ترتكب بواسطته.

حيث أنه بالإضافة إلى كون الجريمة المعلوماتية ظاهرة جديدة، فهي ببساطة استغلال لتكنولوجيات الإعلام والاتصال لارتكاب جرائم قديمة بطرق جديدة وبدون شك للانخراط في أنواع غير محدودة من النماذج الجديدة للأنشطة الإجرامية، لذا نجد المشرع الجزائري من خلال المادة 2 من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال قد صنف هذه الأخيرة إلى طائفتين رئيسيتين، إذ تتمثل الطائفة الأولى في جرائم المساس بأنظمة المعالجة الآلية للمعطيات المنصوص عليها في قانون العقوبات، أما الطائفة الثانية فتتمثل في كل جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية.

4. خاتمة:

مما سبق تناوله نخلص إلى القول بأن الجريمة المعلوماتية هي كل نشاط إجرامي مرتبط باستخدام تقنية المعلومات، وغياب هذا الارتباط يمنع ارتكاب مثل هذا العمل غير المشروع، ولا يختلف هذا الأمر سواء أكانت وسيلة تقنية المعلومات أداة لإتمام النشاط الإجرامي أم كانت محلا له.

فالجرائم المعلوماتية طائفة من الجرائم التي تتميز بطبيعة خاصة عن غيرها من الجرائم، فهي جريمة عابرة للحدود، ذات خصوصية سواء من حيث قلة عدد الحالات التي يتم اكتشافها مقارنة في ضوء ما يتم اكتشافه من الجرائم التقليدية، وصعوبة إثباتها حتى في حال اكتشاف وقوعها والإبلاغ عنها، وتبرز ذاتيتها بصورة أكثر وضوحا في أسلوب ارتكابها وطريقتها وتعدد طوائف مجرميها.

وتجدر الإشارة إلى أن تنوع وتباين التعبيرات والتعريفات التي استخدمت للدلالة والتعريف بظاهرة جرائم المعلوماتية، أدى إلى عدم التوصل إلى نموذج واحد متفق عليه فيما يتعلق بالنشاط الإجرامي لهذه الجرائم، ذلك أن الفقه والأنظمة القانونية في بلدان العالم قاطبة لم تتفق على صور محددة يندرج في إطارها ما يسمى بجرائم المعلوماتية، وما استتبع ذلك من تعذر إيجاد فهم مشترك لهذه الظاهرة الجرمية.

وبناء عليه نقترح ما يلي:

- بما أن لحد الآن لا يوجد إجماع حول المصطلح المعبر لهذه الطائفة من الجرائم، فإنه بالمقابل لا يوجد إجماع فقهي على تعريف موحد لها، لهذا يجب الاتفاق على مصطلح موحد يعبر عن هذه الطائفة الإجرامية المستجدة.

- لابد أن من الإحاطة الكاملة والتحديد السليم لماهية تقنية المعلومات والتي تشكل إطارا وبيئة هذه الجريمة وذلك لإيجاد تعريف سليم لجريمة المعلوماتية.

- إعطاء تعريف للجريمة المعلوماتية وحصرها في إطارها الخاص، وذلك من خلال وضع نظام قانوني وأحكام متميزة تخرج عن دائرة التجريم التقليدي نظرا لخصوصيتها.

-يجب أن يوضح التعريف خصوصية الجريمة المعلوماتية، بحيث يبدو واضحا الدور الذي تقوم به وسيلة تقنية المعلومات في ارتكاب الجريمة، أي أن تقوم هذه الوسيلة بدور في الجريمة على قدر من الأهمية، كأن تسهل ارتكاب الجريمة، أي أن يكون لها دور في إتمامها على النحو الذي تمت به.

-توحيد جهود المجتمع الدولي وكذا المختصين في هذا المجال لوضع تعريف موحد للجريمة المعلوماتية باعتبارها العقبة الأساسية لتحقيق التعاون الدولي لمكافحة هذه الجريمة.

- يجب أن يراعى في تصنيف الجرائم المعلوماتية معيار الحق المطلوب حمايته، وهو التصنيف المعتمد في أي قانون عقوبات، كما يجب أن يراعى في التصنيف التطور المتلاحق لتكنولوجيات الإعلام والاتصال، والذي ينعكس بدوره على الجريمة المعلوماتية بحيث يسمح باستيعاب ما قد يظهر من جرائم جديد.

5. هوامش:

[1] تجدر الإشارة إلى أن هناك تباين كبير بشأن المصطلحات المستخدمة وذلك تبعا لتطور الظاهرة الإجرامية ووضوح صورها، فلم يتفق فقهاء القانون الجنائي في القانون المقارن على الوصف القانوني السليم أو التسمية الفقهية لهذا المصطلح، وهذا ما يثبت أن هذه الظاهرة معقدة ولا يمكن حصرها، فابتداء من اصطلاح استخدام الكمبيوتر مرورا باصطلاح احتيال الكمبيوتر، الجريمة المعلوماتية ، جرائم الكمبيوتر والجريمة المرتبطة بالكمبيوتر، جرائم التقنية العالية، جرائم الهاكرز أو الاختراقات، جرائم نظم المعلومات، الجريمة الالكترونية، جرائم الانترنت، جرائم السيبرانية، وهناك من يطلق على هذه الظاهرة جرائم الكمبيوتر المتقدمة، والإجرام المعلوماتي، والجرائم الرقمية، جريمة أصحاب الياقات البيضاء والجرائم الناعمة والجرائم النظيفة.

والجدير بالذكر أن المشرع الجزائري استخدم في قانون العقوبات مصطلح جرائم المساس بأنظمة المعالجة الآلية للمعطيات، كما أضاف مصطلحا أخر على المنظومة القانونية وذلك من خلال القانون رقم 09-04 المتضمن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال. ونحن من جانبنا نفضل استخدام مصطلح الجريمة المعلوماتية كمصطلح مرادف للمصطلح الذي جاء به المشرع الجزائري من خلا القانون 09-04.لمزيد من التفصيل أنظر: أسامة أحمد المناعسة، جلال محمد الزغبي، جرائم تقنية المعلومات الالكترونية، دراسة مقارنة، ط1، دار الثقافة، عمان، 2014، ص66،67. نبيلة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، دراسة مقارنة، ط1، دار الفكر الجامعي، الإسكندرية، 2007، ص31. أحمد بن عبد الرحمن البغادي، دعاوى الجرائم الالكترونية وأدلة إثباتها في التشريعات العربية بين الواقع والمأمول، المؤتمر الثالث لرؤساء المحاكم العليا بالدول العربية في الفترة 23-25 سبتمبر 2015 بالخرطوم، إدارة الدراسات والبحوث، 1433هـ، ص4. ناول عبد الهادي، تقييم فعاليات المواجهة التشريعية لجرائم الانترنت، مجلة العدل، العدد31 رجب 1427، ص130. سيناء عبد لله محسن، المواجه التشريعية للجرائم المتصلة بالكمبيوتر في ضوء التشريعات الدولية والوطنية، أعمال الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر 19-20 نيسان/ يونيو 2007 المملكة المغربية، ص52.

Nidal El chaer, la criminalité informatique devan

[2] خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، الدار الجامعية، 2008، ص40،41.

[3] le sommet de Berlin, relatif à la cybercriminalité n'aura permis de dégager qu'une seule certitude ; il est pour l'instant impossible de s'accorder sue une définition universelle de la cybercriminalité. Et l'on peut même se demander si une entente sera un jour possible . L'impossible définition universelle de la cybercriminalité, disponible en Ling à l'adresse suivante : www.Village-justice.com. Date de consultation 03/01/2017

[4] نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، دراسة نظرية وتطبيقية، ط1، منشورات الحلبي الحقوقية، بيروت، 2005، ص27،28.

[5] La criminalité informatique est « une action illicite ou l'ordinateur joue un rôle principal pour la commettre ». M chawki, essai sur la notion de cybercriminalité, IEHEI, juillet, 2006 , p26 .

[6] M Tiedmann, la criminalité informatique recouvre « tout acte illégale commis par ordinateur »

نقلا عن عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون النموذجي، دراسة معمقة في القانون المعلوماتي، ط1، دار الفكر الجامعي، الإسكندرية، 2006، ص24.

[7] نسرين عبد الحميد نبيه، الجريمة المعلوماتية والمجرم المعلوماتي، منشأة المعارف، الإسكندرية، 2008، ص56.

[8] أنظر المادة (1) فقرة 8 من نظام مكافحة جرائم المعلوماتية السعودي.

[9] أيمن عبد الله فكري، جرائم نظم المعلومات، دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية، 2007، ص84.

[10] نسرين عبد الحميد نبيه، المرجع السابق، ص58.

[11] أيمن عبد الله فكري، المرجع السابق، ص84.

[12] Monique Hébert, Marilyn Pilon, les délits informatiques, Févrie1984, P3.

[13] محمد علي قطب، الجرائم المعلوماتية وطرق مواجهتها، مركز الإعلام الآلي، الأكاديمية الملكية للشرطة ووزارة الداخلية، البحرين، ص9. مقال منشور على الموقع الالكتروني:-https://www.fichier 1-622375140523727143/10/2015/04/pdf.fr/. تاريخ الدخول إلى الموقع: 2017/01/04.

[14] محمد حماد مرهج الهيتي، التكنولوجيا الحديثة والقانون الجنائي، دار الثقافة، الأردن، 2004، ص152.

[15] وقد وضع هذا التعريف من قبل مجموعة الخبراء المتخصصون في اجتماع باريس الذي عقد عام 1983 ضمن حلقة الإجرام المرتبط بتقنية المعلومات، ويتبنى هذا التعريف الفقيه الألماني Ulrich Sieber. أمير فرج يوسف الجريمة الالكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والانترنت، ط1، مكتبة الوفاء القانونية، الإسكندرية، 2011، ص67.

[16] يونس عرب، جرائم الكمبيوتر والانترنت، إيجاز في المفهوم والنطاق والخصائص والصور والقواعد الإجرائية للملاحقة والإثبات، ورقة عمل مقدمة إلى مؤتمر الأمن العربي 2002، تنظيم المركز العربي للدراسات والبحوث الجنائية، أبو ظبي، 10-2002/02/12، ص4.

[17] M. Chawki, Op.Cit, p27.

[18] عادل يوسف عبد النبي الشكري، الجريمة المعلوماتية وأزمة الشرعية الجزائية، العدد السابع، مجلة مركز الدراسات، جامعة الكوفة، 2008، ص113.

[19] يونس عرب، المرجع السابق، ص5.

[20] أيمن عبد الله فكري، المرجع السابق، ص88.

[21] « Toute infraction susceptible d'êtres commis a l'aide d'un système ou d'un réseau informatique dans un système ou un réseau informatique ou conter un système ou un réseau informatique ». Protéger les internautes, rapport sur la cybercriminalité, groupe de travail interministériel sur la lutte contre la cybercriminalité, Février 2014, p12.

[22] محمد حماد مرهج الهيتي، جرائم الحاسوب، دراسة تحليلية لواقع الاعتداءات التي يتعرض لها الحاسوب وموقف التشريعات الجنائية منها، ط1، دار المناهج، عمان، 2006، ص85.

[23] المادة 2 فقرة أ من القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غش سنة 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر ع 47، الصادرة بتاريخ 5 غشت 2009، ص5.

[24] حيث قال "كولن روز Colin ROSE" وهو خبير في نظم المعلوماتية وأمن الشبكات أن جرائم المعلوماتية هي أكبر ثالث تهديد للدول العظمى بعد الأسلحة الكيمائية والبكتريولوجية والنووية".

Voir : M.Chawki, op cit, p2.

[25] أسامة أحمد المناعسة، جلال محمد الزغبي، المرجع السابق، ص95.

[26] لينا محمد الأسدي، مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية، دراسة مقارنة، ط1، دار الحامد، الأردن، 2015، ص26.

[27] نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة، عمان، 2008، ص55.

[28] حمد محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة، الإسكندرية، 2001، ص103.

[29] أسامة أحمد المناعسة، جلال محمد الزغبي، المرجع السابق، ص96.

[30] نهلا عبد القادر المومني، المرجع السابق، ص58.

[31] نهلا عبد القادر المومني، المرجع نفسه، ص58.

[32] تحفظ البعض من الفقه حيال رسم صورة عامة للمجرم المعلوماتي متسمة بصفة الذكاء، ذلك على سند من القول أن بعض أنماط الجريمة المعلوماتية مثل إتلاف أو تدمير الحاسوب كليا أو جزئيا، لا تحتاج من مرتكبها أن يكون على قدر كبير من الذكاء. حاتم عبد الرحمن منصور الشحات، الإجرام المعلوماتي، دار النهضة العربية، القاهرة، 2003، ص88.

[33] عمر أبو الفتوح عبد العظيم الحمامي، الحماية الجنائية للمعلومات المسجلة الكترونيا، دراسة مقارنة، دار النهضة العربية، القاهرة، 2010، ص79.

[34] عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، دار الفكر الجامعي، الإسكندرية، 2006، ص45.

[35] نائلة عادل محمد فريد قورة، المرجع السابق، ص57.

[36] عمر أبو الفتوح عبد العظيم الحمامي، المرجع السابق، ص80،81.

[37] نائلة عادل محمد فريد قورة، المرجع السابق، ص57.

[38] نائلة عادل محمد فريد قورة، المرجع نفسه، ص58، 59.

[39] حاتم عبد الرحمن منصور الشحات، المرجع السابق، ص93.

[40] فبالنسبة لطائفة صغار السن: يطلق عليهم البعض الآخر صغار نوابغ المعلوماتية، ويقصد بهم الشباب البالغ المفتون بالمعلوماتية وأنظمتها، ويسميهم البعض بمجانين معدلات ومعدلات العكسية بالاستناد إلى كثرة استخدامهم لتقنية المعد والمعدل العكسي (الموديم)، الذي يعتمد على الاتصال الهاتفي لاختراق شبكة النظم. أما طائفة القراصنة: فهم في الغالب مبرمجون من أصحاب الخبرة يهدفون إلى الدخول إلى أنظمة المعلوماتية غير المسموح لهم بدخولها وكسر الحواجز الأمنية المحيطة بهذه الأنظمة، ويمكن تصنيفهم إلى صنفين هما القراصنة الهواة العابثون (Hackers) والقراصنة المحترفون (Crackers)، أما طائفة مجرموا المعلومات أصحاب الآراء المتطرفة: فيقصد بهم طائفة من الناس نزلت بهم عقولهم إلى مستنقع الشطط في التفكير، متطرفون لأفكارهم وأرائهم، ومتجاوزون بذلك كل الحدود المعقولة والمقبولة للتحاور والنقاش، وذلك بخصوص قضية أو غاية ليس لها علاقة بمصالحهم الشخصية، وهم في سبيل تحقيق ما يعتقدونه، على استعداد لارتكاب أنشطة إجرامية مختلفة. أما فيما يتعلق بطائفة الحكومات الأجنبية: فهو يعني تجسس الحكومات على التطور التكنولوجي تجسيدا للتقدم الصناعي، والمتمثل في ثورة المعلومات. لمزيد من التفصيل أنظر: عمر أبو الفتوح عبد العظيم الحمامي، المرجع السابق، ص86 وما يليها. محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري، دار الجامعة الجديدة، الإسكندرية، 2007، ص36 وما يليها. حاتم عبد الرحمن منصور شحات، المرجع السابق، ص97.

[41] لمزيد من التفصيل راجع:

Seiber Ulrich, the international emerfence of criminal information law, carl Heymanns verlag K , G; 1992, pp3-27

مشار إليه تهميش رقم 1 لدى أيمن عبد الله فكري، المرجع السابق، ص121.

[42] علي عبود جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، دراسة مقارنة، ط1،منشورات زين الحقوقية، لبنان، 2013، ص87.

[43] نائلة عادل محمد فريد قورة، المرجع السابق، ص235.

[44] علي عبود جعفر، المجرع السابق، ص88.

[45] لمزيد من التفصيل أنظر: بولين أنطونيس أيوب، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، دراسة مقارنة، ط1، منشورات الحلبي الحقوقية، 2009، ص293 وما يليها.

[46] لمزيد من التفصيل أنظر، بولين أنطونيس أيوب، المرجع نفسه، ص401 وما يليها.

[47] نائلة عادل محمد فريد قورة، المرجع السابق، ص238.

[48] أيمن عبد الله فكري، المرجع السابق، ص122.

[49] نائلة عادل محمد فريد قورة، المرجع السابق، ص243.

[50] Martin Wasik, computer crime, oxford university press, 1991, p41.

مشار إليه لدى أيمن عبد الله فكري، المرجع السابق، ص123.

[51] نائلة عادل محمد فريد قورة، المرجع نفسه، ص244.

[52] بتاريخ 20 نوفمبر 2000 تقدمت اللجنة الأوروبية لمشكلات الجريمة CDBC ولجنة الخبراء في حقل جرائم التقنية بمشروع اتفاقية جرائم الكمبيوتر، وخضعت مواد الاتفاقية المقترحة للمناقشة وتبادل الآراء خلال الفترة من إصدار مشروعها الأول وحتى إعداد مسودتها النهائية التي أقرت لاحقا في بودابست 2001 وتعرف باتفاقية بودابست 2001 (اتفاقية الجرائم الالكترونية- سايبر كرايم)، وجدير بالذكر أن مشروع الاتفاقية قد طرح للحوار المجتمعي عن طريق مواقع عديدة أوروبية وأمريكية على شبكة الأنترنت. وليد طه، التنظيم التشريعي للجرائم الالكترونية في اتفاقية بودابست، ص4. مقال منشور على الموقع الالكتروني الآتي: http://www.lasportal.org/ar/legalnetwork/Documents/%D8%A7%D9%84%D8%AA%D9%86%D8%B8%D9%8A%D9%85%20%D8%A7%D9%84%D8%AA%D8%B4%D8%B1%D9%8A%D8%B9%D9%8A%20%D9%84%D9%84%D8%AC%D8%B1%D8%A7%D8%A6%D9%85%20%D8%A7%D9%84%D8%A7%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A%D8%A9.pdf. تاريخ الدخول 2017/01/16.

[53] الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 21 ديسمبر 2010.

6. قائمة المراجع:

- القوانين

-الاتفاقية الأوروبية لمكافحة الجريمة المعلوماتية (بودابست 2001).

-الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 21 ديسمبر 2010.

-القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غش سنة 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر ع 47، الصادرة بتاريخ 5 غشت 2009.

-نظام مكافحة جرائم المعلوماتية السعودي الصادر بموجب المرسوم الملكي رقم م/17 في 1428/3/8هـ.

- الكتب

-أيمن عبد الله فكري، جرائم نظم المعلومات، دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية، 2007.

-أمير فرج يوسف الجريمة الالكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والانترنت، ط1، مكتبة الوفاء القانونية، الإسكندرية، 2011.

-أسامة أحمد المناعسة، جلال محمد الزغبي، جرائم تقنية المعلومات الالكترونية، دراسة مقارنة، ط1، دار الثقافة، عمان، 2014.

-حاتم عبد الرحمن منصور الشحات، الإجرام المعلوماتي، دار النهضة العربية، القاهرة، 2003،

-لينا محمد الأسدي، مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية، دراسة مقارنة، ط.، دار الحامد، الأردن،2015.

-محمد حماد مرهج الهيتي، التكنولوجيا الحديثة والقانون الجنائي، دار الثقافة، الأردن، 2004.

-محمد حماد مرهج الهيتي، جرائم الحاسوب، دراسة تحليلية لواقع الاعتداءات التي يتعرض لها الحاسوب وموقف التشريعات الجنائية منها، ط1، دار المناهج، عمان، 2006.

-محمد محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة، الإسكندرية، 2001.

-محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري، دار الجامعة الجديدة، الإسكندرية، 2007.

-نبيلة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، دراسة مقارنة، ط1، دار الفكر الجامعي، الإسكندرية، 2007.

-نسرين عبد الحميد نبيه، الجريمة المعلوماتية والمجرم المعلوماتي، منشأة المعارف، الإسكندرية، 2008.

-نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، دراسة نظرية وتطبيقية، ط1، منشورات الحلبي الحقوقية، بيروت، 2005.

-نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة، عمان، 2008.

-عمر أبو الفتوح عبد العظيم الحمامي، الحماية الجنائية للمعلومات المسجلة الكترونيا، دراسة مقارنة، دار النهضة العربية، القاهرة، 2010.

-عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون النموذجي، دراسة معمقة في القانون المعلوماتي، ط1، دار الفكر الجامعي، الإسكندرية، 2006.

-عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، دار الفكر الجامعي، الإسكندرية، 2006.

-علي عبود جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، دراسة مقارنة، ط1،منشورات زين الحقوقية، لبنان، 2013.

-خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، الدار الجامعية، 2008.

-Nidal El chaer, la criminalité informatique devant la justice pénale, Sader, Beyrouth, 2004.

- المقالات:

-ناول عبد الهادي، تقييم فعاليات المواجهة التشريعية لجرائم الانترنت، مجلة العدل، العدد31 رجب 1427.

-عادل يوسف عبد النبي الشكري، الجريمة المعلوماتية وأزمة الشرعية الجزائية، العدد السابع، مجلة مركز الدراسات، جامعة الكوفة، 2008.

-M chawki, essai sur la notion de cybercriminalité, IEHEI, juillet, 2006 .

- المداخلات:

-أحمد بن عبد الرحمن البغادي، دعاوى الجرائم الالكترونية وأدلة إثباتها في التشريعات العربية بين الواقع والمأمول، المؤتمر الثالث لرؤساء المحاكم العليا بالدول العربية في الفترة 23-25 سبتمبر 2015 إدارة الدراسات والبحوث، الخرطوم.

-يونس عرب، جرائم الكمبيوتر والانترنت، إيجاز في المفهوم والنطاق والخصائص والصور والقواعد الإجرائية للملاحقة والإثبات، ورقة عمل مقدمة إلى مؤتمر الأمن العربي10-2002/02/12، تنظيم المركز العربي للدراسات والبحوث الجنائية، أبو ظبي.

- مواقع الانترنيت:

-محمد علي قطب، الجرائم المعلوماتية وطرق مواجهتها، مركز الإعلام الآلي، الأكاديمية الملكية للشرطة ووزارة الداخلية، البحرين. مقال منشور على الموقع الالكتروني:-https://www.fichier pdf.fr/2015/04/10/634372714052375622-1/. تاريخ الدخول إلى الموقع: 2017/01/04.

L'impossible définition universelle de la cybercriminalité, disponible en Ling à l'adresse suivante : www.Village-justice.com. Date de consultation 03/01/2017.